Thèse
de doctorat
de l'UTT

Fatima CHAHAL

Distributed Approaches for Proximity Marketing Environments

Champ disciplinaire :
Sciences pour l'Ingénieur

2024TROY0039 **Année 2024**



utt
UNIVERSITÉ DE TECHNOLOGIE
TROYES

THESE

pour l'obtention du grade de

DOCTEUR
de l'UNIVERSITE DE TECHNOLOGIE DE TROYES

en SCIENCES POUR L'INGENIEUR

Spécialité : SYSTEMES SOCIOTECHNIQUES

présentée et soutenue par

Fatima CHAHAL

le 2 décembre 2024

Distributed Approaches for Proximity Marketing Environments

JURY

M. Toufik AHMED	PROFESSEUR DES UNIVERSITES	Président (Rapporteur)
M. Alvaro ARAUJO	PROFESOR ASOCIADO	Rapporteur
Mme Brigitte KERVELLA	MAITRE DE CONFERENCES	Examinatrice
M. Rida KHATOUN	PROFESSEUR TELECOM PARIS – HDR	Examinateur
M. Marc LEMERCIER	MAITRE DE CONFERENCES	Examinateur
M. Hacène FOUCHAL	PROFESSEUR DES UNIVERSITES	Directeur de thèse
Mme Dominique GAÏTI	PROFESSEURE DES UNIVERSITES	Directrice de thèse

Acknowledgments

I would like to express my deepest gratitude to all those who have supported me throughout my research journey. First and foremost, I extend my sincere thanks to my thesis supervisors, *Pr. Dominique GAITI* and *Pr. Hacene FOUCHAL*, for their invaluable guidance, encouragement, and insights, which have been instrumental in shaping this work.

My heartfelt appreciation goes to the Université de Technologie de Troyes and the *LIST3N* laboratory for providing the resources and environment necessary to conduct my research. I am equally grateful to my colleagues and peers, especially *Dr. Fadhila TLILI, and Antonella YAA-COUB*, for their collaboration, feedback, and the stimulating discussions that enriched my work. I would also like to extend my sincere thanks to the doctoral school, particularly to *Mrs. Pascale DENIS* and *Mrs. Isabelle LECLERCQ*, for their invaluable support and assistance throughout the three years, especially in the final months.

I would like to thank my family, especially my father *Eng. Abdel Majid CHAHAL*, mother *Dr. Malak AFYOUNI*, and *Eng. Wafaa CHAHAL*, whose unwavering support and understanding have been a constant source of strength. Your belief in me has kept me motivated throughout this journey. I also wish to thank my friends, particularly *Dr. Racha SOUBRA*, and *Dr. Bouchra FAKHER*, for their companionship and encouragement.

To everyone who has been a part of this journey, thank you for helping me achieve this significant milestone.

Abstract

Proximity marketing involves communicating targeted messages tailored to consumers based on their geographic location, in real-time. Sending relevant offers based on users' locations allows companies to effectively engage with them and boost customer engagement. However, this field faces challenges: Data security, privacy, and trust issues are hampering widespread adoption. Additionally, current consent mechanisms are often inadequate, providing users with limited control over their data. Many customers are worried about how their information is collected and used, raising transparency concerns. Existing solutions remain limited and do not fully address user concerns. To address these gaps, our research proposes distributed strategies focused on building trust in proximity marketing. We examine trust from three perspectives: protocols, consensus processes, and actor interactions. By improving the security of network protocols, we aim to protect users from unauthorized tracking. We also propose a new consensus method to ensure data integrity and transparency in decision-making. Finally, a new classification mechanism gives users more control over their data, strengthening trust between consumers and retailers.

Key Words: *Proximity Marketing, Electronic data processing—Distributed processing, Digital trust, Wireless LANs, Consensus, Wireless communication system, Consent*

Résumé

Le marketing de proximité consiste à communiquer des messages ciblés et adaptés aux consommateurs en fonction de leur localisation géographique, en temps réel. L'envoi d'offres pertinentes en fonction de la localisation des utilisateurs permet aux entreprises d'interagir efficacement avec eux et de renforcer l'interaction client. Cependant, ce domaine fait face à des défis : les problèmes de sécurité des données, de confidentialité et de confiance freinent l'adoption généralisée. De plus, les mécanismes de consentement actuels sont souvent inadéquats, offrant aux utilisateurs un contrôle limité sur leurs données. De nombreux clients se méfient de la manière dont leurs informations sont collectées et utilisées, soulevant des inquiétudes en matière de transparence. Les solutions en place demeurent limitées et ne répondent pas pleinement aux préoccupations des utilisateurs. Pour combler ces lacunes, Nous proposons des stratégies distribuées axées sur l'instauration de la confiance dans le domaine. Nous examinons la confiance sous trois angles : protocoles, processus de consensus et interactions entre acteurs. En améliorant la sécurité des protocoles, nous visons à protéger les utilisateurs contre le suivi non autorisé. Nous proposons également une nouvelle méthode de consensus pour garantir l'intégrité des données et la transparence dans la prise de décision. Enfin, un nouveau mécanisme de classification donne aux utilisateurs plus de contrôle sur leurs données, renforçant la confiance entre consommateurs et détaillants.

Mots clés :- *Marketing de proximité, Traitement réparti, Confiance numérique, Réseaux locaux sans fil, Consensus, Système de communication sans fil, Consentement.*

Contents

1 Introduction **1**
- 1.1 Environment: Proximity Marketing . . . 2
- 1.2 The General Problematic in Proximity Marketing . . . 3
  - 1.2.1 Privacy Concerns . . . 3
  - 1.2.2 Trust Issues . . . 3
  - 1.2.3 Data Security and Regulation . . . 3
  - 1.2.4 User Engagement and Control . . . 3
  - 1.2.5 Economic Implications . . . 3
  - 1.2.6 Political Factors . . . 3
  - 1.2.7 Ecological Problems . . . 4
- 1.3 Motivation Behind the Research Problem . . . 4
  - 1.3.1 Lack of Clear Classification in the Domain . . . 4
  - 1.3.2 Insufficient Consent Mechanisms and User Trust . . . 4
  - 1.3.3 Lack of Trust Between Actors . . . 5
  - 1.3.4 Inadequate Client Control Over Personal Data . . . 5
  - 1.3.5 Inconsistent Integration Across Network Technologies . . . 5
- 1.4 Objectives of the Research . . . 6
  - 1.4.1 Trust with the Network Tools . . . 6
  - 1.4.2 Trust Using Consensus Mechanisms . . . 6
  - 1.4.3 Trust in the Interaction between the Actors . . . 6
- 1.5 Structure of the Thesis . . . 7

2 Context: Proximity Marketing **9**
- 2.1 Proximity Marketing . . . 10
- 2.2 Use Cases . . . 11
  - 2.2.1 Proximity Marketing in Retail Environments . . . 11
  - 2.2.2 Enhancing Customer Engagement at Events . . . 11
  - 2.2.3 Personalized Offers in Public Spaces . . . 11
  - 2.2.4 Real-Time Analytics and Adaptive Marketing . . . 11
- 2.3 Core Challenges . . . 12
  - 2.3.1 Network Tools Tracking . . . 12
  - 2.3.2 Trust . . . 13
  - 2.3.3 Agreements Mechanisms between Actors . . . 13
  - 2.3.4 Data Protection and Regulation . . . 14
- 2.4 Conclusion . . . 14

3 State of the art: Agreement framework useful for Proximity Marketing **16**
- 3.1 Introduction . . . 17
- 3.2 Network Tools Tracking . . . 17
  - 3.2.1 Network Tools . . . 17

3.2.2 MAC Address . . . 18
3.2.3 Network Integration and Challenges . . . 20
3.2.4 Impact of Proximity on Innovation Networks . . . 21
3.3 Trust . . . 28
3.3.1 State of Privacy Concerns in Proximity Marketing . . . 28
3.3.2 Consent in Proximity Marketing . . . 33
3.3.3 Classification of Proximity Marketing . . . 38
3.4 Agreement Mechanisms . . . 41
3.4.1 Navigating Consensus Algorithm in Cryptocurrency . . . 41
3.4.2 Consensus Algorithm in V2X Communication . . . 45
3.4.3 Consensus algorithm in Commerce . . . 47
3.5 Specific Problems Addressed by This Research . . . 49
3.6 Conclusion . . . 49

4 Contribution 1: MAC Swapping for Enhancing Privacy 51
4.1 Introduction . . . 52
4.2 Privacy Challenges in Proximity Marketing . . . 53
4.2.1 MAC Address Tracking . . . 53
4.2.2 Legal Implications . . . 54
4.3 A Consensus Approach with MAC Address Swap . . . 55
4.3.1 Mechanism of MAC Address Swap . . . 55
4.3.2 Technical and User Benefits . . . 56
4.4 Evaluation . . . 56
4.5 Conclusion . . . 60
4.5.1 Objectives achieved . . . 60
4.5.2 Summary of the chapter . . . 61

5 Contribution 2: A New Agreement Mechanism in Proximity Marketing 62
5.1 Introduction . . . 63
5.1.1 Weaknesses in Consent Management in Proximity Marketing . . . 63
5.1.2 Consent Algorithms . . . 63
5.1.3 Research Questions . . . 63
5.2 Comparative Analysis of Algorithmic Performance . . . 64
5.3 Control Algorithm (CA) . . . 65
5.3.1 Opt-in / Opt-out . . . 65
5.3.2 Do we require more than just opt-in and opt-out? . . . 66
5.3.3 Implementation steps and processes . . . 67
5.3.4 Advantages and Challenges . . . 69
5.3.5 Simulation and Results . . . 70
5.4 Conclusion . . . 74
5.4.1 Objectives achieved . . . 74
5.4.2 Summary of the chapter . . . 75

6 Contribution 3: Classifying Proximity Marketing Actors and Establishing Interaction Levels through Consensus 76
6.1 Introduction . . . 77
6.1.1 The Impact of Uncategorization . . . 77
6.1.2 Addressing the Gap with a New Framework . . . 77
6.1.3 Research Questions . . . 78
6.2 Key Players in Proximity Marketing . . . 78

6.3 Proximity Marketing Category Criteria . . . 79
6.4 Proximity Marketing Categorization . . . 81
6.4.1 Among Prospects: NearBySync . . . 82
6.4.2 Between Prospects and Proxies: ZoneLink . . . 82
6.4.3 Among Marchants and Proxies: GlobeHub . . . 82
6.5 The advantages . . . 83
6.6 The restrictions: . . . 84
6.7 Privacy-Driven Consensus Mechanisms . . . 85
6.8 Implementation in Proximity Marketing . . . 86
6.8.1 Message Queuing Telemetry Transport (MQTT) . . . 86
6.8.2 Paxos . . . 87
6.8.3 Raft . . . 89
6.8.4 PBFT . . . 90
6.8.5 CA . . . 90
6.9 Evaluation . . . 91
6.9.1 Consensus Time . . . 92
6.9.2 Fault tolerance . . . 92
6.9.3 Consistency of offers . . . 93
6.9.4 Composite Metric Analysis of Consensus Algorithms . . . 96
6.10 Conclusion . . . 99
6.10.1 Objectives achieved . . . 99
6.10.2 Summary of the chapter . . . 99

7 Conclusion and Perspectives **100**
7.1 Conclusion . . . 101
7.2 Perspectives . . . 102
7.2.1 Short-term Perspective . . . 102
7.2.2 Long-term Perspective . . . 102

Publications List **104**

Bibliography **105**

A Résumé de la thèse **116**
A.1 Environnement : Marketing de proximité . . . 117
A.2 La problématique générale du marketing de proximité . . . 117
A.2.1 Problèmes de Confidentialité . . . 117
A.2.2 Problèmes de confiance . . . 117
A.2.3 Sécurité des Données et Réglementation . . . 118
A.2.4 Engagement et Contrôle des Utilisateurs . . . 118
A.3 Motivation derrière le problème de recherche . . . 118
A.3.1 Manque de Classification Claire . . . 118
A.3.2 Mécanismes de Consentement et Confiance des Utilisateurs . . . 118
A.3.3 Manque de Confiance Entre Acteurs . . . 118
A.3.4 Contrôle Insuffisant des Données par les Utilisateurs . . . 119
A.3.5 Intégration Incohérente des Technologies Réseaux . . . 119
A.4 Orientations de la Recherche et Contributions . . . 119
A.4.1 Échange des adresses MAC pour améliorer la confidentialité . . . 119
A.4.2 Un nouveau mécanisme d'accord dans le marketing de proximité . . . 120
A.4.3 Classification des acteurs du marketing de proximité et établissement des niveaux d'interaction par consensus . . . 120

A.5 Structure de la thèse . . . 121

B Regulatory Framework in Proximity Marketing **123**
B.1 General Data Protection Regulation (GDPR) . . . 123
B.1.1 Principles and Requirements . . . 123
B.1.2 Impact on Proximity Marketing . . . 124
B.2 California Consumer Privacy Act (CCPA) . . . 124
B.2.1 Principles and Requirements . . . 124
B.2.2 Impact on Proximity Marketing . . . 125
B.3 Colorado Privacy Act (CPA) . . . 126
B.3.1 Principles and Requirements . . . 126
B.3.2 Impact on Proximity Marketing . . . 127
B.4 California Privacy Rights Act (CPRA) . . . 128
B.4.1 Principles and Requirements . . . 128
B.4.2 Impact on Proximity Marketing . . . 129
B.5 Lei Geral de Proteção de Dados (LGPD) . . . 129
B.5.1 Principles and Requirements . . . 129
B.5.2 Impact on Proximity Marketing . . . 130
B.6 Personal Information Protection and Electronic Documents Act (PIPEDA) . . . 131
B.6.1 Principles and Requirements . . . 131
B.6.2 Impact on Proximity Marketing . . . 132
B.7 Personal Data Protection Act (PDPA) . . . 133
B.7.1 Principles and Requirements . . . 133
B.7.2 Impact on Proximity Marketing . . . 133

List of Figures

2.1 Proximity Marketing illustration 10

3.1 MAC Address 19
3.2 Blocks structure 43
3.3 PoW scenario 43
3.4 PoS scenario 44
3.5 PoB scenario 45
3.6 PBFT 47
3.7 Paxos scenario 48
3.8 Raft node state 49

4.1 Broadcast the offers 57
4.2 Receive the offers 57
4.3 Make a decision 57
4.4 Send the decision 57
4.5 Swap MAC every 15 min 58
4.6 Only the first request is accepted and ignore the others 58
4.7 Consensus Correctness 60
4.8 Convergence 60

5.1 CA Steps 68
5.2 Speed 73
5.3 Convergence 74

6.1 Implementation of Proximity Marketing Levels 79
6.2 Illustrative of Proximity Marketing Scales 83
6.3 MQTT with consensus 87
6.4 Consensus Speed 93
6.5 Fault Tolerance 94
6.6 Consistency of Offer for NearBySync 95
6.7 Consistency of Offer for ZoneLink 95
6.8 Consistency of Offer for GlobeHub 96

List of Tables

4.1 MAC Address Resistance 59

5.1 Comparison of consensus algorithms. 64
5.2 Evaluating 72

6.1 Criteria of Proximity Marketing Categories 81
6.2 Comprehensive Examination of Proximity Marketing Categories 83
6.3 Consensus Speed (ms) 92
6.4 OPS Set 1 97
6.5 OPS Set 2 98
6.6 OPS Set 3 98
6.7 Overall Performance Scores 98

B.1 Comparison of Regulatory Frameworks 139

Chapter 1

Introduction

This chapter presented the idea of proximity marketing and explained the rationale for the study, setting the stage for the rest of the thesis. It lists the difficulties that the industry faces, including the absence of formalized categories, privacy issues, and the requirement for consensus-building techniques that build customer and marketer confidence. Also included are the research's goals and major contributions.

1.1 Environment: Proximity Marketing

Proximity marketing is a creative approach that utilizes the power of new communication technology to send tailored marketing messages and offers depending on a consumer's geographic position. Because it may maximize engagement and conversion rates while providing individualized experiences for customers, this strategy has become rather popular in the field of digital marketing. Retailers can create tailored offers that appeal to individual interests by employing location-based data, which increases the relevance and effectiveness of their marketing campaigns. Traditional advertising is made more dynamic and responsive by the ability to reach customers at the precise moment they are near a store or product.

The capacity of proximity marketing to promote improved consumer involvement is one of its main benefits. Proximity marketing generates opportunities for meaningful connections between consumers and brands by providing timely and relevant information. In addition to enhancing the consumer experience, this direct interaction promotes repeat business and fosters brand loyalty. Receiving customized offers throughout a customer's buying experience, for example, fosters a sense of connection and attentiveness from the business and raises the possibility of favorable brand sentiment. In highly competitive markets, this type of connection is especially helpful since it makes brands stand out by giving customers a sense of value and understanding. Moreover, the prompt presentation of tailored offers at pivotal moments—like when a customer is in close proximity to a store or product—dramatically enhances the probability of conversion and purchase. Customers are effectively prompted to take action by proximity marketing because it meets their requirements and preferences at the ideal moment. This may cause people to behave impulsively and make purchases they otherwise might not have thought about. Retailers can use this advantage to increase sales during particular seasons or special events, which will ultimately lead to revenue growth. Additionally, proximity marketing gives companies priceless data-driven insights into the tastes and habits of their customers. Real-time data collection and analysis of consumer habits is made possible for businesses through the integration of technologies like Bluetooth, Wi-Fi (also referred to as the IEEE 802.11 protocol), and 5G. Retailers can use this data to analyze foot traffic, determine dwell periods, and pinpoint popular products. This information helps them make well-informed decisions about inventory control, shop design, and marketing tactics. Businesses may continuously improve their marketing tactics and stay relevant and successful in a market that is changing quickly by examining this data. Not only does proximity marketing increase interaction and yield insights, but it is also a more economical kind of advertising. Instead of aiming wide, businesses should focus their resources on particular target populations. This focused approach reduces waste in advertising expenditures and facilitates more effective marketing budget distribution. Because of this, firms can obtain a larger return on investment (ROI) from their marketing initiatives, which makes proximity marketing a desirable choice for companies of all kinds. Using proximity marketing can provide you a big competitive edge in an industry that is getting more and more crowded. Businesses that use this tactic can set themselves apart by providing distinctive, customized experiences that are tailored to the individual tastes and habits of their customers. Brands who do not offer comparable customized experiences run the danger of losing customers as they become used to customized interactions in other areas of their lives, like social media or streaming services. Thus, by utilizing proximity marketing, companies may both satisfy customers and establish themselves as leaders in their sector for innovation.

To sum up, proximity marketing offers a host of benefits that can greatly increase the efficacy of marketing campaigns. Businesses may navigate the complexity of contemporary marketing settings and build meaningful engagements with customers by concentrating on focused communication and utilizing real-time data. This will increase engagement and boost sales. The function of proximity marketing is expected to become even more crucial as consumer behavior continues to change, providing companies with the resources they need to succeed in a cutthroat industry.

1.2 The General Problematic in Proximity Marketing

Although proximity marketing offers organizations a lot of potential, it also comes with a number of difficult issues that might hinder its application and effectiveness. These challenges include scientific issues including privacy concerns, trust issues, data security and regulation, user participation, and control, in addition to political, economic, and environmental issues. In the context of proximity marketing, the following issues are especially pertinent:

1.2.1 Privacy Concerns

Location-based data collecting frequently happens without express user consent, which raises moral concerns regarding invasions of privacy. Customers are becoming more suspicious of proximity marketing tactics because they are concerned about the collection, storage, and use of their personal data. These worries are made worse by the opaqueness around the use of data.

1.2.2 Trust Issues

The establishment of trust between consumers and retailers is crucial for the effective execution of proximity marketing. Users are likely to disengage and choose not to receive personalized communications if they believe that marketing activities are intrusive or manipulative. Clear communication regarding data policies and the advantages consumers can receive from giving their information is necessary to build confidence.

1.2.3 Data Security and Regulation

There are serious data security risks due to the growing amount of personal information being gathered through proximity marketing. Strict legal frameworks, such the General Data Protection Regulation (GDPR), must be followed by systems to safeguard user data against breaches and misuse. Consumer trust may be lost and there may be serious legal ramifications if these standards are broken.

1.2.4 User Engagement and Control

Giving people real control over their data and interactions is a big problem in proximity marketing. It should be possible for users to alter their choices and select the manner in which they receive marketing communications. Consumers may feel overpowered or alienated without this control, which makes engagement attempts more difficult.

1.2.5 Economic Implications

Proximity marketing can cause differences in market access and economic benefits across enterprises. Smaller retailers could find it difficult to compete with larger companies because they lack the financial means to purchase advanced proximity marketing solutions. This disparity might impede the expansion of regional companies and result in financial injustices.

1.2.6 Political Factors

Regulations and laws governing proximity marketing activities are shaped in large part by political settings. Changing political environments can result in uneven legislation, which can limit the marketing methods that businesses can use and cause uncertainty for them. Furthermore, governmental agendas related to consumer protection and data privacy may have an impact on the application of proximity marketing.

1.2.7 Ecological Problems

It is important to consider how using proximity marketing technologies would affect the environment. Beacons and cell phones are examples of electronic gadgets whose manufacture and disposal add to the problem of electronic waste and resource depletion. In order to reduce the environmental impact of proximity marketing solutions, sustainable practices must be taken into account.

While this research does not aim to address every one of these intricate problems, it does give some suggestions that can help to raise consumer trust and confidence as well as the overall effectiveness of proximity marketing. The primary issues with motivation in the sector that we hope to consider will be looked at in the sections that follow in this thesis.

1.3 Motivation Behind the Research Problem

The swift expansion of proximity marketing, propelled by breakthroughs in Bluetooth, Wi-Fi, and 5G communication technology, has revolutionized the manner in which companies interact with their clientele. Real-time, location-based interactions are made possible by proximity marketing, which also provides businesses with chances to boost conversion rates, better customer experiences, and tailored promotions. But even with its bright future, a number of major obstacles stand in the way of fully reaping its rewards. These problems have aspects that are related to technology, privacy, and trust.

1.3.1 Lack of Clear Classification in the Domain

Lack of a clear framework for categorizing different marketing contexts is one of the main problems with proximity marketing. When it comes to classifying the technologies utilized in these contexts and distinguishing between different levels of proximity (such as personal, local, and global interactions), current methodologies are unclear. Businesses find it difficult to create cohesive tactics that work in a variety of situations when they lack a strong classification system, which can result in inconsistent user experiences and lost marketing opportunities. An organized method is necessary to handle the complexity of proximity-based interactions across several networks (Bluetooth, Wi-Fi, 5G). However, the industry lacks standardized frameworks or clear rules to assist organizations in navigating the operational and technical variations among these environments. Because of this, companies frequently choose ad hoc solutions, which result in inefficiencies and do not fully realize the potential of proximity marketing.

1.3.2 Insufficient Consent Mechanisms and User Trust

User consent and trust are crucial concerns in proximity marketing, when companies track users' physical locations and personal information. Strong, established procedures to guarantee users' explicit, informed permission are lacking, though. Many of the solutions in use today only offer consumers the option to opt-in or opt-out, giving them little control over the types of data that are gathered, how they are used, and how long they are utilized. Because consumers frequently are not aware of the complete scope of data being shared when they interact with proximity marketing technology, this lack of transparency undermines user trust. Consent procedures frequently lack the granularity needed to give users control over particular components of their data. Users are consequently compelled to either unintentionally accept to data practices they find uncomfortable or completely opt out, forfeiting any potential benefits. In the absence of robust user permission mechanisms, proximity marketing is susceptible to privacy infractions, which can result in unfavorable user perceptions and regulatory difficulties for participating organizations. This is especially

crucial in light of Europe's tough data protection regulations, such as the General Data Protection Regulation (GDPR), which have severe consequences for noncompliance.

1.3.3 Lack of Trust Between Actors

In order for proximity marketing efforts to be successful, trust is essential. The lack of trust between customers and retailers, on the other hand, is a recurring issue in this industry. Because they are worried about data exploitation, unlawful tracking, and privacy breaches, many consumers are reluctant to interact with proximity marketing tools. Conversely, retailers frequently lack the resources necessary to convince consumers that their personal data is being managed securely or to clearly explain their data policies. This causes a gap to arise between the expectations of customers and the intents of retailers. Businesses risk lower user engagement, increased opt-out rates, and lost opportunities to profit from proximity-based interactions if they do not have a solid strategy for building trust.

1.3.4 Inadequate Client Control Over Personal Data

The fact that users have no control over their own data is another serious problem. Proximity marketing systems frequently gather a lot of location-based data without giving users enough tools to handle or regulate its usage. Users are rarely offered the opportunity to withdraw or amend their consent when their preferences change, even in cases when data collection is done with their consent. Furthermore, users no longer have control over the processing or transfer of their data after sharing it with marketing platforms or other third-party service providers. The inability to manage personal data is a contributing factor to customer mistrust and reluctance to use proximity marketing apps. Additionally, it brings up moral questions of data ownership and accountability, which must be resolved in order for proximity marketing to develop into a more transparent and user-friendly industry.

1.3.5 Inconsistent Integration Across Network Technologies

Bluetooth, Wi-Fi, and 5G network integration presents opportunities as well as technological difficulties for proximity marketing solutions. The operational parameters of various systems, including range, latency, bandwidth, and energy efficiency, vary. But current proximity marketing solutions frequently have trouble fusing these technologies together in a way that makes sense. Inconsistent user experiences may arise from different communication protocols not working together. For instance, a user may get alerts on time in one place but encounter lag or network problems in another. Users become frustrated and disengaged from proximity marketing initiatives as a result of these anomalies, which reduce their effectiveness.

The absence of classification frameworks, inefficient permission procedures, inadequate data control, and technical difficulties with network integration are some of the many aspects of the multifaceted research problem in proximity marketing. These problems highlight the need for dispersed strategies that can improve privacy, security, and trust while enabling seamless device connectivity. By resolving these issues, proximity marketing can develop into a more dependable and approachable instrument for companies to interact with clients in a way that upholds client privacy and fosters confidence.

1.4 Objectives of the Research

By examining trust from three distinct angles—network technologies, consensus processes, and interactions between marketing actors—this research seeks to enhance trust and confidentiality in proximity marketing contexts. To make proximity marketing more safe and easy to use, each dimension addresses a particular facet of trust.

1.4.1 Trust with the Network Tools

Network tools like Bluetooth, Wi-Fi, and 5G are essential for proximity marketing since they allow for the transmission of marketing messages and the gathering of user data. These tools do, however, frequently encounter issues with data privacy, illegal access, and tracking without user authorization. Since these network tools serve as the primary means of communication between the user and the marketing platform, building user trust in them is crucial to the success of any proximity marketing system. The study will look into how to secure and improve these network technologies to give consumers a safe environment. This entails looking into ways to guarantee safe data transfer, lowering the possibility of data breaches, and putting tighter privacy safeguards in place such MAC switching to stop unwanted tracking.

1.4.2 Trust Using Consensus Mechanisms

Consensus mechanisms are essential for distributed systems, like proximity marketing, to ensure data integrity and accuracy. The absence of a distributed consensus mechanism in conventional marketing systems might result in problems like data manipulation, inconsistent message, or even fraud. This research will guarantee that all participants in the proximity marketing environment concur on the validity of data transactions by presenting a novel consensus technique. The main goal of the study is to create and put into use a distributed consensus method that is especially suited for proximity marketing. This system will guarantee that all marketing offers, consumer data exchanges, and network interactions are approved through a decentralized process by prohibiting any one node or player from changing data without the permission of other participants.

1.4.3 Trust in the Interaction between the Actors

An imbalance of power and control frequently characterizes interactions between various parties in proximity marketing, including retailers, customers, intermediaries, and technology suppliers, particularly when it comes to user data. Consumers frequently do not know how their data is gathered, shared, or utilized, which erodes consumer confidence in the parties involved. Moreover, a lack of openness in the agreements between retailers and intermediaries may also lead to user mistrust. The goal of this research is to create visible, unambiguous processes that promote confidence between all parties. By offering users with greater control over their personal data, such as the ability to opt-in or opt-out of data gathering and sharing, this research will empower users and establish an environment of mutual trust. In order to guarantee that all parties are aware of and abide by ethical data usage standards, the study will also include recommendations for clear and concise data-sharing agreements between merchants and intermediaries.

The purpose of this thesis is to contribute to the creation of a more dependable and safe proximity marketing ecosystem by addressing these three important factors of trust. It highlights the significance of security, transparency, and user empowerment as the main cornerstones of establishing trust in the context of digital marketing.

1.5 Structure of the Thesis

The thesis is divided into seven chapters, each addressing different facets of proximity marketing, focusing on distributed approaches and their implications. The introductory chapters lay the groundwork by exploring the concept, importance, and challenges of proximity marketing, followed by a thorough analysis of the current state of research, particularly in relation to privacy and consumer consent. Subsequent chapters present novel contributions, including mechanisms like MAC swapping for privacy enhancement, a control algorithm for user empowerment in data management, and a consensus framework to classify proximity marketing actors, aiming to build trust and transparency. The conclusion synthesizes these distributed approaches, emphasizing their potential to reshape proximity marketing environments:

- **Chapter 1 Introduction** - This chapter presented the idea of proximity marketing and explained the rationale for the study, setting the stage for the rest of the thesis. It lists the difficulties that the industry faces, including the absence of formalized categories, privacy issues, and the requirement for consensus-building techniques that build customer and marketer confidence. Also included are the research's goals and major contributions.

- **Chapter 2 Context: Proximity Marketing** - This chapter moves the emphasis to proximity marketing's larger context. It describes the fundamental ideas behind proximity marketing, the technology that support it (including Bluetooth, Wi-Fi, and 5G), and the different contexts in which it is used. To demonstrate the useful uses of proximity marketing, a number of use examples are provided, spanning from public areas and events to retail settings. The main issues with data privacy, trust, and network tracking are highlighted in the chapter's conclusion.

- **Chapter 3 State of the Art** - This cutting-edge chapter examines current proximity marketing research with an emphasis on consumer permission and privacy. Developments in network tools, privacy challenges, classification of marketing tactics, and moral dilemmas involving customer consent are important subjects. The chapter looks at issues with online consent, how businesses handle it, and the legal laws of using data. It also emphasizes how developments in communication technologies, which address issues like user acceptance, scalability, and privacy-preserving frameworks for managing data permissions, can improve proximity marketing.

- **Chapter 4 Contribution 1: MAC Swapping for Enhancing Privacy** - This chapter presents a way to change a device's MAC address dynamically in order to safeguard user privacy in proximity marketing. The method keeps secure and effective connections while interfering with unauthorized entities' efforts to track. The technique improves privacy without degrading service quality by periodically switching MAC addresses. This approach gives users more secure space, which not only lowers tracking concerns but also fosters user trust. Results from experiments demonstrate how well this method works to protect privacy in wireless communication settings.

- **Chapter 5 Contribution 2: A New Agreement Mechanism in Proximity Marketing** - The Control Algorithm, a new proposal added to proximity marketing that puts user privacy and control first, is introduced in this chapter. The consensus system incorporates an opt-in/opt-out option that enables consumers to control their data and interactions with marketing efforts. The Control Algorithm has the ability to enhance user engagement, data security, and business insights despite certain obstacles. The present study underscores the significance of user empowerment and establishes the foundation for forthcoming advancements in consensus processes.

- **Chapter 6 Contribution 3: Classifying Proximity Marketing Actors and Establishing Interaction Levels through Consensus** - This chapter presents a consensus framework that categorizes consumers, merchants, and proxy devices and defines levels of interaction in order to improve trust and collaboration in proximity marketing. The paradigm emphasizes user permission and data control while striking a balance between privacy concerns and engagement. It addresses both technical integration and concerns by fostering more individualized, transparent, and trustworthy proximity marketing encounters through the establishment of clear roles and safe communication.
- **Chapter 7 Conclusion** - The study's main results and findings are outlined in the last chapter, which also provides an overview of how the dispersed techniques that have been suggested have addressed the issues of trust, privacy, and data protection in proximity marketing contexts. Furthermore, the chapter provides suggestions for further research, highlighting the necessity of investigating cutting-edge technology, broadening the range of case studies, and scrutinizing the enduring viability of proximity marketing strategies.

Chapter 2

Context: Proximity Marketing

This chapter moves the emphasis to proximity marketing's larger context. It describes the fundamental ideas behind proximity marketing, the technology that support it (including Bluetooth, Wi-Fi, and 5G), and the different contexts in which it is used. To demonstrate the useful uses of proximity marketing, a number of use examples are provided, spanning from public areas and events to retail settings. The main issues with data privacy, trust, and network tracking are highlighted in the chapter's conclusion.

2.1 Proximity Marketing

The practice of sending relevant marketing messages or material to people based on where they are—typically within a predetermined geographic area—is known as proximity marketing. This type of marketing makes use of technology such as Bluetooth, Wi-Fi, and 5G to reach out to prospective clients at the precise moment when they are near a business or attraction.
The main concept of proximity marketing is to improve customer experience, encourage engagement, and increase conversions by offering timely, relevant, and personalized information or offers (figure 2.1). It is frequently used to present specials, customized messaging, or loyalty awards to customers who are in the vicinity of businesses, events, and public areas.
Given that proximity marketing frequently entails gathering location-based data and providing tailored notifications, client consent and privacy are important factors to take into account.
In the past, marketing tactics have mostly depended on general advertising techniques that lack the focus required to successfully target particular consumer segments. By concentrating on the consumer's immediate surroundings, proximity marketing, on the other hand, offers a more sophisticated strategy. As a result of this change, marketing communications can now more effectively target consumers based on their location, activity, and preferences. Consequently, companies may design customized experiences that connect with customers more deeply, increasing engagement and conversion rates.
The field of proximity marketing has undergone tremendous change as a result of the quick development of communication technologies. For instance, Bluetooth Low Energy (BLE) offers a battery-saving way to send brief, focused messages to devices in close proximity. While 5G and upcoming 6G networks offer previously unheard-of speeds and connectivity, creating new opportunities for real-time interactions and data-rich marketing techniques, WiFi technologies, on the other hand, allow businesses to connect with consumers over established network infrastructures.



Figure 2.1: Proximity Marketing illustration

Proximity marketing has potential, but it also has drawbacks, such as privacy and data security issues. In order to establish and preserve customer trust, organizations must address these concerns as they work to capitalize on the advantages of proximity-based interactions. Putting into practice successful proximity marketing strategies also requires careful consideration of the requirement for seamless integration across multiple platforms and technologies.
All things considered, proximity marketing is a major advancement in consumer engagement for businesses as it provides a more sophisticated and focused kind of advertising that meets the needs and expectations of the digital age. In order to give a thorough grasp of proximity marketing's influence and potential in the modern marketing environment, this study will investigate the

different facets of the strategy, including its technological foundations, classification schemes, and real-world implementations.

2.2 Use Cases

This section looks at particular use examples that show how Bluetooth, Wi-Fi and 5G technology can be used to improve local marketing tactics. These examples are intended to demonstrate how these technologies can be used to efficiently provide users in different locations with timely, tailored marketing content.

2.2.1 Proximity Marketing in Retail Environments

Bluetooth, Wi-Fi and 5G can be combined in a contemporary retail setting to produce a smooth and interesting shopping experience. For example, Bluetooth beacons can be placed all over the store to recognize when clients are present and to send customized offers or product details to their smartphones when they get close to particular sections or items. The marketing system of the business can modify offers based on a customer's activity in the store, such as how long they spend in a certain area or what they add to their shopping cart, thanks to the real-time data analysis made possible by the ultra-low latency of 5G network. In order to ensure that consumers can access rich media information, such as video demos or customer evaluations, Wi-Fi adds another layer of connectivity. This helps customers make better decisions.

2.2.2 Enhancing Customer Engagement at Events

Bluetooth can be used to provide location-based alerts to visitors of events like trade exhibitions or big conferences. These messages could be personalized invitations to visit particular booths or reminders about future sessions. These interactions take place in real time with little delay thanks to 5G networks' high-speed data transfer capabilities, which is essential in hectic work environments. To improve overall happiness and engagement, event organizers can use Wi-Fi to give participants access to digital event programs, live-streamed sessions, and interactive maps that are customized based on their past interactions and interests.

2.2.3 Personalized Offers in Public Spaces

Airports and retail centers are two examples of public locations that offer special advantages for proximity marketing. When a consumer enters a designated area, like a food court or a certain business, Bluetooth beacons positioned at key locations can recognize them and send them personalized offers or coupons straight to their smartphone. These interactions can be tailored in real time using the 5G network, based on the user's preferences or past purchases, by suggesting things they might like or giving discounts on their preferred brands. These public areas' Wi-Fi can be used to entice users to join the network so they can take advantage of location-based loyalty programs and receive additional offers.

2.2.4 Real-Time Analytics and Adaptive Marketing

Real-time analytics made possible by 5G network can greatly increase the efficacy of proximity marketing efforts in a dynamic marketing environment. Bluetooth beacons, for instance, can be used by a chain of retail outlets to monitor consumer movements and collect information on their purchasing habits. This data is quickly sent to a central system via the 5G network, where it is processed to find patterns and user preferences. Adaptive information, such flash offers or product

recommendations that match customers' buying habits, may then be pushed to consumers via Wi-Fi by marketers, guaranteeing that their messages stay impactful and relevant.

2.3 Core Challenges

2.3.1 Network Tools Tracking

Since proximity marketing depends on the smooth operation of numerous network tools and platforms, communication technology integration is a major difficulty. In order for proximity marketing to be effective, a number of technologies, including as GPS, Bluetooth, Wi-Fi, 5G, and 6G, must cooperate to give users timely and pertinent information. For the creation of a seamless and productive user experience, this technological synergy is essential. Achieving this degree of integration, nevertheless, requires overcoming a number of challenges pertaining to device interoperability and network compatibility.

A fundamental problem in the tracking of network tools is that communication methods are not standardized. Disparities in these protocols can result in differences in how proximity marketing systems perform across devices. Various network protocols operate according to different standards. For example, Wi-Fi and Bluetooth have different benefits, but how they work with smartphones and other linked devices varies greatly based on the brand, settings, and operating system. This lack of consistency may lead to uneven performance, with some consumers possibly receiving marketing messages as intended and others possibly seeing communication breakdowns or delays. Due to their disruption of the user path and creation of gaps in the customer experience, such inequalities have the potential to reduce the effectiveness of proximity marketing initiatives.

The devices' inherent heterogeneity presents another difficulty. Owing to the widespread use of smartwatches, smartphones, and other Internet of Things devices, proximity marketing systems need to support a variety of hardware setups. Different features, such as variances in processing power, battery efficiency, and signal strength, may be available for each device. Because of this diversity, complex network tracking techniques are required that can optimize information delivery to various devices without sacrificing accuracy or speed. The integration of these instruments needs to take into consideration not only the current technical environment, but also the possible effects of signal interference, network congestion, and connection stability variations. Furthermore, the integration issues will get more complex as proximity marketing develops with the advent of sophisticated technologies like 5G and 6G. Although these next-generation networks offer improved connectivity, reduced latency, and higher speeds, they also call for sophisticated architecture and tracking system optimization. Marketers must make sure that their campaigns can change with the network environment. This may include replacing or updating outdated systems to keep them compatible with devices and protocols that are more recent.

User trust and engagement can be severely damaged by inconsistent user experiences brought on by proximity marketing systems' incapacity to operate well across a variety of network protocols and devices. For instance, a consumer may feel irate and choose to unsubscribe from future marketing efforts if they receive numerous notifications or unrelated content as a result of communication lag. This emphasizes how crucial it is to provide resilient, flexible network solutions that can monitor and react to various technological situations instantly, guaranteeing a smooth and customized user experience across all platforms. In conclusion, the effectiveness of proximity marketing depends on resolving the issues raised by network tool tracking. Marketers can make sure that their campaigns are not only successful but also dependable and consistent by investing in more sophisticated and interoperable systems that support a variety of communication technologies and devices. This will increase user satisfaction and brand loyalty.

2.3.2 Trust

Trust and user involvement are essential to proximity marketing's effectiveness. It can be difficult to engage people without coming across as invasive, even while the intention is to do so by giving them timely and relevant information. In order to preserve trust, personalized marketing techniques must strike a balance between user privacy and engagement. Users may choose to opt out of proximity marketing campaigns if this is not done.
The goal of proximity marketing is to improve the shopping experience for customers by offering tailored offers or information at critical times. But, consumers can respond badly to these initiatives if they believe they are an invasion of their privacy, which would cause them to lose faith in the company and stop interacting with it. Since it can be challenging to regain trust once it has been damaged, marketers must implement privacy-preserving techniques.
Personalized marketing strategies need to carefully balance user privacy with engagement in order to maintain confidence. This includes open data policies, in which users are notified about the types of data being gathered, how it will be utilized, and what advantages they may stand to gain. Furthermore, giving consumers control over their data—by giving them the ability to alter privacy settings or refuse data gathering, for example—can greatly increase their feeling of security and confidence in the company.
Users may decide to completely opt out of proximity marketing efforts if marketers are unable to strike this balance. Users who make such choices may lose out on potentially advantageous interactions that are catered to their tastes, which can result in missed chances for both marketers and consumers. As a result, developing trust and placing a high value on confidentially improves user connections and proximity marketing methods' overall efficacy.

2.3.3 Agreements Mechanisms between Actors

Effective execution is currently seriously hampered by these actors' severe lack of mutual trust and unambiguous agreements. For example, insufficient transparency about the use of personal data by firms frequently makes consumers uncomfortable about sharing that information with them. Participation in proximity marketing campaigns may be impeded by this mistrust.
Furthermore, companies could find it difficult to come to trustworthy agreements for data sharing with outside service providers like technological intermediaries or data brokers. Businesses run the danger of unapproved data usage without clear agreements, which could have negative legal effects and erode customer trust.
Furthermore, companies could find it difficult to come to trustworthy agreements for data sharing with outside service providers like technological intermediaries or data brokers. When businesses use proximity marketing technology without telling customers about their data collection activities, for example, various difficulties can be observed. Customers may feel violated and skeptical if they receive unsolicited advertising messages and do not know how their data was collected. Furthermore, companies may unintentionally expose private customer information if they lack strong contracts with service providers, which would further erode confidence in the proximity marketing ecosystem.
To sum up, building confidence and enabling safe data sharing amongst all parties engaged in proximity marketing requires the implementation of strong agreement procedures. By addressing these issues, marketing interactions will become more transparent and user-centric.-defined agreements, companies run the danger of unapproved data use, which might have negative legal effects and erode customer trust.

2.3.4 Data Protection and Regulation

While proximity marketing gains a lot from the integration of bluetooth, Wi-Fi, and 5G technologies, it also poses serious privacy and ethical issues. The issue of data collection, which involves the massive collection of personal data—including location and consumer behavior—without always getting the express approval of the user, lies at the heart of these worries. Users must give their informed consent after being made fully aware of the data being collected, its intended use, and the individuals who will have access to it. Retaining confidence and complying with laws such as GDPR, which require data gathering to be restricted to vital information, depend on this transparency.
Furthermore, giving consumers control over their data and being transparent about how it is used are essential ethical precepts. It should be simple for users to manage their consent and to choose to delete or opt out of having their data used. Preventing privacy intrusions requires a fundamental respect for the autonomy of the user. Furthermore, the possibility of data breaches and illegal access exacerbates privacy issues, which is why strong data security measures are essential. These dangers can be reduced by using strong encryption, safe data storage, and privacy by design.
Lastly, manipulative techniques must be avoided in the ethical use of data. Although proximity marketing can improve user experience by personalizing it, it must be careful not to take advantage of users' weaknesses or put them under undue pressure. Fair marketing tactics should steer clear of bias or discrimination in content delivery and targeting. Adherence to legal and regulatory frameworks, such as GDPR, is not only legally mandated but also morally required, guaranteeing that proximity marketing strategies uphold users' rights and foster their confidence.
Regulations pertaining to proximity marketing seek to strike a compromise between the necessity for companies to obtain important customer information and the requirement to safeguard personal information. Strict guidelines for the handling of personal data are established by important regulations like the Singapore Personal Data Protection Act (PDPA), the California Consumer Privacy Act (CCPA), the General Data Protection Law (LGPD) in Brazil, the General Data Protection Law (LGPD) in the European Union, the General Data Protection Regulation (GDPR) in the European Union, and the Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada. These rules place a strong emphasis on responsibility, transparency, and user permission. They also apply heavy consequences for non-compliance. We will not explore this topic in greater detail in this thesis because it is not relevant to our aims. Please see Appendix B for further information on these requirements.

2.4 Conclusion

In summary, proximity marketing is a complex field that interacts with many facets of society, such as the political, economic, and ecological spheres. But in this changing environment, this thesis focuses particularly on the crucial domains of network and data protection. The relationship between user engagement, trust, and confidentiality is becoming more and more crucial as proximity marketing gains momentum.
Because there are so many different protocols and devices in use, it can be difficult to integrate communication technologies in a way that makes proximity marketing methods work. Marketers can improve user experiences and build trust by putting efficiency and compatibility first. Without it, consumers would stop interacting with companies, which would undermine the possible advantages of proximity marketing campaigns. Therefore, trust is crucial.
Moreover, any effective approach must include user data protection and compliance with legal requirements. Building trust and promoting user engagement can be greatly aided by openness in data gathering procedures, strong security measures, and giving users control over their personal data.

This thesis attempts to offer a concentrated analysis of how network and data dynamics impact this sector, even though the wider implications of proximity marketing deserve more investigation. We can provide a path for more responsible and successful proximity marketing techniques that respect consumers' privacy and security while simultaneously engaging them by tackling issues with trust, confidentiality, and network security.
We will cover the most important research contributions in this area in the next chapter 3 along with the techniques, important findings, and technical developments that have shaped our understanding of proximity marketing. We will contextualize our work and identify gaps that our research aims to fill by synthesizing the body of previous literature.

Chapter 3

State of the art: Agreement framework useful for Proximity Marketing

This cutting-edge chapter explores how proximity marketing is changing and emphasizes the importance of trust mechanisms and agreement frameworks in raising client involvement. Proximity marketing, which provides individualized advertising based on customers' real-time physical locations, has gained popularity as a result of the widespread use of smartphones and location-based technologies. Important subjects include the use of network tools for tracking, the importance of MAC addresses, and the difficulties in integrating them into current infrastructures. The chapter classifies numerous marketing tactics and addresses ethical implications while critically examining privacy concerns, with a particular focus on user consent in proximity marketing. It also looks at the implications of data consumption for the law and how closeness affects innovation networks. This chapter also explores consensus algorithms in a variety of settings, including bitcoin, voice-to-text (V2X) communication, and commerce, demonstrating how these processes might promote cooperation and trust in proximity marketing settings. In the end, the chapter highlights particular difficulties encountered throughout the research, opening the door for additional studies into privacy-preserving frameworks and variables affecting user data permissions.

3.1 Introduction

Using location-based technologies, proximity marketing is a cutting-edge strategy that targets customers with offers and adverts in real-time depending on their geographic position. The growing popularity of smartphones and developments in mobile technology have led to significant adoption of this approach. Due to this increased interest, proximity marketing has emerged as a hot topic in scientific study since the early 2000s, sparking a number of studies that try to explore its possibilities and overcome its difficulties. Proximity marketing has the ability to increase consumer involvement and boost sales, but it also has drawbacks. These include issues with client consent, privacy, and marketing strategy classification.
One important topic that has been researched in recent years is the clients' agreement to receive proximity-based offers. Nowadays, a lot of companies use invasive surveillance techniques without getting the express consent of their customers, which presents moral and legal issues. In order to address this, the researcher investigates a few technological instruments to give the clients a better environment. In this chapter, we analyzed current mechanisms, assessed their efficacy, and offered our opinions.
Furthermore, the analysis attempted to create a systematic framework that distinguished between various degrees of proximity marketing according to their operational characteristics and advantages for both clients and businesses, even though the sector is acknowledged as being large and diverse. Do they actually make it obvious, though? This chapter looks at the methods used in categorization today and presents the researcher's framework, which aims to provide the field structure and clarity.
The development of proximity marketing is greatly aided by the evolution of network tools. The scientific work has made it possible for businesses to reach and engage customers more efficiently using proximity marketing techniques, as evidenced by the rapid development of communication technologies. An overview of these technical developments and how they affect proximity marketing is given also in this chapter.
Last but not least, privacy is still a top priority in proximity marketing. Companies regularly monitor customers around their locations, frequently with insufficient privacy protections. In order to address these worries, researchers and legal experts collaborated on the consent algorithm with the goal of enhancing security and safeguarding user privacy. Additionally, we examined the privacy concerns that currently exist, studied the available solutions, and talked about these approaches to improve privacy in proximity marketing.
In conclusion, this chapter offers a thorough analysis of proximity marketing's current state of the art, pointing out problems and gaps in the field while also setting the stage for creative solutions that the scientific community has to offer. We seek to contribute to the creation of a more moral, practical, and user-friendly proximity marketing environment by investigating consent procedures, categorization frameworks, technology developments, and privacy protection tactics.

3.2 Network Tools Tracking

3.2.1 Network Tools

The growing desire for tailored, location-based content distribution and the unique characteristics of Bluetooth, Wi-Fi, and 5G network are the driving forces for their incorporation into local marketing campaigns. Because Bluetooth, or wireless personal area network technology, can run at minimal energy consumption and still maintain a reliable connection over short distances, it is very useful for proximity marketing. This makes it perfect for delivering promotions or tailored ads to customers in the area.This section delves into the details of the three main technologies that underpin contemporary proximity marketing strategies. When combined, the distinct capabilities

of each technology provide a potent ecosystem that facilitates the delivery of location-based, targeted marketing information.

Bluetooth

A wireless communication protocol called Bluetooth is intended for short-range data exchange with low battery consumption. It is better suited for uses like proximity marketing that call for sporadic data transfer. Bluetooth beacons are tiny, always-broadcasting devices that connect with neighboring smartphones and tablets to facilitate proximity marketing.
The main benefit of bluetooth is its low energy consumption, which enables beacons to run for longer periods of time between battery changes. Because of this, it is perfect for use in settings like retail establishments, where customers can be detected and location-based messages may be triggered by strategically placing beacons. Depending on the surroundings and the arrangement of the beacon, Bluetooth's range can vary from a few millimeters to over 100 meters, making it adaptable for a variety of marketing scenarios [93].

Wi-Fi

Wi-Fi is a widely used wireless networking technology that enables localized internet connections for devices. It uses the 2.4 GHz and 5 GHz frequency bands for operation, with Wi-Fi 6 and other more recent standards providing increased performance, efficiency, and speed in crowded places.
Wi-Fi provides a flexible framework for content distribution in proximity marketing. It is a great way to reach a large audience because it is widely available in both public and private settings. Users connecting to the network can get rich media material via Wi-Fi, including interactive ads, digital brochures, and films. Moreover, Bluetooth and 5G can be combined with Wi-Fi networks to improve location-based services' accuracy and give consumers uninterrupted connectivity across various environments [142].

5G cellular network

Fifth-generation (5G) cellular networks are expected to improve upon the capabilities of 5G with even faster speeds, lower latency, and more dependable connections. Data transfer rates have increased significantly from 4G to 5G, reaching up to 10 Gbps, and latency has decreased to as low as 1 millisecond.
Because of these improvements, 5G network is especially well-suited for real-time applications where rapid information delivery is essential, such proximity marketing. In the context of local marketing, 5G can facilitate real-time analytics, augmented reality experiences, and high-definition video streaming—all of which depend on dependable and quick data connections. Additionally, 5G's enhanced network capacity guarantees the simultaneous connection of numerous devices, which is crucial in congested settings like festivals or retail malls.

3.2.2 MAC Address

A network interface's Media Access Control (MAC) address is a special identification given to it for data link layer communications inside a network segment. Devices on a local network can be uniquely identified using it, ensuring that data packets are delivered to the right place [6, 129]. Particularly in Ethernet and Wi-Fi networks, MAC addresses are crucial parts of many networking protocols (figure 3.1). Because MAC addresses let marketers identify, follow, and interact with customers based on their actual location, they are a crucial facilitator of proximity marketing [155].

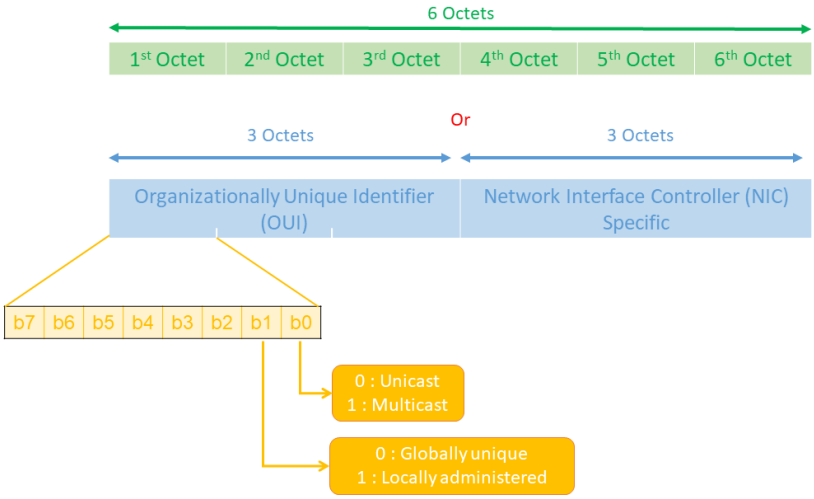


Figure 3.1: MAC Address

Technical Details:

A MAC address structure comprises six groups of two hexadecimal digits, totaling 48 bits that are often shown in hexadecimal format. A MAC address could look like this, for instance: 00:1A:2B:3C:4D:5E. The Organizationally Unique Identifier (OUI), which identifies the network interface card's manufacturer, is normally represented by the first three octets (24 bits). Each NIC has its remaining three octets (a total of 24 bits) allocated to it specifically by the manufacturer.

Address Types:

Within a network, MAC addresses come in three main varieties that are utilized for diverse communication needs. A single network interface can be uniquely identified by a unicast address, which is the first type. Data packets are routed to a particular device when transmitted to a unicast address, guaranteeing that the data is processed by the intended recipient exclusively. In a network, one-to-one communication requires this kind of address. Broadcasting data packets to several devices is possible with the second form of address, known as a multicast address. All other network devices disregard the packets, but the devices that are a part of this multicast group process them. This technique works well for applications like streaming movies to multiple users since it can send the same material to multiple devices efficiently without overloading the network. The MAC address **FF:FF:FF:FF:FF:FF** is the representation of the broadcast address, which is the third type. Data packets are sent to each device on a local network segment using this address. Sending information that must reach every device, like network announcements or IP address requests during the earliest stages of network configuration, can be accomplished through broadcasting.

Layer Functionality:

The MAC address operates at the Data Link Layer, or Layer 2, in the OSI model. This layer contains error detection and management methods and is essential for node-to-node data transport. Because they are incorporated into the frame headers of data link layer protocols like Ethernet, MAC addresses are crucial to this process. The source and destination MAC addresses are included in every frame header, guaranteeing that data packets are sent to the right people. In order to keep communication inside a network structured and effective, this addressing scheme is essential.

Permanent vs. Temporary:

A MAC address may be assigned temporarily or permanently. The actual MAC address, also known as the Burned-in Address (BIA), is hard-coded into the network card during manufacturing with the goal of ensuring global uniqueness. This guarantees that each device is uniquely identified. Nonetheless, devices can be configured by network administrators to utilize a Locally Administered Address (LAA) in place of the BIA. Because LAAs are modifiable, unlike BIAs, they are especially helpful for handling network policies and addressing potential MAC address conflicts. Better control and customization within the network are made possible by this flexibility.

Address Resolution Protocol (ARP):

In a local network, the Address Resolution Protocol (ARP) is necessary for translating IP addresses to MAC addresses. ARP is used by a device to find the MAC address linked to the IP address of the target device when it needs to communicate with another device on the same network. Broadcasting a request to every device on the local network to find out which device has the unique IP address is known as the ARP procedure. In response, the device with the same IP address provides its MAC address. With this response, the starting device can create the frame header required for data transmission, which makes device-to-device communication precise and effective.

3.2.3 Network Integration and Challenges

There are several operational and technological difficulties with using bluetooth, Wi-Fi, and 5G technologies into proximity marketing plans. Ensuring compatibility with current systems, especially legacy infrastructures that might not be compatible with more recent wireless standards, is one of the main issues. This frequently calls for expensive and complicated system changes, such as new hardware and software.

Another major problem is signal interference, which is particularly problematic in settings when several wireless technologies are in use at the same time. For instance, there may be interference due to bluetooth and Wi-Fi sharing the 2.4 GHz frequency range, which could lower the dependability and quality of the signal. For businesses to minimize these issues and preserve peak performance, sophisticated network management tools and meticulous planning are essential.

Scalability is another issue, especially with proximity marketing environments seeing an increase in the number of linked devices. Large-scale deployments are limited by bluetooth, Wi-Fi, and 5G network; to accommodate higher device density without sacrificing performance, novel network topologies and management tools are needed.

Energy efficiency is very important, particularly for beacons and other battery-operated equipment. Even though bluetooth is meant to use little energy, high-density situations can nevertheless put a strain on battery life. To maintain long-term operating efficiency, businesses need to investigate energy harvesting technologies and employ power-saving initiatives.

Sustaining uninterrupted connectivity in a variety of settings is necessary to deliver standardized user experiences. Brief disruptions in the handoff between various network types, such Wi-Fi and 5G, can impact the transmission of marketing content. Businesses can solve this by utilizing edge computing and network aggregation technologies to guarantee continuous service.

Lastly, there are additional security issues brought about by the integration of various technologies. Given the growing susceptibility of proximity marketing systems to cyberattacks, it is critical to put strong security measures in place, including encryption, secure authentication, and frequent software updates. Maintaining the integrity of the marketing infrastructure and safeguarding user data require ensuring security at every level of the system.

3.2.4 Impact of Proximity on Innovation Networks

In the work of *Francesco Capone and Luciana Lazzeretti* [70], they explore how proximity affects innovation network dynamics as clusters change. The high-tech products used in Tuscany's cultural goods industry are highlighted. The authors examine how these networks have changed over a ten-year period using stochastic actor-oriented models (SAOM). Their results show that organizational, cognitive, and geographic proximity are important in the establishment of networks, but that these factors become less significant as the cluster gets older.

The goal of the study is to fill a vacuum in the literature by focusing more on the dynamic evolution of innovation networks than their static structure. The authors offer new insights into the dynamic nature of innovation networks by examining the effects of different forms of proximity on the establishment and evolution of these networks within a cluster context.

The evolution of innovation networks in the high technology applied to cultural products industry in Tuscany is examined through the use of stochastic actor-oriented models (SAOM) in this study. The data comprises 42 policy-supported networks and covers more than ten years. The authors are able to capture the dynamic changes in network architecture over time thanks to their analytical technique. The results may not fully capture the dynamics of informal networks, which are equally important for innovation, as the study primarily examines formal innovation networks backed by regulations. One of the main conclusions is that, in the early stages of a cluster's creation, physical closeness plays a critical role in promoting initial network formation. That being said, as the cluster ages and develops, its influence decreases. The establishment of innovation networks is facilitated by cognitive closeness, which is important at first but becomes less so as the cluster gets bigger. Institutional closeness plays an important role in the early stages of network formation during the emergence phase, but its impact lessens during the development phase. Organizational closeness is crucial initially, but as the cluster develops, it becomes less important. Social closeness is important during the emergence and development stages, but its influence wanes with time.

There are some shortcomings in the study, even with its thorough investigation. The research is concentrated on the high technology applied to the Tuscany cultural products sector; hence, although the results offer insightful information on the dynamics of innovation networks in this particular setting, they might not apply to other industries or geographical areas. Furthermore, just three snapshots of the network—from 2000, 2005, and 2010—are provided, despite the study spanning more than ten years. The dynamic and ongoing nature of network evolution might not be well conveyed by this.

The study offers a strong foundation for examining network dynamics since it mainly depends on quantitative approaches and sophisticated econometric tools. But this quantitative emphasis could ignore the subtleties and qualitative elements that are crucial for comprehending the underlying mechanisms. Moreover, the study's data originates from policy-supported networks, which might not encompass all pertinent actors and linkages in the industry, thus providing an imperfect depiction of the dynamics of innovation networks.

When using stochastic actor-oriented models (SAOM), it is assumed that actors employ the objective function to guide their rational decision-making. In practice, a variety of factors, such as irrational actions and outside events that the model might not have fully accounted for, impact network dynamics. Furthermore, the study does not explore the particular actions and tactics of individual individuals inside the network, instead concentrating on network-level dynamics. Deeper understanding of how proximity influences business and organizational decisions and interactions may result from this.

The study comes to the conclusion that while various forms of closeness are important in the establishment of innovation networks, their influence changes with time. As the cluster grows, institutional and social proximity loses significance, although geographic and cognitive proximity does. The management of innovation networks and the creation of public policies meant to

promote innovation within clusters will be significantly impacted by these findings.
The knowledge gathered from this research indicates that while developing strategies to assist innovation networks, managers and policymakers should take the dynamic nature of proximity into account. To help networks establish, efforts could first concentrate on improving cognitive and geographic proximity. Strategies should change to reflect the evolving importance of various forms of proximity as the cluster matures. Policymakers and practitioners who want to foresee and influence the direction of innovation in the industry may find this useful.
Notwithstanding these drawbacks, the paper significantly advances our knowledge of innovation networks and the function that proximity plays in their dynamics. By combining qualitative and quantitative methodologies, broadening the scope to encompass informal networks and a wider range of industries and geographies, and explicitly accounting for outside influences and actor-level behaviors, future study could solve these shortcomings.

The deployment and efficacy of proximity marketing utilizing network technologies are examined in the paper **"IoT based Proximity Marketing"** by *Zanele Nicole Mndebele and Muthu Ramachandran* [95]. The study focuses on a system dubbed Precinct PMaaS (Proximity Marketing as a Service). The report highlights that Wi-Fi is a better option for proximity marketing than Bluetooth since it is more widely used, has faster connectivity, and has a wider coverage, particularly in cities like Leeds.
Precinct PMaaS determines a subscriber's eligibility for message delivery by using GPS characteristics and network information such the network name (SSID). This guarantees that messages are sent to devices only within the specified geographic area and to those linked to a certain network. To guarantee pertinent and timely message delivery, the system can recognize and retrieve network service information, uniquely identify devices, and validate network connections.
Experiments contrasting Precinct PMaaS with Bluetooth alternatives indicated the higher efficiency of the Wi-Fi-based system. Message delivery speeds were faster with Precinct PMaaS, average 1.24 seconds, than with Bluetooth solutions, which also had limits on how many devices they could connect to at once. Wi-Fi did not require a detection interval of approximately 10 seconds prior to transmission, whereas Bluetooth-based solutions did. Furthermore, Precinct PMaaS offered greater performance and capacity than Bluetooth solutions, which could only manage seven devices at once. Data from the testing phase demonstrated Precinct PMaaS's constant performance under a range of situations, including dependable message delivery timings and signal strength. According to the study, Big Data analytics may be used to further improve IoT-based proximity marketing that is fueled by network information in order to better understand customer behavior and increase the efficacy of proximity marketing tactics. But the study also points up a number of shortcomings and flaws. Users must install a certain mobile application and register for the service in order to utilize Precinct PMaaS, which could restrict the reach and potency of the marketing messages. Because the system depends on Wi-Fi networks to relay messages, it may not work well in places with spotty coverage or erratic connections. Wi-Fi has benefits in terms of speed and range, but its usefulness depends on the network's quality and availability.
The tracking of user locations and the delivery of tailored messages based on proximity generate privacy concerns due to data consumption and intrusive marketing methods. Precinct PMaaS was tested using a small number of devices in a controlled setting at Leeds Beckett University. This may not fully reflect how the system performs in a variety of real-world scenarios with different network infrastructures and more devices.
The study mainly contrasts Precinct PMaaS with freeware Bluetooth solutions, which might not be the most sophisticated or economically feasible substitutes. A more thorough evaluation of its shortcomings and efficacy might come from a more extensive comparison with comparable for-profit proximity marketing programs. Furthermore, the system's current emphasis on message delivery via a Wi-Fi network and mobile app may restrict connection with other IoT platforms or

devices that could improve the proximity marketing experience.
These drawbacks point to areas where IoT-based proximity marketing solutions should be improved in the future. To improve the scalability and resilience of such systems, more investigation and development may be necessary to solve these problems. In summary, the study emphasizes the benefits of utilizing Wi-Fi for proximity marketing, specifically in Precinct PMaaS. Wi-Fi offers notable advantages over Bluetooth with respect to speed, capacity, and efficiency, making it a feasible choice for focused digital marketing campaigns.

Using a variety of network technologies, proximity marketing targets prospective consumers with messages and ads according on their physical vicinity to a certain site. The **"Beacon for Proximity Target Marketing"** study explores various technologies, with particular emphasis on RFID, Bluetooth, and Wi-Fi [8].
One of the main technologies utilized in proximity marketing is Bluetooth. It is dependent on beacons, which transmit signals to neighboring Bluetooth-capable gadgets. If the consumers have the appropriate software loaded on their mobile devices, these signals may cause notifications or adverts to appear. Bluetooth offers several benefits, including low power consumption and multi-device pairing within a given range. Its drawbacks include a seven-device maximum connection capacity and the requirement that the device identify the beacon prior to transmission, which causes a ten-second message delivery delay.
Wi-Fi uses the current network infrastructure to send messages, making it a strong substitute for proximity marketing. The study suggests a concept dubbed Proximity Marketing as a Service (PMaaS), which delivers personalized communications to subscribers based on their position using GPS data and Wi-Fi network information. Compared to Bluetooth, Wi-Fi is more widely used and provides faster connection and more coverage. In comparison to Bluetooth alternatives, the Precinct PMaaS system performed better in the tests, handling more devices at once and delivering messages on average faster.
Although it is not as popular as Bluetooth and Wi-Fi, Radio Frequency Identification (RFID) is another technology used in proximity marketing. It is possible to strategically arrange RFID tags such that an RFID reader will identify them and send out a marketing message. In contrast to Wi-Fi and Bluetooth, RFID has a shorter range but is more accurate and can function without an app.
For the Precinct PMaaS system to work well, it incorporates a number of components:

- Data Storage: A database that holds contact preferences, user data, and message delivery history.
- Mobile Application: An Android application that functions as a messaging platform and lets users sign up and subscribe to notifications.
- Messaging Service: Sends messages to devices that have registered using Google Cloud Messaging (GCM).
- Web interfaces: Make it easier to create and manage broadcast messages and monitor message delivery results.
- Location Verification Engine: Ascertains the subscriber's whereabouts by utilizing GPS data and network names, guaranteeing that messages are only sent to customers who are in the right place.

Notwithstanding its benefits, the report notes a number of flaws and shortcomings in the application of network-based proximity marketing:

- Intrusiveness: Improper management of proximity marketing can make it invasive, which can result in complaints from customers about too many, pointless, or badly timed communications.
- Bluetooth Limitations: The delivery of messages may be delayed by the restricted connection capacity and initial device discovery required by Bluetooth-based solutions.
- Wi-Fi Dependency: The viability and dependability of Wi-Fi networks, which may not always be constant across several places, are prerequisites for the success of Wi-Fi-based proximity marketing.
- Privacy Issues: Location data collection and use can give rise to privacy concerns, which calls for tight compliance with privacy laws and the assurance of user consent and data protection.

In summary, even while network technologies like Bluetooth, Wi-Fi, and RFID present exciting new opportunities for proximity marketing, their deployment needs to be carefully considered in order to minimize any potential negative effects and optimize the positive ones. By utilizing the current Wi-Fi infrastructure, the Precinct PMaaS system offers a novel approach to proximity marketing by offering a more effective and scalable solution.

The article explores the use of Near Field Communication (NFC) technology in proximity marketing, highlighting the technology's rising acceptance and adaptability. NFC technology enables smooth data transfer between devices by enabling wireless communication over very short distances, usually a few centimeters. Users of this proximity-based interaction must put their devices close to one another in order for the procedure to be secure and intuitive, even in the absence of physical contact [32].
Mobile devices frequently include NFC technology built-in, which can be used for sharing information and making contactless payments, among other things. By only putting their cell phones close to a payment terminal, consumers using NFC-enabled smartphones may make payments, doing away with the need for traditional credit or debit cards. The appeal of NFC in retail settings, where it is used to give customers product details, special deals, and other pertinent information, has been attributed to its simplicity and convenience of use.
Compared to Bluetooth beacons, NFC technology provides a passive marketing solution in the context of proximity marketing. When a device is in close proximity to an NFC tag or terminal, the user must actively engage with NFC, in contrast to beacons that can send warnings to devices within a specific range. By giving the user a clear indicator of when data transmission takes place, this interaction paradigm improves their perception of security and control over their personal data.
The Slovak Republic confronts a number of obstacles in its adoption of NFC technology for proximity marketing, notwithstanding its benefits. Even while smartphones—the major devices used for executing proximity marketing—are owned by more than half of Slovaks, the real application of NFC technology is still quite low. Research shows that while a sizable segment of the population either does not own NFC-capable smartphones or has phones with NFC capabilities but does not use the function, just a small number of customers use NFC features for mobile payments or other applications.
The study reveals a void in the market where Slovakian companies and marketing firms have not completely adopted proximity marketing technologies, such as NFC technology. A lack of awareness of the technology's advantages and an emphasis on conventional marketing techniques are contributing factors to this lack of acceptance. Instead of investigating cutting-edge techniques like NFC, a large number of business owners and marketing experts in Slovakia are more focused on keeping an eye on the competition and preserving their current market presence.

The study also shows that NFC technology is affordable and simple to integrate, making it useful for small and large retail chains alike. Its allure is further enhanced by the fact that it requires no maintenance because the passive RFID chips do not need a power source. Raising awareness and showcasing the real advantages of NFC technology, however, will still be necessary to encourage broad market adoption in the Slovak industry.
Therefore, even though NFC technology has a lot of potential to improve proximity marketing campaigns by giving customers personalized, timely, and relevant communication, its success in markets like Slovakia will depend on raising consumer awareness, educating consumers, and encouraging a move toward adopting cutting-edge marketing tools.

The application of proximity marketing utilizing Bluetooth Low Energy (BLE) in a retail setting is examined in the study **"Implementation of Proximity Marketing Leveraging Bluetooth Low Energy"** by *Ruchika Muddinagiri*, *Vivek Jadhav, Shubham Ambavane*, and *Prof. Santosh Tamboli* [98]. A practice called proximity marketing includes putting helpful information in front of potential customers at particular places. The BLE method is selected due to its user-friendliness, robust hardware, and energy efficiency. With the goal of automating the shopping process and saving consumers time, the built system includes an indoor positioning system, a recommendation engine, and Web APIs to handle web queries.
A marketing tactic known as proximity marketing targets consumers in particular regions by utilizing a variety of wireless technologies. BLE is unique among the technologies available because it is compatible with the majority of contemporary smartphones and is energy-efficient. Among the techniques employed are Java applications developed for mobile devices using Android Studio and taking advantage of smartphones that support Bluetooth 4.0 or higher. ASP.NET and C were used in website creation for administration to produce a website that lets store administrators handle inventory, deals, and consumer purchases. For centralized data storage that was accessible from the website and mobile application, SQL Server was used.
Among the discoveries is an indoor navigation system that shows information unique to each aisle and guides customers throughout the store using BLE beacons. Information about available products and promotions could be extracted thanks to the mobile application's ability to recognize beacons. To give tailored recommendations, a recommendation engine used collaborative filtering based on past purchases made by the user.
The conclusion emphasizes the many benefits of using proximity marketing with BLE in a retail setting, including lower expenses for marketing personnel, enhanced consumer satisfaction, and effective process automation. This strategy shows how automation and the Internet of Things can benefit the retail industry.
On the other hand, a number of possible shortcomings and weak points are apparent. Although BLE works well for close proximity communication, its restricted range might be an issue in bigger retail settings. It may be necessary to use a large number of beacons to ensure constant signal coverage throughout the store, which could raise expenses and complicate matters. Despite BLE's reputation for low energy usage, batteries are still needed for the beacons, and these will ultimately need to be changed. These beacons could provide a logistical difficulty to maintain and operate, particularly in larger establishments.
Customers' cellphones with Bluetooth 4.0 or higher and their continued Bluetooth enabled are prerequisites for the system's efficiency. The system might not be useful to users of older devices or to people who would rather not enable Bluetooth. Privacy problems are raised by the collection and use of client data for customized suggestions. Maintaining trust and adhering to standards such as GDPR necessitates ensuring the security and ethical utilization of client data.
It can be theoretically challenging to integrate different technologies like recommendation engines, BLE, and indoor positioning. This intricacy could result in difficulties with implementation and increased development and maintenance expenses. Customers' desire to download and use the

retail store's mobile application is a key component of the system's success. Low adoption rates could reduce the marketing's efficacy.
Multiple factors, including device sensitivity variations and physical impediments that attenuate signal strength, might impact Bluetooth signals. These problems may result in inaccurate beacon detection and indoor positioning system results. Developing the mobile application, installing beacons, and configuring the server architecture could all demand a sizable upfront cost, particularly for small and medium-sized businesses.
Although the system is theoretically scalable, rapid growth may present infrastructure and data management problems, particularly as the volume of consumers and transactions rises. Training may be necessary for customers and retail employees to properly comprehend and operate the system. It could take a lot of resources to troubleshoot and provide continuing assistance.
To ensure the system's performance and customer happiness, addressing these flaws and weak points will require careful planning, investment in a strong infrastructure, and an emphasis on the user experience.

The paper by *Aaron Shapiro* and *Gabriel Nicholas* explores in detail Bluetooth Low Energy (BLE) beacons' history in the context of proximity marketing [102]. At the outset, BLE beacons were hailed as a revolutionary tool that would transform targeted advertising by improving the accuracy of online and offline marketing campaigns. Despite significant investments from VC firms, tech giants, and startups, BLE beacons were soon phased out because of a number of important issues. Scalability was one of the main problems. Reaching a critical mass of beacons and related devices turned out to be an expensive and logistically challenging task. Widespread adoption was hampered by the high expenses of setting up and maintaining a big network of beacons. In an attempt to bring their beacon networks up to a practical size, companies encountered substantial operational and financial challenges. The requirement for ongoing upgrades and maintenance added to the operating load and made the scalability problem worse.
Furthermore, the competitive environment between tech giants and mobile operating systems restricted the uniqueness of beacon-collected data. Because of the competition, it was challenging for businesses to successfully commercialize the technology because the data was neither proprietary nor unique. The data's total worth was diminished by the ease with which competitors could access or duplicate the information gathered by one company's beacons due to the absence of exclusivity. This problem was made worse by the fact that several IT behemoths were fighting for dominance over mobile operating systems and the data they produced.
Visibility posed a serious additional difficulty. Mobile operating systems changed their privacy policies, which decreased beacons' visibility and usefulness for marketers. The effectiveness of beacons in proximity marketing was further reduced by these policy changes, which made it more difficult for them to operate as planned. Stricter privacy protections on mobile operating systems drastically limited beacons' capacity to monitor and communicate with devices. Because beacons could no longer give the kind of detailed data that marketers had hoped for, their perceived value decreased as a result of this decrease in visibility.
Though BLE beacons have not been successful in the commercial marketing space, they have been revived in other domains. The authors draw attention to their application in surveillance systems, including contact tracing during the COVID-19 pandemic and tracking college students. These uses show that even while BLE beacons may not have achieved their intended marketing goals, they are nonetheless helpful in situations where institutional power can require their use. This change in use highlights how flexible BLE beacons are and how useful they are in certain situations. BLE beacons can still be very useful in situations where using them is expressly required, like in institutional surveillance or public health campaigns.
The study comes to the conclusion that the intrinsic conflicts between platform and infrastructure are the reason why BLE beacons were never able to take off as a proximity marketing infrastructure.

But their legacy lives on in a variety of monitoring and public health applications, demonstrating their flexibility and ongoing use in certain situations. This paper highlights the intricate interactions between technology, market dynamics, and regulatory settings, offering insightful information about the possibilities and constraints of BLE beacons. The authors contend that although the original excitement surrounding BLE beacons in the marketing industry may not have materialized, the technology is still developing and finding new uses in a variety of fields.

The study [87] presents a novel theoretical model to forecast how consumers will respond to marketing that uses omnipresent technology. The model attempts to provide a strong foundation for comprehending how consumers react to technology like RFID tags and smart gadgets in marketing contexts by incorporating components like consumer innovativeness, emotions, privacy and security concerns, and connective proximity.
Pervasive technology integration in marketing has demonstrated promise to improve consumer experiences and collect useful data. But it also brings up worries about invasions of privacy and unfavorable customer feedback. These issues have not been sufficiently addressed by earlier models, hence a new framework has to be created.
To test a variety of factors related to customer reactions, the researchers developed an extensive questionnaire. There were 71 items in the poll, most of which had a Likert scale with seven points. Furthermore, a few questionnaires assessed customers' prior technological experiences using an ordinal scale. Consumer emotions, including joy, delight, pleasure, fear, unease, and worry, were measured using six binary measures. These were combined into a single, six-point scale to indicate the valence of each feeling.
A measuring model was created by the researchers to verify the constructions and their connections. Confirmatory factor analysis was used in this to make sure the scales were valid and reliable. The structural model was assessed using a two-stage process in this study. To evaluate the invariance of the structural routes, a multiple-group SEM analysis was carried out among five distinct sets of groups (gender, age, education level, marital status, and country of origin).
The way that consumers react to pervasive technology is greatly influenced by their expectations regarding privacy and security. When these expectations are satisfied, customer feedback is more favorable. Customer responses are positively impacted by customer innovativeness, or the willingness to accept new technologies. Positive feelings are also very important in determining how consumers feel about all-pervasive technology. Consumers respond more favorably the closer they feel to the technology. If consumers are at ease with the type and quantity of information offered, they are more likely to respond favorably. As users grow more accustomed to the technology, frequent use can result in more positive sentiments. Customers' sentiments are greatly influenced by their sense of control over technology and the data it gathers.
The study effectively presents a novel model for forecasting customer responses to marketing-related omnipresent technology. The model offers a thorough foundation for comprehending customer behavior in this situation by taking into account elements like emotions, connective proximity, consumer inventiveness, and expectations for privacy and security.
When omnipresent technology is employed in marketing, the perceived metaphysical distance between the customer and the company is known as "Connective Proximity." Perceived intimacy, information openness, exposure duration, and appropriation are some of its dimensions. Positive customer reactions are correlated with higher degrees of perceived intimacy and openness. If a customer experiences a sense of overwhelm or if privacy issues are not sufficiently handled, extended exposure may occasionally result in unfavorable reactions.
Case studies like Club Tigre in Argentina show the possibility for improved customer experiences. There, spectators were given the option to receive subcutaneous RFID chips for fast stadium entrance. Tesco demonstrated the data-gathering powers of ubiquitous technology by using RFID scanners in its UK stores to send targeted advertising messages based on consumers' whereabouts

and purchase histories. Wearing RFID bracelets for interactive features and event admission during the Osheaga Festival in Canada demonstrated how technology can improve visitors' experiences at events.
In conclusion, the study offers a strong and thorough model for comprehending how customers respond to ubiquitous technology in marketing. Through the consideration of important variables including customer inventiveness, emotions, privacy and security requirements, and connective closeness, the model provides insightful information for marketers who wish to effectively use ubiquitous technology.

Conversely, the researchers in [77] examine how proximity marketing and Bluetooth beacon technologies are utilized to boost consumer interaction and create stronger relationships with customers. The writers discuss the advantages of proximity marketing, such as its ability to deliver personalized and relevant material to consumers according to their location and interests. In addition, they consider Bluetooth beacons to be a proximity marketing tool and a way to get more data on the tastes and actions of their clientele. The authors provide examples of successful proximity marketing techniques and discuss potential roadblocks, including concerns about privacy and the necessity of explicit opt-in and opt-out processes. As a result, the paper offers useful information about leveraging proximity marketing and Bluetooth beacon technologies to boost customer interaction and create stronger relationships with customers. In [102], the writers also look at the history and evolution of Bluetooth proximity marketing, including its early stages, eventual collapse, and eventual resurgence. The advantages of Bluetooth proximity marketing are discussed, including how it may provide relevant information to customers based on their location and activity.
Other studies discuss how advancements in technology have facilitated the ongoing collection of real-time location data by mobile devices. Thus, location-based data has had a major impact on the evolution of modern proximity marketing, which considers "closeness" and leverages it to achieve marketing objectives. The interplay between mobile devices and proximity technology allows marketers to identify and track specific client locations as they enter or leave predefined virtual limitations [10]. As the writers address these concepts in [25,76,96], this enables the launch of pre-planned marketing campaigns and the delivery of the appropriate information to clients at the appropriate time and location. There is concern, too, that these tactics can discourage potential customers from pursuing their original consumption objectives. Researchers and business professionals are becoming increasingly interested in geographic location-based interactive proximity marketing because of the increased security concerns, which we will address in more detail in the following section.

3.3 Trust

3.3.1 State of Privacy Concerns in Proximity Marketing

Proximity marketing's effects are covered in the paper "**The Impact of Proximity Marketing on Consumer Reaction and Firm Performance**", with special attention to how these effects relate to wireless and geolocation technologies like Bluetooth and RFID [20].
Using technologies like RFID, Bluetooth, GPS, and Wi-Fi, proximity marketing includes delivering advertising information to customers based on their geographic location. By using this strategy, businesses can focus on particular regions where they have the potential to attract clients, increasing the efficacy and relevancy of their marketing campaigns.
Some people may find proximity marketing devices to be invasive. The geolocation and real-time tracking features cause serious privacy concerns for users. The literature emphasizes how important it is for businesses to take privacy into account when implementing proximity marketing

methods.
It is critical to have confidence in the way personal data is handled. Research indicates that addressing privacy concerns requires an understanding of consumer values. If consumers believe their data is being utilized properly and with their agreement, they are more likely to embrace proximity marketing.
Businesses are required to abide by data protection laws, which set down guidelines for the collection, storage, and use of consumer data. These rules are intended to safeguard customer privacy and guarantee the secure and transparent handling of personal data.
RFID: Studies have shown that one major concern with RFID technology is privacy. Customers are leery of how their information is being collected and utilized without their express permission.
Bluetooth and NFC: These technologies raise issues regarding tracking and illegal data access even if they also provide advantages like better customer involvement and tailored offers.
Customer Response: Consumer response is crucial to the effectiveness of proximity marketing. A favorable reaction from customers can boost sales, improve brand perception, and increase loyalty. However, unfavorable responses brought on by privacy infractions can damage the company's brand and erode customer confidence. Technology Adoption: Businesses must weigh the benefits of proximity marketing against the possible privacy concerns related to consumer data. Adoption success depends on clear communication about data protection measures and guaranteeing legal compliance.

The paper emphasizes how proximity marketing is a two-edged sword: while technology breakthroughs have tremendous marketing potential, they also present major data privacy issues. Leveraging proximity marketing's full potential without sacrificing data protection requires addressing privacy issues and fostering consumer confidence. This synopsis highlights the significance of data security in proximity marketing, stressing that customer confidence and legal compliance are essential to its effective execution.
On the other hand, the impact of perceived privacy issues and the intrusiveness of proximity-based SMS marketing messages on consumers' inclination to visit an outlet is examined in the study by *Perera and Wijetunga* [110]. It also looks at whether younger and older consumers have different concerns. The results show that older customers are far more likely to perceive privacy concerns and intrusiveness, which has a negative effect on their inclination to visit an establishment. The only factor influencing younger consumers' intentions is perceived intrusiveness.
Regression analysis was used to examine data from a cross-sectional survey of 208 Sri Lankan customers for the study. The study comes to the conclusion that, although this impact varies by consumer age, consumers' desire to visit an outlet in response to proximity-based SMS marketing is highly impacted by perceived privacy and intrusiveness concerns. These results have significant ramifications for marketing plans aimed at various age groups.
The study, however, has a number of shortcomings. The 208-person sample size could not be sufficient to extrapolate the results to a larger population, and the findings' applicability to other cultural or geographic contexts might be restricted due to the study's concentration on Sri Lankan consumers. It is not possible to examine changes over time or causal linkages with the cross-sectional design. The study's internal consistency of the measure for attitudes about proximity-based SMS marketing was problematic, despite the fact that it makes use of known scales to measure variables.
Furthermore, the study does not account for other potential elements that can affect the propensity to visit an outlet, nor does it thoroughly investigate the causes of the perceived intrusiveness and privacy concerns. It is possible that the theoretical framework, which is based on the Theory of Reasoned Action, underestimates the intricacy of how customers react to mobile marketing. Although the study does not offer particular tactics for easing older consumers' concerns about privacy and intrusiveness, its implications for marketers are predicated on the idea that younger

consumers are less worried with these issues.
Larger and more varied sample sizes, longitudinal investigations, and a closer look at the underlying causes of perceived intrusiveness and privacy concerns should all be used in future research to mitigate these shortcomings. More theoretical frameworks and control variables may help to create a more sophisticated picture of how consumers react to proximity-based SMS marketing.

The use of geo-fencing and geo-conquesting strategies, which necessitate exact location tracking of customers, is a component of proximity marketing. These strategies are seen to be extremely complex and possibly invasive, which could cause a backlash from customers who feel vulnerable and that their privacy is being violated as the researchers shown in [91].
As consumers become more conscious of the value of their personal data, they also voice worries about privacy infringement, the possibility of fraud, and the general "creepiness" of marketers using their data. Studies show that consumers are becoming less inclined to divulge personal information, which could result in a large drop in the amount of data that is voluntarily shared.
The essay addresses businesses' moral duty to safeguard customer privacy, highlighting how frequently organizations mishandle data or increase privacy dangers by utilizing new technologies. Nonetheless, a few businesses are utilizing data privacy as a means of strategic differentiation, pledging to employ technology in an ethical manner and to bolster privacy safeguards.
Numerous techniques, including cookies, GPS monitoring, and loyalty cards, are emphasized for obtaining customer information. The environment of consumer data collecting and usage has become more complex as a result of the evolution of these techniques from conventional, face-to-face contacts to technologically assisted procedures.
According to the report, privacy concerns can reduce unfavorable customer behaviors like spreading false information or bad word of mouth. Establishing trust is essential for encouraging the sharing of information and the development of relationships. For marketers, lowering privacy concerns and building trust are critical tactics.
The investigation suggests that firms may use more subversive data collection techniques in the future as a result of restricted access to voluntarily supplied consumer data. This change emphasizes how important it is for proximity marketers to manage their data responsibly and adhere to moral principles.
In conclusion, the study emphasizes how crucial it is to strike a balance between effective data protection procedures and complex marketing strategies. In order to reduce the hazards related to proximity marketing, it is necessary to take ethical considerations, comply with regulations, and implement techniques that improve customer trust and privacy.

The obstacles and privacy problems related to proximity marketing in the Vehicle-to-Everything (V2X) space are covered in the study "**Efficient and Privacy-Preserving Ad Conversion for V2X-Assisted Proximity Marketing**" [78]. Sensitive information sharing—where roadside vendors advertise to passing cars or travelers—is one of the primary privacy concerns brought up. Merchants typically provide sensitive transaction records, including customer information like email addresses, names, and mailing addresses, to ad networks in order to calculate ad conversion rates. If these records are not sufficiently protected, this poses serious privacy issues.
The study suggests utilizing a privacy-preserving technique based on Private Set Intersection (PSI) to address these privacy challenges. Without disclosing any more sensitive information, PSI enables ad networks and merchants to calculate the intersection of their datasets (consumers who got ads and customers who made transactions). Present PSI procedures, however, might permit parties to stray from the rules, which could result in privacy violations. It takes a lot of computing power to ensure that just the intersection cardinality is revealed, and current approaches that use input certification can be unfeasible because of their substantial computational overhead, particularly when dealing with big datasets.

In order to improve security, the study presents a unique PSI-based protocol that combines zero-knowledge proofs with homomorphic encryption. The protocol ensures input privacy, unlinkability, unforgeability, and output verifiability and is built to function well even in the face of hostile opponents. This means that even in the event that one of the parties tries to deceive, the protocol can safely calculate the ad conversion rate without disclosing any private client information.
In addition to addressing privacy issues, the suggested method seeks to be computationally efficient, making it suitable for implementation in actual settings. Security research shows that, in comparison to other methods, the protocol is more robust under common cryptographic assumptions and offers a higher assurance of privacy. The significance of safeguarding consumer privacy in proximity marketing with V2X assistance is emphasized in the article. By utilizing cutting-edge cryptographic techniques, the suggested protocol fills a major vacuum in the V2X domain's present proximity marketing tactics by providing a safe and effective way to compute ad conversion rates without jeopardizing sensitive data.

We must handle the psychological concerns of the client in addition to the technical problems relating to privacy concerns. *Manfred Krafft, Christine M. Arden, and Peter C. Verhoef*'s article **"Permission Marketing and Privacy Concerns — Why Do Customers (Not) Grant Permissions?"** was published in the Journal of Interactive Marketing in 2017 and examines the variables that affect consumers' choices to allow or deny businesses to contact them via personalized communications [61]. The authors distinguish between benefit-related and cost-related aspects in their conceptual framework, which they use to investigate the impact of different drivers on consumers' decisions to grant permission.
Perceived personal relevance, entertainment value, consumer control over information, financial incentives, and lottery participation are examples of benefit-related characteristics. These elements are seen to be possible inducements for customers to give consent. Conversely, cost-related variables include the registration procedure, privacy issues, and perceived intrusiveness, all of which may discourage customers from giving consent.
The results of the study show that, aside from financial incentives and lottery participation, the majority of the factors that were found to have a substantial impact on consumers' readiness to grant consent. Permission is highly unlikely to be granted when privacy concerns are present. Two benefit-related elements, however, can lessen this negative effect: message content that has entertainment value or that the customer can relate to personally.
The significance of permission marketing for businesses is emphasized in the article because of its reciprocal advantages and legal compliance. It draws attention to the difficulty presented by privacy issues and makes recommendations for ways to improve interactive marketing efforts by taking customer motivations into account. The study sheds light on the variables that encourage or discourage customers to consent to interactive marketing campaigns, highlighting the need to strike a balance between the advantages and disadvantages of disclosing personal information.
Although not stated clearly, the document suggests a number of possible issues related to permission marketing and privacy concerns. Permission marketing initiatives may be less successful if consumers are reluctant to grant permissions due to their growing concerns about privacy and data security. Customers may be discouraged from giving consent if they believe the registration process is excessively complicated or time-consuming, or if it is too difficult to complete. Customers may react negatively or decline to provide authorization if they believe that tailored communications are bothersome or disruptive. The results of the study indicate that the chance of providing permission was not significantly impacted by lottery participation or monetary incentives, indicating that other benefit-related considerations may be more successful in determining permission. It can be difficult for businesses to adopt permission marketing tactics that are both successful and compliant with the ever-complex web of data protection laws and regulations. Permission marketing effectiveness depends on establishing and preserving consumer trust, but this can be challenging,

particularly in light of data breaches and abuse of personal information. When weighed against the costs (time, effort, privacy hazards) of targeted communications, consumers may choose not to consent if the advantages outweigh the costs. Constantly asking consumers for permission to receive communications can wear them out and make them less eager to give consent. Although personalization has advantages, it can also be difficult to divide and tailor communications in a way that does not come off as obtrusive. In order to guarantee continuous consent and engagement, permission marketing necessitates continual client relationship management, which can be resource-intensive.
These difficulties imply that, although permission marketing can be a successful tactic, its implementation calls for cautious oversight and careful consideration of the privacy and preferences of the consumer.

The present application of proximity marketing (PM) is examined from an experiential standpoint in the essay **"Proximity Marketing as a Facilitator of an Enhanced Service Experience"** by *Nataly Levesque, Harold Boeck, and Marc-Antoine Vachon* [73]. In order to determine which experiential characteristics are most and least employed in the context of this new marketing strategy, the authors examined 16 cases from the entertainment sector. Of the five experiencing dimensions (SENS, FEEL, THINK, ACT, RELATE), only the SENS and RELATE aspects are frequently asked, despite the fact that PM enhances the total experience.
Through the use of one of the newest marketing technologies, the research seeks to maximize the entertainment industry experience. The writers offer management recommendations aimed at enhancing the customer experience. They emphasize the significance of constant electronic connectivity and smartphone reliance, which make it possible for customers and enterprises to interact more easily through technology.
Using technologies like wireless devices, GPS, radio frequencies, Wi-Fi, Bluetooth Low Energy, and Near Field Communication, PM is described as the wireless and localized dissemination of advertising content relevant to a particular area. The foundation of this research is the idea that PM gives customers hyperconnectivity by offering them a fully immersive sensory and technical experience.
A deeper comprehension of the encountered circumstance and a clearer grasp of the related and enhanced service experience are made possible by the case study-based methodology employed for case analysis. The selection of cases was based on an analysis of how the entertainment business has changed since the introduction of mobile technology.
According to the findings, of the 16 examples that were examined, two had four dimensions, one had three, five had two, and eight had just one. THINK was the least used dimension, FEEL and ACT were less used, while SENS and RELATE were the most used. Analysis of the various combinations of dimensions showed that when two dimensions were present, they were always SENS and RELATE.
In summary, by comprehending the several applications of PM that are already in use and providing an answer to the research question of how PM enhances the customer experience, the study advances the field of research. The management implications indicate that in order to provide a comprehensive experience, elicit pleasant emotions, and concentrate on the RELATE dimension by enabling users to instantly post their status updates on social media, practitioners should incorporate as many experiential aspects as they can.
The study has certain limitations, such as the fact that all of the instances it examined solely involved the entertainment sector and that the cases' examination of customer emotions (the FEEL dimension) was not always evident. Future research possibilities include expanding the study to other industries and examining the impact of PM on consumer commitment to the brand.
The Transat Chair in Tourism at the École des sciences de la gestion de l'Université du Québec à Montréal (ESG-UQAM), the Fonds de recherche du Québec - Société et culture, and the Social

Sciences and Humanities Research Council of Canada all provided funding for the study.

Another study explores how people's perceived value of sharing information and their level of personal inventiveness relate to one another, and how this affects people's privacy concerns when utilizing proximity Bluetooth-beacon technology (PBBT). It also looks at how self-control functions as a moderator in these connections. The results imply that those with fewer privacy concerns are typically more inventive and value sharing their information more. Higher degrees of self-control exhibit a more noticeable effect, suggesting that self-regulation can lessen privacy concerns [76]. The second study examines how digital technologies affect privacy and marketing simultaneously. It demonstrates how the development of digital technologies has greatly improved marketing capabilities, opening the door to more specialized and focused marketing approaches. But these developments have also made people more concerned about their privacy. The study highlights the significance of consumer privacy-protective activities as well as the necessity of legislative actions to preserve consumer privacy. It implies that customers are growing more vigilant about protecting their privacy, which affects businesses' data policies and advertising tactics [117]. And there is a study, which focuses on proximity marketing for merchants, examines the fine line that needs to be drawn between protecting privacy and offering helpful information. It highlights how vital it is for consumers to have opt-in systems for location tracking in order to preserve their trust. According to the study, proximity marketing can provide customers with useful, tailored information, but it needs to be handled properly to prevent privacy invasion. The takeaway is that preserving customer trust necessitates striking a careful balance between providing useful information and protecting privacy. Achieving this balance requires opt-in techniques since they provide users authority over their data and permission for location tracking [4, 75].

3.3.2 Consent in Proximity Marketing

"The Mediating Role of consent in Business Marketing" by *Stefanos Mouzas* and *David Ford* is among the most comprehensive examinations of consent in the proximity marketing field [97]. It examines how consent between businesses influences business marketing strategies, with a particular focus on interactions between German manufacturers and retailers. Here, consent is seen to be an understanding between business parties that is necessary to create binding legal agreements and direct marketing campaigns. It affects a number of things, including trade agreements, the creation of new products, and the introduction of new markets or distribution routes. According to the study, permission mediates business contacts at four different levels: Consent functions as a stratifying process that first arranges and shapes the actions and reactions of business players throughout time. Second, consent is viewed as a recurring, changing process where judgments are made based on past consents since it is a recursive practice. Third, consent encourages continuing conversations and teamwork toward mutual gain because it is a stimulating engagement. Finally, by assisting in the reallocation of resources to more fruitful endeavors, consent contributes to the economy of activities, resources, and actors while also improving profitability and efficiency. The authors suggest that instead of seeing company marketing as a set of personal decisions, we should see it as an evolving, relational practice that is mediated by permission. The interdependencies between participants in intricate business networks are highlighted by this viewpoint. The study's empirical data comes from exchanges between well-known German grocery merchants (such *Lidl, Aldi, Wal-Mart, Metro, Rewe*, and *Nestlé*) and manufacturers (including *Mars, Kellogg, Nestlé*, and *Unilever*). It looks into how these entities' consent influences their marketing plans and corporate choices. The study casts doubt on conventional wisdom on autonomous decision-making by emphasizing the function that consent plays in mediating commercial dealings. Managerial Takeaways: To improve teamwork, optimize resource allocation, and expedite interactions, managers ought to concentrate on cultivating consent. An example of a case study would be *Sunways*

and *Primus*, wherein *Primus* committed to producing a mega-pack only for *Sunways* at a reduced cost, and *Sunways* committed to distributing *Primus*'s novel and inventive items at full price. An further instance involves *Sunways* and General Foods, wherein the latter created a proprietary brand for Sunways at a cost that was 60% less expensive than full-price brands. Research and development expenses were shared, and after five years, intellectual property rights were transferred. There are a few possible weaknesses in the study. Its emphasis on the relationships between particular German firms and shops may restrict the findings' applicability to other areas or sectors of the economy. The over-reliance on certain case studies, like *Primus* and *Sunways*, may not fully capture the range of consent dynamics and commercial relationships. Although the study adopts a relational and evolutionary viewpoint, it might not have a strong theoretical foundation that is applicable to all situations. Furthermore, the empirical data may not fully represent the experiences of smaller or less well-known companies because it is derived from well-known manufacturers and grocery shops. Potential bias in the data could also result from the unique business practices and market conditions in Germany. Without additional simplification, the study's conception of consent as a multi-level, dynamic process may be too complicated for real-world implementation. Additionally, the study only looked at the firms involved, ignoring the involvement of clients or customers. Finally, because the business world is changing, new business models and technological advancements may swiftly replace the findings and change how consent is obtained and used.

Daniel W. Woods and *Rainer Böhme*'s **"The Commodification of Consent"** is another study that looks at how online consent—a legal notion meant to uphold user rights—became a traded asset among companies [150]. The authors underline the ramifications for the protection of personal data and look at how this change affects how money is distributed across businesses. To examine the emergence of consent coalitions and their impact on corporate profits, they create an economic model. Online permission is frequently regarded as an essential formality that permits companies to gather and utilize consumers' personal information. The monetization of consent, however, begs the question of how companies may take advantage of and profit from this consent—often at the price of user privacy. The authors model the creation of consent coalitions and examine their effects on revenue distribution using economic theory and game theory. They also look at how these coalitions affect the privacy of personal data. The findings suggest that companies with significant consent deficits can benefit greatly from consent coalitions. Through bilateral agreements, companies who lead in consent can monopolize coalition fees. Though the inherent probability of inaccuracy in consent conversations is still present, there is a chance that consent coalitions will force users to give consent against their will. Consent has become a commodity, turning it from a legal notion meant to safeguard consumers into a financial resource. This change has important ramifications for how businesses divide revenue and how private personal information is kept. To protect user rights, the authors urge contemplation on methods to control and monitor the use of consent.

The study " **Ethical concerns about social media privacy policies: do users have the ability to comprehend their consent actions?**" by *Annmarie Hanlon* and *Karen Jones* [44] explores the complex world of social media privacy regulations and the vital problem of user consent understanding. It raises concerns about whether users actually understand the consequences of their permission acts and throws light on the moral conundrums raised by privacy policies. These policies' intricacy is examined closely, highlighting the difficulties users encounter in comprehending them. Highlighted as a fundamental component of social media marketing, informed consent draws attention to the moral implications of providing assent without sufficient knowledge. The study examines several consent forms and their far-reaching implications. The study distinguishes between different types of consent, each with unique functions and settings. A valid consent emphasizes legality and authorization by enabling people to conduct actions that would otherwise be prohibited.

Clear and willing data exchanges are ensured by informed consent, which entails voluntary understanding and open communication between competent parties. Consent procedures can be made simpler by using implicit consent, which is implicitly assumed from deeds or statements. To ensure continuous compliance and consent maintenance, continuous consent requires ongoing verification for every instance of data usage. In order to clearly indicate agreement, explicit consent requires active affirmation, usually accomplished via checkboxes or other comparable techniques. Strategically seeking permissions in line with social goals, engineered consent reflects deliberate strategy and execution. On the other hand, when people give their consent without fully understanding the information they are asked to consent to, it is known as uninformed consent. Misunderstandings or false representations cause consent to be given based on inaccurate information, which is known as misinformed consent. The aforementioned categories highlight the intricate and multifaceted nature of consent in relation to legal, ethical, and pragmatic contexts. In social media platforms where user data is monetized for advertising, consent is very important for marketing initiatives. Many jurisdictions have legal requirements pertaining to obtaining valid consent, which highlights the significance of users' awareness and authorization of data processing. The various consent forms—secured, uninformed, and sustained—highlight the disparities in user understanding and participation in the consent procedure. To respect users' autonomy in making decisions and maintain ethical standards, marketing tactics must ensure informed consent. Furthermore, the study delves into the evolving landscape of social media platforms' privacy policies, noting an increase in word counts and reading times over the years. Notably, Meta/Facebook's policy necessitates a reading age of 21-22, while Twitter's policy requires a reading age of 14-15. This underscores the pressing need for clearer, more user-friendly privacy policies to empower users to comprehend and consent to data processing effectively. In conclusion, the paper calls for a concerted effort towards enhancing transparency and user understanding in social media privacy policies to uphold ethical standards and ensure informed consent. The study also emphasizes how little is known about consent-related actions on social media, especially among younger users. It draws attention to the fact that social media companies' present privacy policies are frequently too complicated for users to understand, posing serious ethical questions. We address the ramifications for managers and legislators, arguing in favor of more standardized and easily accessible consent processes. In the end, the study promotes greater knowledge and understanding of the moral conundrums relating to data privacy in the context of social media.

Many studies that address consent in the context of markets have concentrated on the significance of **opt-in and opt-out mechanisms** in order to face the lack of awareness. Examples of these researches include [65, 144]. These studies identify consent gaps and emphasize the need to identify the most effective means of serving members' interests and safeguarding their personal information. A further study by *ERIC J. JOHNSON, STEVEN BELLMAN*, and *GERALD L. LOHSE*, titled **"Defaults, Framing, and Privacy: Why Opting In-Opting Out**," examines the distinctions between opt-in and opt-out responses in relation to online privacy policies and permission marketing [51]. The authors show that default selections have a major impact on users' preferences for future interactions with a website through two online studies. The independent and combined impacts of framing and defaults on preference construction are also investigated in this study. Whether or not customers should be able to opt out of data collecting and marketing programs is a common topic of discussion in relation to internet privacy and permission marketing. The United States typically has an opt-out policy, however, the European Union's Data Directive mandates an opt-in strategy. This study aims to experimentally examine how these two strategies affect consumer participation. They did 2 experiments:

- Experiment 1: A total of 277 participants were split into four groups at random and asked to be contacted if they would like to participate in any more online surveys. The default

options (opt-in vs. opt-out) and framing (positive vs. negative) were different across the formats.

- Experiment 2: Six question forms with a no-default option were employed in a similar setting with 235 participants. This allowed for a clearer assessment of preferences that was not influenced by default effects and controlled for attentional effects.

The study comes to the conclusion that consumer preferences are strongly influenced by the way questions are phrased (opt-in vs. opt-out). Defaults and framing have additive impacts that shape how preferences are formed. These results have consequences for customer behavior, website operations, and consumer consent laws in the public domain. The study sheds light on how customer behavior is influenced by default options and phrasing in online privacy rules and permission marketing. But there are a few issues with it that need to be taken into account. Because of the low demographic predictability of the study, the conclusions might not translate well to other user experiences or demographic groupings. Additionally, there is a chance that respondents did not pay attention, which could compromise the accuracy of the findings. The voluntary nature of the sample's involvement adds bias, and the regulated online setting could not accurately represent behavior in the actual world. The results' applicability to different situations where decisions are made is limited by their concentration on a specific domain—online surveys. Furthermore, the study questions whether the observed preferences represent real, thoughtful decisions because it admits that default effects may be the result of physical or cognitive laziness. The investigation of moderating variables such as education and experience was constrained, and the nuanced variations of framing may not fully reflect the spectrum of effects noted in previous research. Because there is no longitudinal data, the study is unable to investigate how preferences might evolve over time. Lastly, the study falls short in its discussion of the moral ramifications of influencing consumer decisions, especially in important settings, through the use of defaults and framing. Notwithstanding these shortcomings, the study emphasizes how crucial it is to take framing and defaults into account when creating online consent processes.

In this study [63], *V. Kumar, XI (ALAN) ZHANG, and ANITA LUO* examine how the relevancy and intensity of marketing communications affect consumers' decisions to opt-in or opt-out in a permission-based marketing context. The authors investigate the combined impact of email frequency, email open rates, and email click-through rates on customer opt-out probability using a multivariate copula model. According to the research, while receiving a lot of emails may increase opt-out rates, this effect may be offset by interesting and relevant content. Customers' decisions to opt-in and opt-out are also heavily influenced by their past behavior and attributes. With the emergence of interactive marketing, the emphasis has switched from one-way communication to two-way engagement, with a particular emphasis on the significance of comprehending client behaviors and preferences within the framework of permission-based marketing. The timing of opt-in and opt-out decisions, as well as the impact of transactional activity on customer retention in email marketing programs, have not been properly investigated in prior study. The study employs data from a U.S. retailer for data collection, which includes transaction histories, email open and click histories, customer opt-in and opt-out timings, and marketing initiatives. For study, a random sample of 9,180 customers who made their first transactions between February and July of 2007 was selected. In order to simultaneously describe opt-in time, opt-out time, and average transaction amount, the authors employ a multivariate copula model utilizing a pair-copula building approach. When compared to benchmark models, this method enhances opt-out time prediction performance and captures the interdependence between these variables. Their discoveries that opt-out likelihood is influenced in a U-shaped way by marketing intensity as indicated by email frequency. Higher open and click-through rates imply highly relevant emails, which greatly lower the chance of customers opting out. Opt-out decisions are also influenced by customer

attributes like product returns and the frequency of discount redemption. Beside Affluent Aficionados and Second Nature Surfers are two examples of customer subgroups that are less likely to opt out, indicating that they value the email program more than other groups do. Segment-specific factors influence program retention, underscoring the significance of customized marketing approaches. The research offers significant perspectives on the dynamics of consumer opt-in and opt-out choices in permission-based marketing. Businesses may increase consumer engagement and prolong email program participation by proactively controlling the frequency and relevancy of marketing communications. The results emphasize how crucial customized marketing campaigns are and how businesses must refrain from overmarketing in order to keep their clientele. There are various restrictions on the study. It focuses on a retail setting and is industry-specific, thus it might not apply to other sectors like the music industry. It looks mostly at the opt-in and opt-out behaviors of current consumers, possibly ignoring individuals who have never made a transaction before. The study's application to consumers with more complex patterns is limited by its focus on initial opt-in and opt-out selections. Due to the fact that many consumers opted out or did not opt-in before the observation period finished, bias may be introduced into right-censored data. Weibull hazard models and vine copula add complexity and presumptions that might require more research and analysis. Though it does not provide specific recommendations for the ideal marketing intensity, the study cautions against overmarketing. It focuses on empirical modeling rather than generalizing the association between opt-in and opt-out times. Finally, even though it provides information on how to allocate resources, it ignores the possibility that direct mail may have a cannibalization effect on email subscribers, indicating the need for improved marketing coordination.

The literature is replete with academic studies and research that address the role of consent marketing such as [17, 62, 111, 128]; as well as opt-in and opt-out systems in influencing consumer choice and safeguarding interests [18, 64, 126]. These studies demonstrate how important this subject is given the state of the market today. Consent-based marketing, for example, is quickly taking the lead in the industry as a result of growing legal mandates and customer demands for control over personal data and transparency. This strategy makes sure that marketing efforts are sent to people who have specifically consented to receive them, which increases user engagement while also fostering trust. Furthermore, the contrast between opt-in and opt-out systems is crucial for user empowerment and data protection. Users actively giving their consent is required for opt-in systems, which are viewed as more trustworthy and privacy-focused. Opt-out systems, on the other hand, provide convenience and better participation rates but may give rise to worries about unauthorized data use. In these mechanisms, agreement is presumed until the user withdraws it. Each strategy has advantages and disadvantages, and the best option typically relies on the particular situation and target audience.
These processes have a big impact on the market, yet they still have some serious flaws. For instance, adopting opt-in procedures might occasionally be difficult for users, which lowers participation rates. On the other side, even while opt-out options are more practical if they are not handled properly, they may cause customer mistrust. Consequently, in order to strike a balance between consumer protection and successful marketing techniques, continued study and strategy improvement is crucial. Also, it is crucial to remember, that getting user consent is not sufficient to solve every issue facing the industry. The idea of the "consent burden" draws attention to how managing consent can place heavy costs on customers, such as the requirement that they comprehend intricate privacy regulations and make wise selections.1. This may result in dissatisfied customers and diminished efficacy of consent procedures. To further complicate matters, businesses may use consent processes to justify their intrusive data activities. Strong regulatory frameworks and industry best practices must be used in conjunction with consent procedures to fully protect consumers and promote a fair market environment. This entails unambiguous rules

for the use of data, frequent audits, and open dialogue with customers. By doing this, we can make sure that consent mechanisms accomplish their goals without burdening users excessively or jeopardizing their privacy.

3.3.3 Classification of Proximity Marketing

By combining many viewpoints into a single theoretical framework, *François Lenglet* and *Rémi Mencarelli*'s paper **"Proximity in Marketing: An Integrating Theoretical Framework and Research Agenda"** offers a detailed analysis of proximity marketing [71]. The term "proximity" refers to a state of being that is characterized by three factors: physical proximity (geographic proximity), emotional or psychological proximity (relational proximity), and shared identity or values (identity-based proximity). According to the study, there are various types of proximity that are pertinent to marketing, such as closeness based on shared values or culture, relational proximity resulting from emotional bonds with brands, and geographic proximity between customers and retailers.

Numerous academic fields, including economics, psychology, geography, and sociology, have contributed various perspectives to the understanding of the concept of proximity. Anthropology takes into account social distance and the use of space as extensions of the self, psychology looks at interpersonal interactions and emotional intimacy, while geography and economics concentrate on spatial features and ideal business sites. The study emphasizes how proximity is dynamic, how it can change over time, and how comprehending proximity dynamics requires an appreciation of both spatial and non-spatial viewpoints. In a variety of marketing scenarios, such as retail stores, industrial settings, and consumer behavior, proximity is used to affect how consumers perceive and assess brands and products. Comprehending proximity facilitates the development of marketing strategies that aim to boost consumer pleasure, build tailored and successful marketing campaigns, and cultivate loyalty. The study also suggests that more research be done to create a more comprehensive theoretical framework surrounding proximity. This research should look at how different forms of closeness interact with one another and affect consumer behavior, as well as how proximity affects different marketing situations.

But the report also features a number of flaws and omissions. The fragmentation of the body of knowledge on proximity that currently exists is a significant problem that makes developing a cohesive framework more difficult. This disarray may make it difficult to successfully integrate different points of view. Furthermore, the study's practical usefulness may be limited due to its heavy emphasis on theoretical synthesis. It may prove difficult for practitioners to apply these concepts in an effective manner in the absence of case studies or practical examples. The suggested framework is also not supported by any actual data, as the study mainly uses a narrative literature review. The accuracy and practical usefulness of the framework are still unknown in the absence of strong empirical validation.

The study makes an effort to address a variety of proximity-related variables, which may make the framework unduly complicated and wide. Due of its intricacy, it might be challenging to operationalize in particular marketing situations, which could limit its practical application. Although the study recognizes that proximity is dynamic, it does not offer specific management or adaptation solutions for these changes over time. Although the framework must be adaptive and flexible, the study does not provide any instructions on how to do so. The paper talks about the managerial implications of knowing closeness, but it does not give managers any specific, doable solutions. It would be more helpful to practitioners if it included more thorough examples and real-world applications.

While integrating viewpoints from many disciplines is a virtue, it also has drawbacks. It's possible that the study did not go far enough in discussing how these many viewpoints might be logically combined and used in real-world marketing tactics. Moreover, the study fails to sufficiently take

into account how technology shapes closeness. Further investigation is warranted about the impact of technology on geographic and relational proximity, given the growing significance of digital marketing and online interactions. Finally, possible biases in the literature or data sources employed are not addressed in this study. Identifying and reducing biases is essential to creating a framework that is more accurate and dependable.
In conclusion, the study integrates and synthesizes the concept of proximity in marketing in a significant way, but it still has to overcome a number of obstacles, including fragmentation of the literature, theoretical focus, lack of empirical validation, complexity, dynamic nature, practical applicability, interdisciplinary integration, disregard for technology, and potential biases. Future studies could improve the suggested framework's robustness and applicability by addressing these shortcomings, which would offer insightful information to practitioners and scholars alike.

In the paper **"New approach based on proximity/remoteness measurement for customer classification"**, a novel technique for categorizing clients according to how satisfied they are with insurance firms' services is presented [5]. Utilizing proximity/remoteness measures to enhance classification accuracy and gain a deeper understanding of client satisfaction is the main innovation. The study suggests a way to group clients according to how close or far they believe an insurance company's services to be. The goal of this strategy is to offer a more sophisticated comprehension of client pleasure. The paradigm takes into account a number of proximity-related characteristics, such as psychological, relational, and geographic aspects. This evaluates the degree to which clients are close to the service provider, enabling businesses to more successfully customize their marketing campaigns. The approach determines how close or distant consumers feel in connection to the service they receive by using service quality standards to evaluate customer perceptions and expectations. In terms of proximity marketing, this is vital. By adding closeness and remoteness metrics, the study seeks to enhance current categorization techniques, such as the Selectability/Rejectability Measures Approach. Using data from a survey of 384 consumers, a numerical example is given to show how the new classification method is applied. This illustrates how clients can be categorized using proximity metrics.
This evaluates the degree to which clients are close to the service provider, enabling businesses to more successfully customize their marketing campaigns. The approach determines how close or distant consumers feel in connection to the service they receive by using service quality standards to evaluate customer perceptions and expectations. In terms of proximity marketing, this is vital. By adding closeness and remoteness metrics, the study seeks to enhance current categorization techniques, such as the Selectability/Rejectability Measures Approach. Using data from a survey of 384 consumers, a numerical example is given to show how the new classification method is applied. This illustrates how clients can be categorized using proximity metrics.
The study's conclusions might not be as broadly applicable as they could be given its dependence on a single poll with 384 completed questionnaires. The results may not apply to other businesses with differing customer satisfaction patterns due to the focus on insurance companies. Diverse consumer groups may have diverse interpretations of the same service quality requirements, which could present practical implementation issues. The study's suggested method is not thoroughly compared to other currently used classification techniques, which would have improved the study's ability to validate its efficacy. The accuracy of the customer classification results could be impacted by potential biases in the data gathering process, such as response biases or demographic imbalances, which are not taken into account. In conclusion, the study presents a thorough methodology for classifying clients according to proximity metrics, offering a more precise and perceptive strategy for proximity marketing. With the aid of this framework, businesses can better comprehend customer delight and customize their marketing initiatives to cultivate stronger client interactions.
The research explores how proximity marketing is classified by looking at different technology and communication channels in this study [9]. It classifies proximity marketing according to the

kind of technology—RFID, Bluetooth, Wi-Fi, and NFC—that is employed. The efficiency of each technology in reaching consumers with marketing messages is examined.
RFID technology helps businesses reach customers within a specified range with personalized messages, which is a major aspect of proximity marketing. When it comes to personalizing shopping experiences, this technology excels. The ability of Wi-Fi and Bluetooth-capable gadgets to disseminate promotional material to adjacent smartphones and tablets is emphasized. Because these technologies can reach a large number of people within a specific area, they are widely employed. The application of NFC technology in enabling smooth transactions and information sharing between devices and marketing systems is highlighted. This technology is essential for improving customer interactions' efficiency and convenience.
The impact of these technologies on customer behavior is also covered in the study. It examines the ways in which proximity marketing influences consumer choices and improves the shopping encounter. By looking at the substance of marketing messages, their applicability, and consumers' perceptions of their reliability, the classification is further improved.
A primary limitation of the research is its restricted empirical validation. There are questions regarding the practical relevance of the classifications in various situations and industries because they are mainly theoretical and have not undergone significant empirical testing. Another drawback of the study is its restricted focus on specific technology categories, which leaves out important customer perspectives. It places a strong emphasis on technology while leaving out important details on how users view and use these tools. A thorough classification requires an understanding of customer behavior, preferences, and acceptance.
The study's discussion of the integration of various technologies is insufficient. Proximity marketing frequently uses multiple technologies instead of just one in real-world applications. Investigating the possible integrations of various technologies could improve consumer experience and the efficacy of marketing. Ethical and privacy concerns are not taken into account in this classification. The collection and use of personal data for proximity marketing raises serious privacy concerns. The report makes no mention of how privacy issues may affect proximity marketing's efficacy or how businesses may allay these worries in order to gain customers' trust.
Lastly, a more dynamic and developing perspective might be beneficial to the study. Since proximity marketing techniques and technologies are always changing, the study's classification may become out of date very soon. It would be advantageous to have a more adaptable and flexible framework that takes into consideration both shifting customer behavior and continuous technical improvements.
The study offers a fundamental classification of proximity marketing technologies; however, in order to stay relevant in a field that is rapidly evolving, it could be strengthened by adding empirical validation, a consumer-centric approach, integration of multiple technologies, consideration of privacy concerns, and a dynamic perspective.

The study offers a fundamental classification of proximity marketing technologies; however, in order to stay relevant in a field that is rapidly evolving, it could be strengthened by adding empirical validation, a consumer-centric approach, integration of multiple technologies, consideration of privacy concerns, and a dynamic perspective. Several research have examined location-based proximity marketing and its interactive marketing perspective, such as the study by Loussaief et al. [80]. Furthermore, Angue et al. [11] looked into technical proximity in relation to R&D collaborations, emphasizing how crucial it is to gauge technological proximity in order to find possible partners. These studies highlight the necessity of a thorough methodology in proximity marketing research that takes into account both technology and consumer viewpoints.

One of the major obstacles in the field of proximity marketing is the absence of a well-defined and widely recognized classification scheme. Customers and businesses find it challenging to

successfully traverse the environment when there is a lack of a standardized framework since it leads to uncertainty and inconsistent practices. RFID, Wi-Fi, Bluetooth, NFC, and other technologies are all included in proximity marketing; each has special uses and capabilities. But without a precise categorization, it becomes difficult to draw lines and create guidelines that can direct how these technologies are used.

At the moment, proximity marketing is a little dispersed, with various studies and industry practices using different methods to classify and apply these technologies. For example, some studies concentrate mainly on the technology features, like the Bluetooth beacon's potential for user involvement or the RFID's range and data transmission capabilities [2, 3]. Others may place more emphasis on the customer experience, examining the ways in which these technologies affect consumers' pleasure and purchase decisions. Due to their inability to identify the best solutions for their unique needs and situations, organizations may experience confusion and inefficiency as a result of this lack of coherence [1].

Furthermore, a lack of defined guidelines and standards may affect the acceptability and trust of customers. The gathering and use of personal data is a common practice in proximity marketing, which presents serious ethical and privacy issues. In the absence of established protocols, companies might implement actions deemed as invasive or immoral, resulting in negative feedback from customers and regulatory examination. A framework for the ethical and open use of proximity marketing technology might be provided by clear regulations and classifications, which would assist reduce these hazards.

Integrating several technologies is another important problem. Proximity marketing frequently uses multiple technologies instead of just one in real-world applications. For instance, a retail establishment may combine NFC, Bluetooth, and Wi-Fi to offer a smooth and interesting buying experience. However, it might be difficult to comprehend how various technologies can be integrated and managed efficiently without a defined classification system. As a result, marketing initiatives may become dispersed and less effective, failing to fully realize the potential of proximity marketing.

The quick speed at which technology is developing also adds another level of intricacy. Since proximity marketing techniques and technologies are always changing, what is now seen to be best practice could soon become antiquated. To account for these developments and guarantee that companies can modify their strategies appropriately, a dynamic and adaptable classification system is required. This would help businesses remain competitive in a market that is changing quickly, in addition to increasing the effectiveness of proximity marketing.

In conclusion, there are a lot of issues where both firms and customers in proximity marketing are facing because there is not a defined classification system in place. A unified framework could help define boundaries and regulations that direct the responsible and efficient use of these technologies, offering much-needed clarity and uniformity. In the end, this would be advantageous for the whole ecosystem, encouraging innovation, boosting customer confidence, and producing better marketing results.

3.4 Agreement Mechanisms

3.4.1 Navigating Consensus Algorithm in Cryptocurrency

Consensus algorithms are the foundation of decentralized trust in the rapidly developing field of blockchain technology. The ability to reach consensus among dispersed members is essential to any blockchain network in order to maintain the shared ledger's integrity and immutability. We take a deep dive into the complex realm of blockchain consensus methods in this part. Consensus mechanisms have developed and varied, meeting a wide range of use cases and scalability needs, from the early days of Bitcoin to the complex ecology of modern blockchain platforms. We start

our investigation by looking at the fundamental ideas that underlie blockchain consensus. Here, we take a closer look at blockchain consensus and the most well-known algorithms that have influenced the development of decentralized systems. Each algorithm offers a different method for reaching consensus within the network, from the basic Proof of Work (PoW) algorithm—famously used by Bitcoin—to the cutting-edge variations like Proof of Stake (PoS), Proof of Burn (PoB), Proof of Importance (PoI), and Proof of Capacity (PoC). We aim to shed light on the changing landscape of blockchain consensus through this thorough examination, along with the consequences for decentralized systems and the forces that have shaped its evolution.

Proof of Work (PoW)

A white paper explaining the idea of the **Blockchain** was published in 2008 under the pseudonym *Satoshi Nakamoto*, which sparked a number of in-depth investigations in this field. Though not totally new, the concept was already published in 1991 in a paper on cryptographically secure blocks linked by chains by *Stuart Haber* and *W. Scott Stornetta* [101]. Traditional databases could no longer support the increasing number of nodes in different places that businesses needed to support, all of which required synchronized updates due to technological improvements. These requirements were met by blockchain, which offers a distributed database where collections of data are stored in **blocks**. To preserve data integrity, each block is connected to the one before it and has a finite amount of storage as presented in figure 3.2. The decentralized structure of blockchain, in which blocks are dispersed among several networks but maintain connectivity, is what gives it its power. In order to maintain security and coherence, the network uses a **consensus algorithm** to prevent data redundancy and illegal modifications [103]. Preventing several nodes from simultaneously broadcasting identical blocks at the same time poses a key challenge for blockchain technology since it may cause network overload and confusion. The more nodes that concur on a transaction, the more secure the network gets; Consensus on new blocks is essential. The **Proof of Work (PoW)** algorithm was created to stop repeating transactions and preserve ledger integrity. To get the nodes' agreement for a transaction to be executed, players in PoW must solve computational challenges. By making service requesters complete certain duties, *Cynthia Dwork* and *Moni Naor* developed a way to stop denial-of-service attacks and other network abuses. PoW, which was first introduced by *Markus Jakobsson* and *Ari Juels*, has subsequently grown to be a fundamental component of cryptocurrency security [38], [42]. Verifying nodes—which add and validate transactions—is key to the idea as shown in figure 3.3. Blocks are prepared by trusted nodes by adding required data, such as version, size, timestamp, Merkle root, and the hash of the previous block (Prev-Hash). By speculating on a secret value, they solve a mathematical puzzle (Nonce). Following that, a hash function (SHA-256) is applied to the block. The node broadcasts the solution for verification if the result satisfies the necessary degree of difficulty. The method adds the block to the chain if it is validated. Since its launch, PoW has gained widespread recognition in the cryptocurrency community and is used by well-known coins including *Bitcoin, Litecoin, Ethereum, Monero, and Dogecoin*.

Proof of Stake (PoS)

To address the high energy consumption associated with PoW, *Sunny King* and *Scott Nadal* introduced **Proof of Stake (PoS)** in 2012 [69]. The idea behind PoS is simple: nodes show their dedication by staking a piece of their cryptocurrency holdings. Unlike PoW, where all nodes compete at once, one node is then chosen to validate transactions. This selection procedure saves energy while preserving the fairness of the blockchain (figure 3.4).

Which node advances to the next validator is determined by a number of criteria, including randomization algorithms, coin-age-based selection, and stake size:

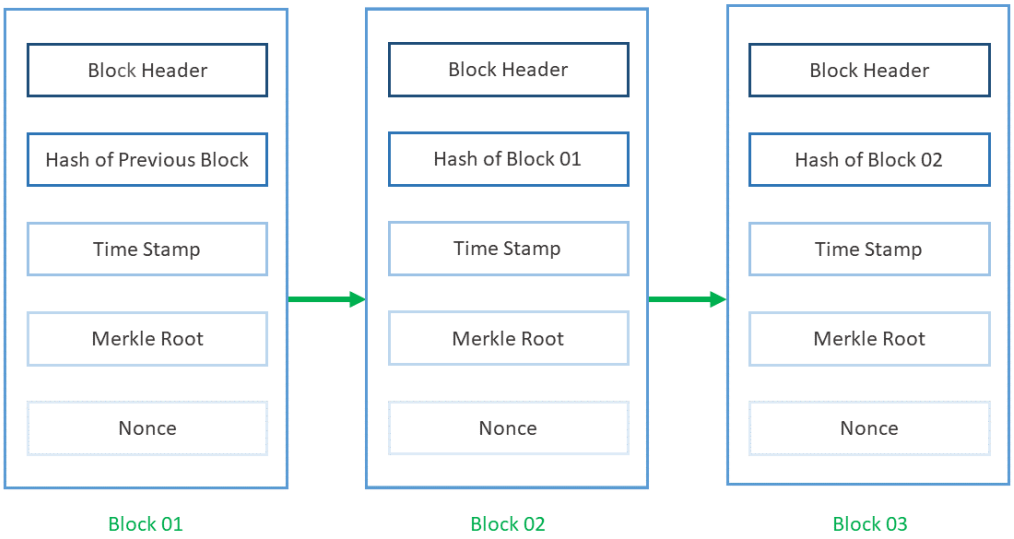


Figure 3.2: Blocks structure

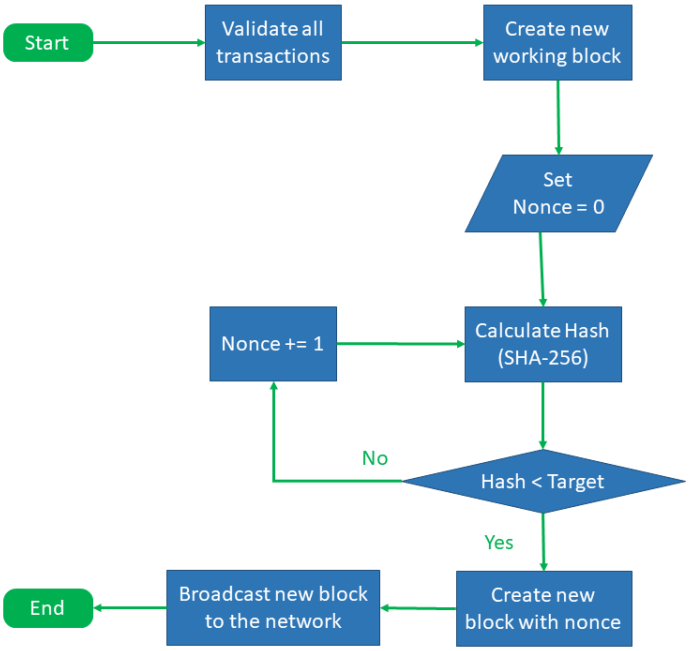


Figure 3.3: PoW scenario

- **Coinage-based selection:** A candidate for validation has a higher chance of being selected as the next validator if they wait a longer period of time.
- **Random Block selection:** A random process is used to determine the next validator, taking into account factors like "largest stake" and "lowest hash value."

Staking more cash than other nodes increases the likelihood of being chosen as the next validator. PoS gained popularity in the cryptocurrency space very quickly, and many cryptocurrencies adopted it. **Peercoin** was the first, and it's still in use today. For its research and development consensus, **Nxt** also uses PoS [24].

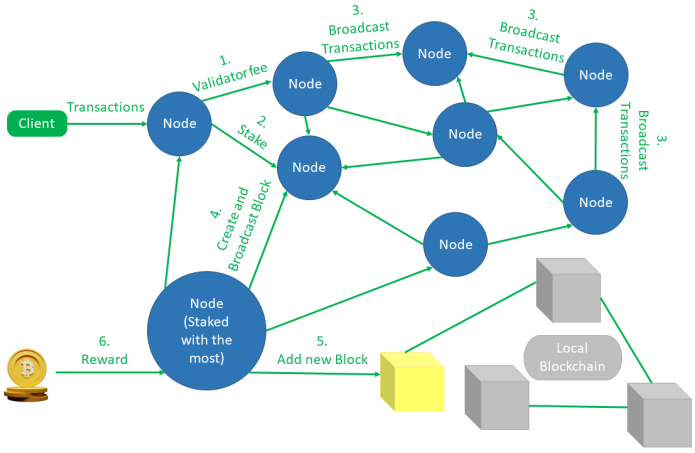


Figure 3.4: PoS scenario

Proof of Burn (PoB)

Due to their numerous shortcomings, PoW and PoS have been condemned by numerous Bitcoin researchers. *Iain Stewart* is one of these opponents, contending that "both proof of work and proof of stake utilize real resources that could be put to better use elsewhere.*Stewart* [54] developed the **Proof of Burn (PoB)** consensus technique in response in 2012. PoB was created to solve the problems with PoW's energy usage. Its main action is to show commitment by "burning" coins. By sending their coins to an unspendable address, participants are essentially taking them out of circulation. While using less energy than PoW, this action raises their chances of being chosen as the next validator. A miner candidate generates an unspendable address with a distinct tag as part of the procedure. By doing this, the candidate preserves network activity and adaptability while consuming a great deal less energy than PoW. A validator confirms that the coins have been burned and are irretrievably lost after receiving the transaction address from the candidate. The miner is rewarded if everything is in order (figure 3.5). Many cryptocurrency systems have implemented PoB, the most well-known is **Slimcoin**, a Peercoin-based cryptocurrency that uses PoB as its consensus method. **TGCoin (Third Generation Coin)** is another example, albeit it is no longer traded or maintained [119].

Proof of Importance (PoI)

NEM (New Economy Movement), a Singaporean group, chose to get involved in March 2015 after realizing the significance of cryptocurrency wallets. They developed the **Proof of Importance (PoI)** consensus mechanism, the Nano wallet, and a brand-new cryptocurrency known as **XEM**. The PoI approach derives its name from the way it assesses each member's importance

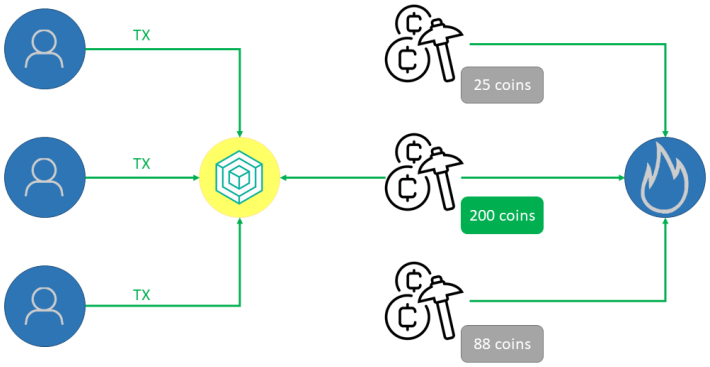


Figure 3.5: PoB scenario

within the blockchain network. A person's likelihood of being selected as the next miner can change based on their importance score, and they may even be kicked off the network. The following variables are used to compute the score:

- **Net transfers:** This is the total amount the participant has paid to add transactions over the previous 30 days.
- **Currency vested:** The sum of money that a participant has contributed to the creation and addition of a new block to the network is indicated here.
- **Cluster nodes:** Users can help other users become miners by lending them their vested score, which raises the user's important score.

The network has more faith in a node's capacity to validate transactions and mine data if it has a higher score. **Harvesting** is the mining procedure in PoI, which does not require a lot of processing power as PoW and PoS do. Rather, block creation is assigned by users to a **Super Node (SN)** that satisfies certain criteria. The popularity of the users who have contracted with a social network (SN) to handle their harvesting determines how many blocks it generates. Ultimately, users receive the blockchain benefits from the SN in accordance with their significance [60].

Proof of Capacity (PoC) Another consensus method for building additional blocks is called **Proof of Capacity (PoC)**, sometimes referred to as **Proof of Space (PoSpace)** and **Proof of Storage (PoStorage)**. Given that the method is based on storage capacity, these names make sense. With minor nomenclature changes, the idea was first presented by *Dziembowski et al.* in 2013 and then again by *Ateniese et al.* in 2014 [109]. The PoW mechanism in blockchain establishes the legitimacy of fresh blocks. It is just one of many techniques used to choose the network node that will produce the following block for the blockchain. PoC is regarded as being extremely resource- and energy-efficient, which opens it up to a larger audience. As a kind of stake and deployment, players in this method assign temporary storage space on their hard drives. They create graphs from hashes using the network's memory; the more memory they set aside for charting, the more likely it is that they will generate the next block. The node validates the plotted hashes to show that it is committed. The node can demonstrate the storage space it has offered if the hashes are accurate. PoC has been further investigated and applied in the cryptocurrency space by projects like **Signum** (formerly **Burstcoin**), **SpaceMint**, **Chia**, and **Spacemesh**.

3.4.2 Consensus Algorithm in V2X Communication

Through their innovative integration of the Internet of Things (IoT) and the automotive domain, researchers have made once-fantastical technologies like driverless cars a reality. The idea of

autonomous cars is no longer far off; all of the big automakers are hard at work improving these cars and making sure they are very secure and functional. To do this, a decentralized database was required, and blockchain technology proved to be the best option. However, an efficient consensus mechanism is also required for blockchain to function as best it can in this situation. This subsection will concentrate on the techniques that support communications in the V2X (Vehicle-to-Everything) business and the Internet of Things (IoT), given the importance of consensus algorithms in the cryptocurrency space, as covered in the previous section. These techniques are essential for facilitating safe, dependable, and effective data flow between autonomous cars and the infrastructure around them.

Proof of Location (PoL)

Recently, the blockchain has attracted a lot of attention due to its effectiveness and capacity to resolve a number of decentralization-related issues. But if its flaws are overlooked, its main asset—consensus—may also be its worst weakness. As a result, new algorithms have to be developed in order to make accommodations for the system's constraints. **Proof of Location (PoL)** consensus is one such approach designed specifically to handle the limitations of V2X communications. A digital certificate attesting to a person's presence in a particular location at a specified time is used. This idea uses the decentralized structure of peer-to-peer networks to improve privacy by limiting access to users' shared information and physical locations by central authorities. PoL is safely kept in the blockchain. One of the main prerequisites for PoL is that all requests and responses must be signed using the sender's private key so that the recipient can use the public key to verify the integrity. Furthermore, PoL checks are carried out with the help of the physical layer capabilities of the system. Even when a vehicle is beyond of direct sensing range, it may nonetheless confirm its location to neighboring vehicles using a decentralized PoL technique. This method has been used to evaluate overhead and detection performance in platooning situations. Moreover, using connection analysis and realistic vehicle mobility datasets, the research investigates the viability of building decentralized PoL systems without the aid of infrastructure [21, 28].

Practical Byzantine Fault Tolerance (PBFT)

The Practical Byzantine Fault Tolerance (PBFT) algorithm was first presented by *Miguel Castro* and *Barbara Liskov* in 1999 [23]. This method has become necessary in tandem with the Byzantine Fault Tolerance issue, which includes multiple reasons for network failures and message manipulation. In V2X communication, where message correctness is critical, such problems are unacceptable. In order to overcome these difficulties and offer a secure environment, PBFT was developed. All nodes in this network are connected, and most of them are reliable and honest. One-third of the system's nodes must remain honest in order for the algorithm to operate properly; otherwise, the system will be vulnerable. This method makes high-performance Byzantine state machine replication possible, which is ideal for Internet of Things and car communication. It can process thousands of requests per second with millisecond latency. Let us now examine the three stages of PBFT operation as presented in figure 3.6, which are pre-prepare, prepare, and commit [22, 57].

- **Pre-Prepare:** Backup nodes get the request at this stage and create a proposal, which is similar to filling out forms to formally submit a request.
- **Get ready:** Nodes handle the request and try to come to an agreement.
- **Commit:** To guarantee consistent outcomes and strengthen consensus security, nodes confirm their agreement and carry out the request twice.

Cars' ability to retrieve consistent information and future improvements, such as *Q/U, HQ, Zyzzyva,* and *Aardvark*, has been shown to be significantly enhanced by PBFT [118].

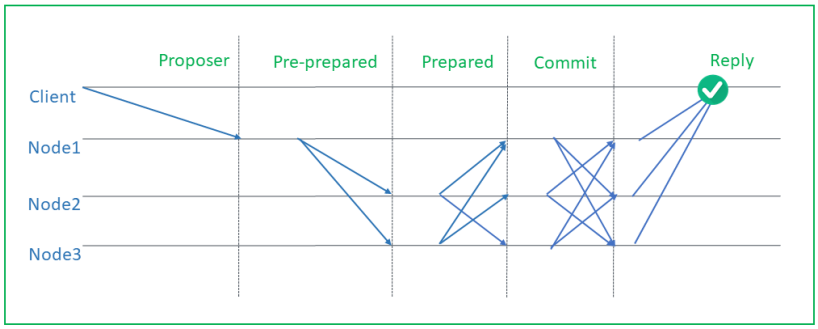


Figure 3.6: PBFT

Proof of Authentication (PoAh)

Proof of Authentication (PoAh) offers a simplified method for block verification while maintaining the core functional concepts of current blockchains. Like any other algorithm, PoAh's function is to authenticate blocks on the blockchain so that the network's mining operation can use them. This is the start of the mining process, where miners rely on the nodes in the network to supervise all transactions by making sure that all nodes keep consistent and identical records. The term "trusted nodes," or "T-Nodes," refers to nodes that authenticate themselves in two steps: first, they confirm the block's source, and then they validate the block using T-Nodes. The ledger gets updated if everything goes according to plan. If a miner makes a mistake, though, it loses its trust status and becomes a regular node again. In the context of the V2X, PoAh provides an energy-efficient alternative to inverse hash computations for distributed secure communications and computing [84, 115, 116].

Proof of Eligibility (PoE)

Intending to achieve consensus on a common set of suggested values, *Saunois, Geoffrey, et al.* created the consensus algorithm **Proof of Eligibility (PoE)** in 2020 [130]. This ensures a high likelihood that all values presented by honest nodes are included in the decision. A straightforward yet incredibly responsive algorithm is desperately needed in the IoT and V2X sectors, and PoE meets this need by supporting both domains. This is especially important in the V2X domain, where all devices must be able to communicate with each other seamlessly [79]. PoE helps identify the party in charge of finishing a work. The method seeks to maximize the likelihood of all honest users in the permissionless, asynchronous system converging on the same set of transactions within a predefined, finite number of rounds. It also needs to be resistant to the effect of a strong enemy that can adapt and corrupt entities in real time. Building a permissionless blockchain necessitates calling consensus instances in a sequential order. Honest users go through three basic processes at the end of each round: validity, agreement, and termination. Consensus is reached after these stages are successfully finished.

3.4.3 Consensus algorithm in Commerce

We will examine the consensus algorithms that are essential in today's business environment in this part, starting with Paxos and moving on to Raft. We additionally use Proof of Work (3.4.1), Proof of Stake (3.4.1), and Practical Byzantine Fault Tolerance (3.4.2). But we would not go over things again here because we have already covered them before.

Paxos

Paxos was first introduced in 1989 with *Leslie Lamport's* paper "*Paxos Made Simple*" which was presented in the part-time parliament [66]. Since then, Paxos has established itself as one of the most reliable algorithms, providing distributed systems with an extremely safe foundation. Paxos is a useful tool for managing data loss, redundancy, and replicating processes with exact duplicates, all while achieving fault tolerance in single processes. This guarantees that other nodes can easily take over in the event of a node failure, preserving system functionality. The fact that client request sequences are distributed to every cluster node accounts for this robustness. As a result, in the event that the node processing the client request runs into trouble, the data is preserved, enabling processing by a different node [68]. Peer-to-peer communication is used in the system, and each peer plays one of three roles: **proposer**, **acceptor**, or **learner**. A **proposer** proposes a value to be agreed upon at the Prepare stage, and acceptors choose whether or not to accept this proposal based on predetermined criteria. When the majority of **acceptors** concur, the value is selected and **learners** are told of the choice during the accept step. This approach offers a reliable solution for distributed computing by guaranteeing that a consensus is obtained even in the event of node failures [143]. The two stages of these roles are **Acceptance** and **Prepare**. To gain further insight into the Paxos algorithm, you can consult the figure 3.7 .

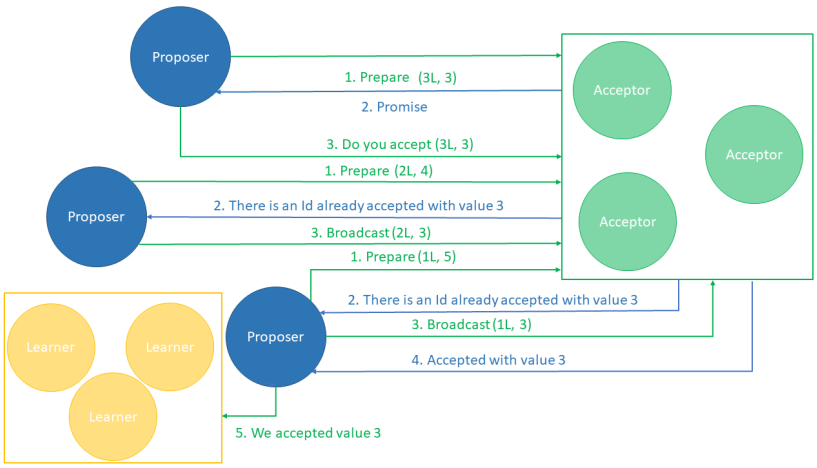


Figure 3.7: Paxos scenario

Raft

The Raft method was developed in 2014 by *Stanford University's Diego Ongaro* and *John Ousterhout* with the goal of making replicated log management easier [104]. Although Raft shares some similarities with the Paxos algorithm, its structure is more straightforward, making it easier to implement. Replicating a log sequence among a network of nodes is Raft's main goal. Raft maintains agreement among the nodes by making ensuring that no node commits a different entry to the same spot when new information is "committed" to the log. The idea of election, in which a chosen leader directs the replication process, is essential to Raft. After winning an election, the leader notifies its supporters of fresh additions, which they must subsequently commit. When a leader's tenure ends, another node takes over as leader and the former leader becomes a follower again. *Howard* (2015) Raft and *Huang* (2019) Performance. Raft nodes function in one of three states: **follower**, **candidate**, or **leader**, as seen in figure 3.8. At first, every node functions as a **follower**, able to vote and take log entries from the **leader**. When nodes do not get entries for a predetermined amount of time, they become **candidate** states and ask their peers for votes.

After obtaining a majority of votes, a **candidate** assumes leadership roles. The **leader** must then approve fresh log entries and distribute them to every **follower**. Furthermore, if stale reads are undesirable, all questions must be directed to the **leader** in order to maintain consistency. The cluster is ready to receive new log entries when a **leader** has been established. The **leader** can be asked by clients to add new log entries to Raft, which are binary blobs that are opaque. The **leader** then attempts to reproduce these entries by putting them in storage for a majority of **followers**. An entry can be applied to a finite state machine once it has been judged committed. This finite state machine's implementation is unique to the given application.

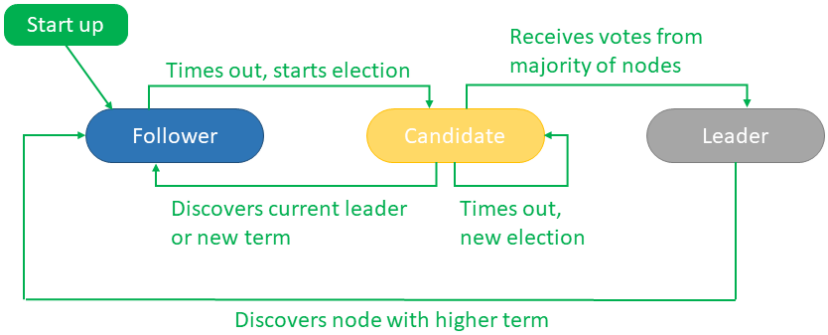


Figure 3.8: Raft node state

3.5 Specific Problems Addressed by This Research

This study attempts to fill up a number of research gaps that the literature review identifies. More all-encompassing solutions that tackle the issues of privacy, technology integration, permission processes, user engagement, and data management holistically are required, even in light of the expanding corpus of research on proximity marketing. By filling in these gaps, the field can progress considerably and proximity marketing tactics can become more successful. This study aims to address a number of important issues surrounding proximity marketing. Firstly,it focuses on fostering trust between customers and retailers by encouraging transparency and dependability in marketing practices based on MAC Swaping methods . Secondly, it attempts to rectify the absence of strict methods for obtaining user consent, with the goal of establishing strong frameworks for consent management. Thirdly, it aims to improve customer control over personal data, guaranteeing that users have more authority over their information. Lastly, the study addresses the necessity for appropriate classification methods that not only ensure accurate categorization of proximity marketing actors but also establish clear standards for their implementation. Resolving these problems is essential to fulfilling the research's overarching objectives, which include optimizing proximity marketing's efficacy and guaranteeing adherence to legal requirements.

3.6 Conclusion

Finally, this cutting-edge chapter offers a thorough examination of proximity marketing, a developing industry that uses location-based technologies to send messages that are specifically targeted. The examination covers a wide range of topics, including proximity marketing methods enabled by technical improvements and ethical issues like client consent and privacy. A crucial discovery in this field is the absence of a well-defined categorization scheme, which makes it difficult to methodically comprehend and implement various forms of proximity marketing, such as identity-based, emotional, and physical proximity.

The study draws attention to important implementation obstacles related to proximity marketing, including handling permission methods, handling privacy issues, and successfully integrating different network technologies. Customers currently have little influence over how their data is used in proximity marketing, exposing a significant power imbalance. This emphasizes how urgently stronger regulatory frameworks and improved data protection procedures are needed to overcome the lack of client confidence and preserve consumer privacy.
In order to solve these problems, our thesis offers creative fixes and improvements, which will be covered in more detail in the upcoming chapters. Our goals are to empower customers through improved permission processes, create a clear classification framework for proximity marketing, and prioritize privacy protection. By addressing these problems, we hope to improve proximity marketing's morality, viability, and user experience while also preserving consumer rights and preferences and fostering the trust required for long-term success in this rapidly evolving industry.

Chapter 4

Contribution 1: MAC Swapping for Enhancing Privacy

This cutting-edge chapter examines current proximity marketing research with an emphasis on consumer permission and privacy. Developments in network tools, privacy challenges, classification of marketing tactics, and moral dilemmas involving customer consent are important subjects. The chapter looks at issues with online consent, how businesses handle it, and the legal laws of using data. It also emphasizes how developments in communication technologies, which address issues like user acceptance, scalability, and privacy-preserving frameworks for managing data permissions, can improve proximity marketing.

4.1 Introduction

As we have seen in an earlier chapter 2, proximity marketing has become a potent tool for companies looking to interact with their target markets in highly customized ways. Based on location, preferences, and behavior, businesses can serve contextually relevant content by taking advantage of consumers' proximity to real venues. Numerous industries have embraced this focused strategy, and merchants in particular are employing proximity marketing to draw clients and provide personalized advice inside their establishments. By monitoring users' real time locations and actions, technologies like Bluetooth, Wi-Fi, and GPS are essential to enabling these tailored interactions. Presence marketing has benefits, but it also poses serious privacy issues. Without the express consent of the consumer, tracking their whereabouts and activities might cause emotions of invasion and mistrust. Mobile device MAC addresses and other unique identifiers are frequently used to track users' whereabouts and provide tailored content, which raises privacy concerns. Striking a balance between preserving user privacy and offering insightful customer data is crucial to resolving these problems. It is impossible to exaggerate the value of privacy in proximity marketing. Maintaining consumer trust and establishing sustainable business practices are two more reasons why protecting privacy is so important. Complying with international regulations like the GDPR (Europe), CCPA (California), CDPA (Colorado), CPRA (enhanced CCPA), LGPD (Brazil), PIPEDA (Canada), and PDPA (Singapore) is just one concern. These laws impose stringent requirements on permission, data processing, and gathering, highlighting the necessity for companies to implement privacy-aware marketing tactics. The purpose of this chapter is to examine the privacy issues raised by proximity marketing and offer solutions to these problems. We will look at current practices, privacy concerns, and possible fixes to improve privacy in proximity marketing campaigns. We provide a novel method for maintaining user anonymity while enabling successful proximity-based marketing through random MAC address switching. Our goal in implementing this randomization process is to strike a balance between giving companies access to useful customer data and protecting user privacy. This is how the rest of the chapter is organized. We will first examine relevant research in proximity marketing, looking at the practices used now, privacy issues raised, and suggested fixes. Next, we will talk about the particular issue of companies tracking clients using their MAC addresses without permission. After that, we will introduce our unique contribution—MAC address swapping—as a way to improve proximity marketing privacy aside from the consensus algorithm. In addition, we will offer a thorough analysis of our suggested algorithm to see how well it works to improve user control, safeguard privacy, and reduce the hazards associated with monitoring and profiling. In conclusion, we will provide an overview of our research, talk about its ramifications, and offer some recommendations for future improvements to proximity marketing campaigns' privacy. This chapter intends to contribute to a more moral and privacy-conscious approach to proximity marketing, in line with both legal requirements and consumer expectations, by addressing privacy concerns and offering creative solutions.

Research Questions

1. Which privacy issues with proximity marketing are the most pressing, especially with reference to the tracking of customers through MAC addresses and other unique identifiers without their express consent?

2. How can the employment of other privacy-enhancing strategies in conjunction with the suggested solution of randomized MAC address switching successfully strike a balance between user privacy and the demands of businesses to obtain important consumer data for proximity marketing campaigns?

4.2 Privacy Challenges in Proximity Marketing

Proximity marketing has significant privacy problems since it uses technologies like GPS, Bluetooth, and Wi-Fi to send customized information and adverts depending on a user's location. MAC address tracking is a major issue in this arena. MAC addresses function as distinct identifiers for devices, enabling advertisers to monitor a person's whereabouts and actions over an extended period of time. Persistent tracking allows for the building of extensive profiles without the knowledge or consent of the user, which might result in serious privacy violations. The insufficiency of the existing opt-in and opt-out solutions exacerbates this problem. The procedures to consent to or withdraw from such data collection are sometimes unclear or too complex, and many users are ignorant of the times and means by which their location data is being gathered. The autonomy and trust of users are undermined by this lack of transparency and control, which makes it challenging to maintain adherence to ethical norms and privacy laws. To enhance user control and protect privacy, effective proximity marketing must address these issues by implementing strong anonymization algorithms for MAC addresses and streamlining the consent process.

4.2.1 MAC Address Tracking

A popular tool in proximity marketing is MAC address tracking, which tracks and identifies devices and, by extension, their users, as they travel across a physical place. This is a thorough explanation of the hazards connected with MAC address tracking and how it operates.

Mechanisms:

- Device Identification: The manufacturer of each network-capable device, including laptops, tablets, and smartphones, assigns a distinct MAC address to each one. On local networks, this address acts as the device's hardware identifier.
- Signal Detection: When devices approach a proximity marketing system, sensors like Bluetooth beacons, Wi-Fi access points, or RFID scanners are used to identify and record the MAC addresses of those devices. These sensors are frequently positioned thoughtfully in busy places like shopping malls, transit hubs, and other public spaces.
- Data collection: When a MAC address is found, the sensor records it together with metadata like the location and time of the find. The device's (and its user's) movements inside the area can be monitored using this data.
- Data analysis: To identify trends, such as visit frequency and length, travel routes, and dwell times at particular sites, the gathered data is examined. Enhancing consumer experiences, operational effectiveness, and marketing strategy optimization can all benefit from this knowledge.

Risks:

- Persistent Tracking: Without the users' knowledge or consent, persistent profiles of them can be created using MAC addresses, which are unique and usually static. Significant privacy dangers are associated with this ongoing tracking because it can disclose specific behavioral patterns and personal preferences.
- Data Correlation: In order to develop full profiles of individuals, MAC address tracking data may be correlated with other personal data (such as transaction records and loyalty program data), raising further privacy concerns.

- Unauthorized Access: MAC address tracking yields sensitive and important data. This data is vulnerable to theft, misuse, and unauthorized access in the absence of appropriate security measures.
- Anonymity Loss: Although MAC addresses themselves do not contain personally identifiable information (PII), the ability to link them with other data sources can lead to the de-anonymization of individuals.

4.2.2 Legal Implications

Privacy Concerns:

- Lack of Consent: The acquisition of data without the express agreement of users is one of the main privacy issues with MAC address tracking. It frequently happens that users are not aware that their devices are being tracked, which goes against the ideas of informed consent and transparency.
- Unwanted Surveillance: As continuous tracking essentially subjects users to unwelcome surveillance, it may feel obtrusive to them. This may undermine confidence in the companies using these technologies and harm their brand.
- Data Misuse: There is always a chance that the information gathered will be utilized for something other than what was revealed or intended, including targeted advertising without the knowledge of the user or, worse, discriminating actions.
- Security Vulnerabilities: Cybercriminals find a lucrative target when massive amounts of location data are aggregated. Sensitive information may become public due to security breaches, which puts consumers at risk of identity theft and other problems.

Legal Implications:

- Regulation Compliance: Strict guidelines are enforced by a number of data protection laws regarding the gathering and use of personal information. The following important laws have an impact on MAC address tracking:
  - General Data Protection Regulation (GDPR): If MAC addresses can be connected to a specific person, they are regarded as personal data under GDPR. Before collecting users' MAC addresses, organizations must get their express consent and give them clear information regarding how the data will be used.
  - Under the California Consumer Privacy Act (CCPA), individuals have the right to know what personal information is being collected about them, to access that information, and to request that it be deleted. If MAC address tracking data can be used to identify or connect to a specific customer, it is covered by the CCPA.
  - Lei Geral de Proteção de Dados (LGPD): Brazil's version of GDPR mandates that enterprises seek user consent before collecting data and provide all information related to data processing activities. The same degree of security that applies to other personal data also applies to MAC address data.
- Data Minimization and Purpose Limitation: The concepts of data minimization and purpose limitation are enforced by laws such as the GDPR and LGPD. This means that organizations cannot gather more data than is strictly required for the intended use, nor can they use it for unrelated reasons without further consent.

- User Rights: Users have a number of rights under regulations about their data, including the ability to access, edit, remove, and limit processing. Establishing procedures to support these rights is a must for organizations, and it can be difficult when working with MAC address data that is intrinsically connected to machines rather than people.
- Security Obligations: Organizations are legally obligated to implement appropriate technical and organizational measures to ensure the security of the data collected. This includes protecting against unauthorized access, data breaches, and other security threats.

4.3 A Consensus Approach with MAC Address Swap

Users frequently voice grave concerns about losing control over their personal information, especially location data. The way things are currently done compromises user privacy and raises ethical concerns because it enables advertising and businesses to follow consumers based just on their MAC addresses. We suggest a novel solution that uses a consensus mechanism with pseudonym MAC address swapping to address these problems. By using this technique, users will have more safety and control over how they interact with proximity marketing campaigns.
Pseudonym MAC addresses swapping and the consensus mechanism are the two primary components of our suggested method. Through the usage of a pseudonymization method, the program makes sure that users' true identities are kept hidden. By constantly switching pseudonymized MAC addresses, users can maintain a better level of anonymity and escape ongoing surveillance.

4.3.1 Mechanism of MAC Address Swap

The suggested method is a multi-step architecture that combines the Advanced Encryption Standard (AES) with the Diffie-Hellman key exchange protocol to secure MAC address shifting. This design takes the following precautions to protect user privacy and anonymity:

1. Consensus Building: Before the algorithm proceeds, proximity network users must give their agreement. A chosen leader facilitates consensus-building when participants assess the possibilities and render decisions in accordance with their preferences and standards. Cost, quality, provenance, and other relevant factors may be included in these standards. To accomplish this:
    - Prior to awaiting user input, the leader must publicize each offer (fig. 4.1).
    - In the interim, users receive offers and have the option to accept them (opt-in) or reject them (opt-out), which enables us to honor their choice to engage in proximity marketing (fig. 4.2).
    - Following his selection based on many factors (fig. 4.3), the customer will provide his comments to the leader, assisting him in coming to a consensus (fig. 4.4).
2. Lifetime and Swapping of MAC Addresses (Figure 4.5):
    - To stay anonymous, each user uses a pseudonymous MAC address that is usually changed every 15 minutes.
    - If MAC addresses are only re-randomized at the beginning of a new connection, businesses can start profiling their users. In order to combat this, when the MAC address lifespan expires, users start the process of exchanging with other users who are close. For this swap, a secure connection is established using the Diffie-Hellman key exchange and AES algorithms, guaranteeing secrecy and integrity.

3. Swapping Procedure (Figure 4.6):
    - Users produce and exchange public and private keys using the Diffie-Hellman key exchange during the swapping process, resulting in the creation of a shared secret key for communication.
    - Users create a secure connection and switch MAC addresses using the AES technique to conceal their true identities from the proximity marketing system.
4. Rotation of MAC Addresses Over Time:
    - By repeatedly exchanging MAC addresses with other nearby users, users regularly rotate their addresses. This preserves greater degrees of privacy and lowers the possibility of long-term tracking.

4.3.2 Technical and User Benefits

The following benefits of the suggested method improve user control, privacy protection, and anonymity:

1. Enhanced User Control: Consumers can impact proximity marketing efforts by voicing their preferences during the decision-making process. This guarantees that user interests are taken into account.
2. Privacy Protection: The method greatly improves privacy by making it harder for proximity marketing systems to monitor or identify users by exchanging pseudonymous MAC addresses with nearby users.
3. Anonymity: Strong anonymity and identity protection are offered by the secure MAC address swapping method that uses the Diffie-Hellman key exchange protocol. User identities are protected during the establishment of a secure connection and the safe exchange of keys.
4. Reduced Tracking and Profiling: By limiting the amount of historical data that accumulates, regular MAC address changes lower the chance of identity theft and unlawful observation. Users reduce the risk of tracking and profiling and retain greater anonymity.

By emphasizing limited data collection and processing, our method not only complies with but surpasses legal standards; it is in line with international privacy regulations such as the GDPR, CCPA, CDPA, CPRA, LGPD, PIPEDA, and PDPA. All of these frameworks stress the need of safeguarding personal information and support the anonymization or pseudonymization of sensitive data—a fundamental component of our suggested remedy. By using this consensus-based pseudonym MAC address switching method, proximity marketing can strike a careful compromise between strong privacy protection and efficient marketing. By using this technique, individuals are empowered, their privacy is improved, anonymity is guaranteed, and the risks related to tracking and profiling are reduced. In the end, our strategy increases openness and confidence in proximity marketing systems, which benefits consumers and companies alike by fostering a more ethical and safe marketing environment.

4.4 Evaluation

In this section, we present a comprehensive examination of our proposed algorithm for enhancing user discretion and privacy in proximity marketing systems. We conducted several experiments

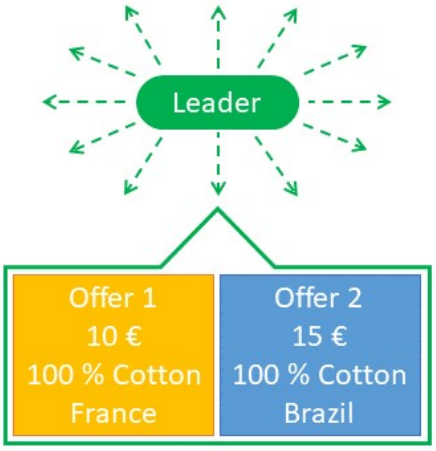


Figure 4.1: Broadcast the offers

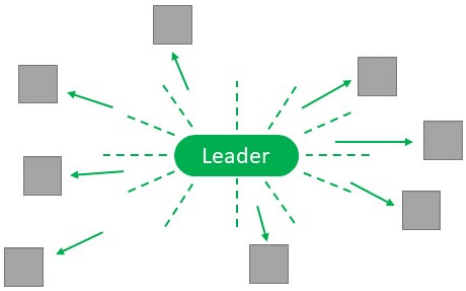


Figure 4.2: Receive the offers

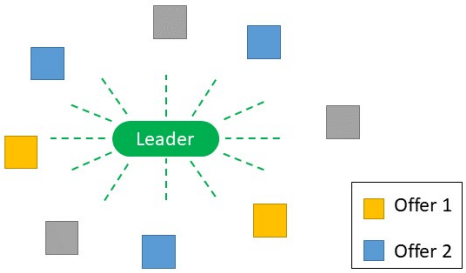


Figure 4.3: Make a decision

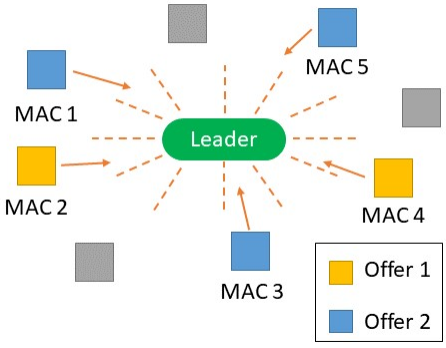


Figure 4.4: Send the decision

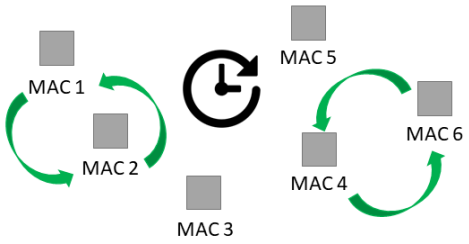


Figure 4.5: Swap MAC every 15 min

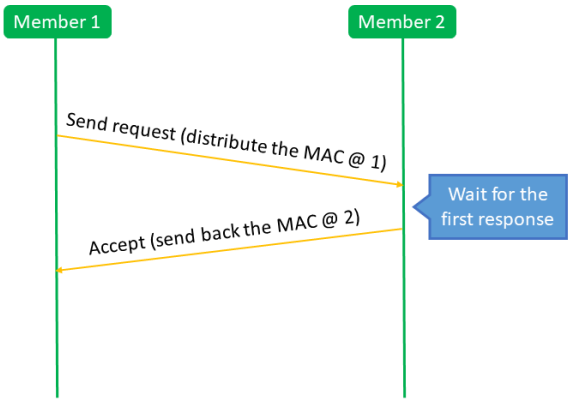


Figure 4.6: Only the first request is accepted and ignore the others

and assessments to determine the effectiveness and resilience of our algorithm against potential attacks and to evaluate its performance through simulation.
The approach was developed using the Python programming language, utilizing its vast ecosystem of tools and frameworks. To be more precise, we used the cryptographic libraries *Diffie-Hellman* and *AES* to provide secure MAC address switching and ensure the integrity and secrecy of data transferred. The project made advantage of the *Raspberry Pi 4*, a versatile hardware platform whose processing capacity and wireless connectivity make it ideal for proximity marketing applications.
We wanted to assess how well our algorithm used a consensus approach to choose and notify clients of the best deals through these simulations. The simulations were created to mimic real-world proximity marketing environments as nearly as possible. Customers received offers using Raspberry Pi devices, which sent specifics about the type, price, material, origin, and other relevant information about the goods. The system employed a consensus technique to examine these offers, with price serving as the primary metric.
Clients received multiple offers from adjacent Raspberry Pi devices during the exercises. The algorithm processed the submitted bids and then started the consensus process to determine which offer was the best. We impose a price metric boundary to guarantee equitable selection, taking into account those proposals that fall below the consensus threshold.
Based on the consensus conclusion, the algorithm presented the client with the best offer, allowing them to study it and decide accordingly. We were able to evaluate the algorithm's effectiveness in determining and providing the best offers to clients while accounting for their preferences and the predefined threshold using this simulation.
Throughout the simulations, we kept track of many algorithm performance metrics, such as consensus correctness, processing speed, and privacy protection. These metrics showed how well the algorithm maintained a fair and flexible decision-making process while providing clients with offers

that were both relevant and appealing.
The simulations were conducted several times to guarantee accurate and consistent results. The collected data was subjected to statistical analysis in order to assess the algorithm's performance and adherence to the predetermined standards.
The following presents the simulation results and an analysis of the algorithm's performance, including its ability to select the best offers, the level of client privacy protection, and the consensus mechanism's overall effectiveness.
Table 4.1 lists each scenario or configuration in the first column, and the second column shows the corresponding resistance level against MAC address correlation attacks, with options like "High," "Medium," "Low," and "N/A" to indicate the degree of resistance for each situation.
MAC address correlation attacks are not carried out in **Configuration A**, which is used as the reference configuration. It serves as a reference point for assessing the intrinsic resilience of the algorithm.
A simple assault is simulated in **Configuration B**, where an adversary looks at network traffic patterns in an attempt to launch a simple MAC address correlation attack. The attacker can examine the MAC addresses of different devices using techniques like packet sniffing or network traffic monitoring, then correlate those addresses with specific users depending on contextual information such as time and place.
A realistic attack scenario using well-known attack channels and strategies employed by adversaries is examined in **Configuration C**. However, the outcome is set to N/A because this case was not encountered throughout the study.

Table 4.1: MAC Address Resistance

Scenarios	Resistance Level
Configuration A: No Attack	High
Configuration B: Basic Attack	High
Configuration C: Real-World Attack	N/A

Figure 4.7 displays a bar chart illustrating the consensus correctness percentage of the proximity marketing system for varying quantities of offers. The x-axis displays the total number of offers, while the y-axis displays the proportion of consensus-accurate responses.
The chart shows that the percentage of consensus correctness varies across different numbers of offers. With 88.4% consensus correctness for 50 offers, there is a high degree of user agreement when it comes to selecting the best offer. With 100 offers, the consensus correctness slightly decreases to 87.2%. The pattern continues as there are 150 offers, and the consensus correctness drops even further to 84.7%. Remarkably, after 200 suggestions, the consensus correctness rises dramatically to 87.4%. This demonstrates that when there are more offers, the algorithm is more successful in getting customers to agree.
Overall, the bar chart provides insight into how well the proximity marketing system's algorithm supports user consensus by illustrating the relationship between the number of offers and the percentage of consensus-accurate judgments.
The line graph in Figure 4.8 illustrates how the algorithmic convergence of the proximity marketing system varies with the number of participants. The convergence rate is plotted on the y-axis, and the number of participants is indicated on the x-axis.
The line graph illustrates how the convergence changes with varying participant counts. The observed convergence percentage of 93.5% with 25 participants indicates a high degree of agreement in the participants' capacity for reaching a consensus. When there are 50 participants, the convergence percentage drastically drops to 90.7%. The percentage of convergence falls with the number of new members. With 75 people, the convergence rate drops to 86.8%, and with 100

participants, it drops to 84.3%.

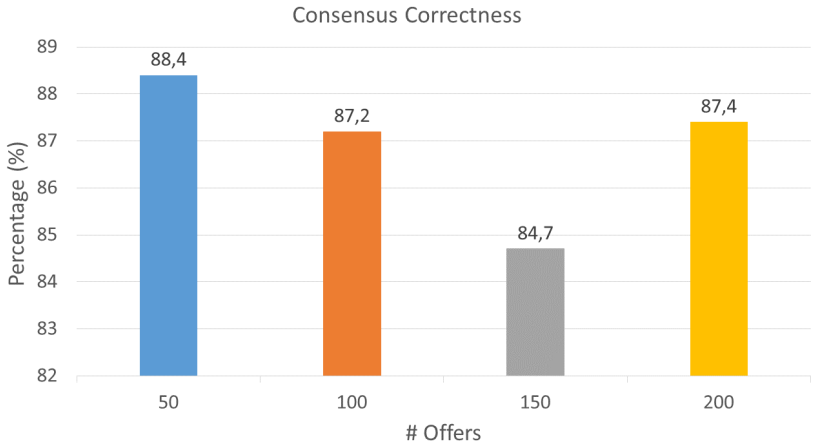


Figure 4.7: Consensus Correctness

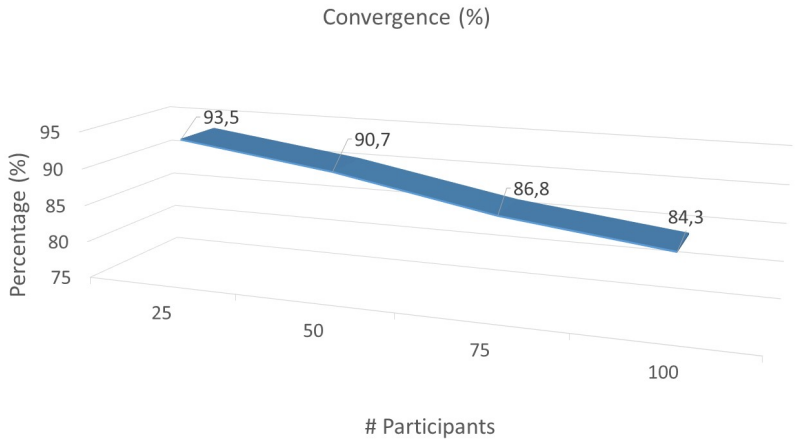


Figure 4.8: Convergence

The obtained findings demonstrate our algorithm's ability to promote user consensus in proximity marketing systems in addition to confirming its effectiveness in enhancing user control, protecting privacy, and reducing tracking and profiling threats. Extensive testing revealed strong resilience against MAC address correlation attacks, safeguarding user identities during the consensus process. By regularly changing MAC addresses, the system effectively secured user privacy by making it impossible for attackers to monitor and identify individual users.

4.5 Conclusion

4.5.1 Objectives achieved

1. Significant privacy issues are raised by proximity marketing, mostly because of the tracking of customers by MAC addresses and other unique identifiers without their express authorization. The main concerns are the possibility of unapproved monitoring and profiling, which can cause consumers to lose faith in businesses and feel as though their privacy has been violated. The chapter highlights how tracking users using their MAC addresses without their

knowledge or consent is a severe concern since it can lead to unauthorized surveillance and profiling, which puts people's privacy at grave risk.

2. Randomized MAC address switching is a suggested approach that attempts to preserve user anonymity while still facilitating successful proximity-based marketing, striking a compromise between user privacy and corporate demands. This technique lowers the possibility of tracking and profiling by routinely changing pseudonymized MAC addresses, safeguarding user privacy. In order to improve security, the chapter offers a consensus-based mechanism that uses pseudonym MAC address shifting and incorporates cryptographic techniques like AES encryption and Diffie-Hellman key exchange. Simulations show how this algorithm works to improve the efficiency and fairness of proximity marketing methods while thwarting MAC address correlation attacks. By maintaining user privacy while enabling businesses to access vital customer data, this creative approach promotes user trust and complies with global data protection regulations.

4.5.2 Summary of the chapter

This chapter discusses the grave privacy issues raised by proximity marketing and looks into possible remedies. In order to customize messages with customers, proximity marketing leverages real-time location and activity data. However, it also has a number of privacy issues, including the ability to monitor people without their knowledge or agreement by using MAC addresses and other unique identifiers. The chapter suggests a novel technique that uses random MAC address shifting to allay these worries. By routinely changing pseudonymized MAC addresses, this method seeks to strike a compromise between the requirement for user privacy protection and the need for customer data. This preserves user anonymity while enabling efficient proximity-based advertising. A thorough analysis of the regulations in different jurisdictions is given, emphasizing the consequences for proximity marketing methods as well as their requirements. The chapter emphasizes the possibility of unauthorized monitoring and profiling while discussing the technical features of MAC addresses, the dangers of MAC address tracking, and the legal repercussions. In order to improve user privacy by decreasing tracking, the chapter presents a consensus-based strategy that uses pseudonym MAC address shifting and cryptographic techniques including AES encryption and Diffie-Hellman key exchange.

To assess how well the suggested algorithm performed, simulations were run. The outcomes show how well the algorithm works to fend against MAC address correlation assaults and enhance the impartiality and efficiency of proximity marketing decision-making. Strong user consensus, fair decision-making, and high levels of user privacy are all guaranteed by the algorithm.

The chapter concludes by arguing for a more moral and private-minded approach to proximity marketing. The chapter contributes to the development of dependable and long-lasting marketing strategies that safeguard user privacy, cultivate consumer trust, and abide by global data protection regulations by addressing privacy concerns and offering creative solutions. This study highlights how crucial privacy-preserving solutions are in the sectors of proximity marketing and other data collection and processing. Subsequent investigations ought to go into other improvements and uses for the suggested method.

Chapter 5

Contribution 2: A New Agreement Mechanism in Proximity Marketing

The Control Algorithm, a new proposal added to proximity marketing that puts user privacy and control first, is introduced in this chapter. The consensus system incorporates an opt-in/opt-out option that enables consumers to control their data and interactions with marketing efforts. The Control Algorithm has the ability to enhance user engagement, data security, and business insights despite certain obstacles. The present study underscores the significance of user empowerment and establishes the foundation for forthcoming advancements in consensus processes.

5.1 Introduction

Decentralized networks and distributed systems are fundamentally based on consensus, which is the members' collective agreement on a shared state or value that is essential to maintaining integrity and dependability. Decentralized systems rely on consensus methods to coordinate this agreement amongst disparate nodes or entities.
This chapter presents the Control Algorithm (CA), a recently created algorithm created especially for the commerce industry. Offering clients more control over their interactions and transactions is the CA's main goal of empowering them. Through its emphasis on augmenting customer autonomy, this algorithm aims to reduce the likelihood of retailers exploiting it, so tackling the frequently seen problem of greed in business practices. Based on the values of openness and confidence, the Control Algorithm makes sure that customers are aware of the conditions of their contracts and are capable of handling their personal information responsibly. The CA promotes a more fair relationship between clients and merchants while simultaneously protecting consumer interests by putting in place systems that give priority to client consent and decision-making. This chapter will examine the Control Algorithm's technical details, including its basic design and functionality and the potential advantages it may provide to organizations and customers in the changing business environment.

5.1.1 Weaknesses in Consent Management in Proximity Marketing

Effectively managing user consent is a critical difficulty for proximity marketing, which uses location-based technologies to send personalized communications. In contrast to blockchain, where permission is intrinsically linked to smart contracts and cryptographic transactions, proximity marketing frequently has challenges in guaranteeing clear and user-focused consent processes. Users' lack of awareness regarding the collection, usage, and sharing of their data in proximity marketing campaigns may give rise to worries about control and privacy violations. Presence marketing strategies currently in use frequently rely on wide opt-in agreements or implicit consent models, which may not be compliant with changing legal frameworks (like the GDPR in Europe) or satisfy customers' rising expectations for openness and control over their personal data. This disparity emphasizes the urgent need for creative consent management solutions that uphold marketing tactics' efficacy while giving users empowerment and privacy protection first priority.

5.1.2 Consent Algorithms

Permission algorithms can be modified and used to improve proximity marketing data management procedures. This is done by taking inspiration from blockchain and other decentralized systems, which have led the way in the development of strong permission mechanisms. Transparent data governance frameworks, explicit opt-in/opt-out processes, and cryptographic user permission verification are all made possible by consent algorithms. Businesses may demonstrate their commitment to privacy and data protection to consumers and meet regulatory requirements by implementing consent algorithms that are specifically designed for proximity marketing. These algorithms can help consumers make more educated decisions about their data, communicate data usage regulations more effectively, and increase user engagement with marketing efforts.

5.1.3 Research Questions

The following research questions are addressed in order to direct our investigation and analysis:

1. What are the main obstacles to and chances for implementing consent management solutions in proximity marketing and other industries, including opt-in/opt-out procedures and beyond?

2. In what ways may the development of user-centric methods for data management and privacy protection in decentralized networks be informed by insights gleaned from consensus algorithms across many industries?

These study questions cover the investigation of consensus algorithms across industries, the difficulties and advancements in consent management in proximity marketing and other domains, and the more general consequences for privacy and user empowerment in decentralized systems. They offer a well-organized structure for analyzing the implications and comparative analysis covered in this chapter.

5.2 Comparative Analysis of Algorithmic Performance

To give a thorough knowledge of the algorithms covered in the earlier parts (3.4), table 5.1 presents a comparison of all the algorithms covered; The color scheme denotes how good or bad the classification is: where Green: represents a good sign and gives +1 to the score, Orange: represents an average sign and gives 0 to the score, and Red: represents a bad sign and gives -1 to the score. The criteria utilized here are centered on the needs of the world outside our own. The criteria we selected for this table are subjective and based on our interest in all domains.

Table 5.1: Comparison of consensus algorithms.

		Criteria					
		Computing Time	Network Exchange	Convergence	Attack Resistance	Popularity	Score
Algorithms	PoW	Low	Medium	High	High	High	+2
	PoS	High	High	High	High	High	+5
	PoB	Medium	High	High	High	Medium	+3
	PoI	High	Medium	High	High	Medium	+3
	PoC	High	High	Medium	High	Medium	+3
	PoL	High	High	Medium	High	High	+4
	PBFT	High	High	High	High	High	+5
	PoAh	High	High	High	High	Low	+3
	PoE	High	High	High	High	Low	+3
	Paxos	High	Medium	Medium	High	Medium	+1
	Raft	High	High	High	High	Medium	+4

Any algorithm's **Computing Time**, referred to as running time, is its main feature. It stands for the amount of time the algorithm needs to generate results. In our analysis, assuming homogeneous computer environments, the differences in computation time are due to the consensus mechanisms of the algorithms. For example, Proof of Work (PoW) requires a lot of processing power, which leads to somewhat longer computation times. On the other hand, PoS performs better, creating a new block every 10 seconds. Algorithms that prioritize speed, like Raft and Paxos, have significant computational power for use in commerce applications. Since these algorithms work in decentralized systems, network speed is important in both areas, especially for business. **Network exchange** capabilities are used to evaluate algorithms. While PoW, PoI, and Paxos show medium degrees of network interaction, the majority of algorithms show high levels. PoW, which has a large worldwide participant base, is limited by network speed. PoI functions in a regulated environment and is mostly utilized in NEM, which may improve network efficiency. Paxos demonstrates reasonable network exchange capabilities as well, despite its high number of nodes and message overhead.

These algorithms' efficiency can vary depending on a number of circumstances, including node failures and latency. Algorithms are grouped in the **Convergence** column according to how quickly they recover; PoW and PoS exhibit quicker recoveries because of their large participant networks. All algorithms exhibit high-security levels in terms of **Attack Resistance**, discouraging malevolent attacks since the costs of such attacks are too great to be worthwhile.
The **Popularity** of algorithms is evaluated, recognizing their importance in every field. Notable in the realms of cryptocurrency, commerce, and V2X applications, PBFT is worth mentioning together with PoC and PoL, which are applied in different contexts. As the cornerstones of Bitcoin, PoW, and PoS are far more well-liked than PoC, PoI, and PoB. While PoAh and PoE show great potential in V2X applications, their relative novelty prevents them from being widely used.
To make comparisons easier, each algorithm's performance is numerically represented in the score column. It is important to remember that different criteria have different levels of significance, therefore a higher score does not always translate into greater efficiency. When PoL and PoAh are compared, for example, PoL has a better numerical score, but PoAh may be more effective in some applications due to its lower popularity criteria, which may be less important than PoL's convergence criterion. As a result, the comparison is subjective because the choice of algorithm relies on the particular application scenario.
All consensus methods have been evaluated, however none of them completely satisfies the needs of the commerce domain. Customers frequently want particular features and performance attributes that are difficult for current algorithms to meet. As a result, the **Control Algorithm** is a brand-new algorithm that was created to close this gap. Control Algorithm is specifically made to meet the demands of the commerce industry, providing customized solutions that meet the wide range of customer needs. Control Algorithm seeks to address the shortcomings of current consensus processes and offers a strong basis for safe and effective transactions in the field of commerce through its novel methodology.

5.3 Control Algorithm (CA)

We suggest creating a novel algorithm to address the common problem of people feeling powerless while interacting with proximity marketing, with the goal of giving users more freedom and control over their information. This suggested method, dubbed the *Control method* (CA), introduces a consensus system that is integrated with an opt-in/opt-out mechanism, thereby shifting the paradigm in the field of proximity marketing. The Control Algorithm's basic idea is to solve the main grievance voiced by users, which is that they do not feel like they have any control over their personal information in proximity marketing settings. Users are frequently overloaded with tailored ads and promotional messages in modern marketing campaigns, frequently without their awareness or agreement. Users become less trusting of this lack of transparency and control, and serious privacy issues are raised. Through the use of a consensus system and an opt-in/opt-out mechanism, the CA gives users the ability to take charge of how they interact with proximity marketing campaigns. User consent and choice are given priority by the CA, in contrast to traditional marketing strategies that depend on indiscriminate data collecting and targeted advertising.

5.3.1 Opt-in / Opt-out

In this section, let us take a closer look at the Opt-in/Opt-out notion before delving into the specifics of our architectural framework.
The enormous amount of data that is produced and consumed every day is driving the modern economy. Businesses in a variety of industries will undoubtedly face previously unheard-of difficulties in the future, which will call for creative solutions in order to stay competitive. The utilization

of data will become more and more important in this changing environment, since it provides the foundation for well-informed decision-making and strategic planning. The field of web data collection is rapidly rising due to technological improvements and the increasing need for tactics that are insights-driven. Interestingly, a recent survey by *Bright Data* and *Vanson Bourne* [107] highlights how commonplace data-collection bots are, with over half (57%) of technology, financial services, and IT organizations in the US and UK using them. Although data has enormous potential, privacy and security issues are also brought up by it. Legislation controlling the gathering and use of personal data is therefore necessary to protect user privacy and reduce dangers. The Opt-in/Opt-out mechanism is a crucial component of data protection frameworks and is at the core of data privacy and user consent. Despite their apparent contradiction, these two ideas work well together to give people autonomy and control over their personal data. When a user opts in, they are expressing their clear consent to the gathering and use of their data for particular uses, including data analysis or targeted advertising. There are two main methods in the field of opt-in mechanisms: single opt-in and double opt-in. With single opt-in, people may sign up for services or newsletters by just entering their email addresses, giving permission for communication to begin right away. On the other hand, double opt-in verifies the legitimacy of users' consent by requiring them to confirm their subscription through text message or email. On the other hand, opting out is the procedure via which consumers withdraw their agreement to additional data collection or processing. Opt-out procedures are essential for ensuring user preferences remain intact, lowering the number of spam complaints, and protecting businesses' reputations. In the end, user empowerment serves as the guiding concept for both opt-in and opt-out processes, giving people the power to decide how their personal information is shared and used. These techniques contribute to a more moral and responsible data ecosystem where users' rights and preferences are recognized and preserved by promoting accountability and trust [63, 90].

5.3.2 Do we require more than just opt-in and opt-out?

Expanding upon our previous discussion, proximity marketing, characterized by the targeted delivery of advertisements or promotional messages based on consumers' physical locations, has gained considerable traction in recent times. However, ensuring the ethical and effective implementation of proximity marketing requires consideration of additional factors beyond traditional opt-in and opt-out methods. While these methods are essential for granting consumers control over their data and the messages they receive, they may not suffice when assessed against various criteria such as personalization, transparency, frequency, and opt-out options.

- **Personalization:** Consumers want more control over the kinds of communications they receive, going beyond opt-in/out procedures. Marketers can improve user engagement by providing individualized content based on the choices and interests of each individual user. However, it is crucial to find a balance between privacy concerns and personalization. To make sure that consumers are aware of and at ease with the process of acquiring data, it is imperative to maintain transparency on the methods and purposes of data collection.

- **Transparency:** In addition to personalizing efforts, openness is necessary to establish trust with clients. Marketers ought to be transparent about the data they gather, how they use it, and who the third parties are. Open and honest procedures give customers more faith in proximity marketing campaigns and may even boost opt-in rates.

- **Frequency:** Although proximity marketing allows for prompt client interaction, too much messaging may turn off the intended audience. Sending too many messages at once could irritate or distract recipients. The frequency of messages must be carefully calibrated by marketers to ensure relevancy and prevent overloading customers.

- **Opt-out Options:** Offering unambiguous and easily available opt-out methods are just as important as offering opt-in. It is important to respect customer preferences by making opt-out procedures simple. Consumers ought to be free to reject communications or unsubscribe from proximity marketing campaigns whenever they see fit.

It makes sense that people might be concerned about how their data is used in proximity marketing. Even with opt-in and opt-out mechanisms in place, the gathering and use of personal data, including location information, can cause people to feel as though their privacy is being violated. Furthermore, insufficient data security protocols may expose gathered information to online attacks, hence creating hazards like identity theft. Thus, in order to maintain customer confidence and secure data privacy, organizations need to give careful consideration to data protection methods.

5.3.3 Implementation steps and processes

We provide an algorithm that combines a consensus system with an opt-in/opt-out mechanism to provide users greater control over their interactions with proximity marketing. We provide the *CA*, acknowledging that users' main issue is their lack of control over their data. By offering consumers more flexibility over how they interact with proximity marketing, this algorithm seeks to empower users. It does this by combining a strong consensus mechanism with adaptable opt-in/opt-out choices. Making sure users have total control over their data is our main goal. We shall go into detail about the Control Algorithm's phases in order to accomplish this. The method operates in five time slots, denoted by $\tau = \delta 1, \delta 2, \delta 3, \delta 4, \delta 5$, during each operational cycle. We will give a detailed description of how the algorithm works, breaking down each step inside these time intervals, in the following:

1. **Request for Consent ($\delta 1$):** Our algorithm's initial phase entails sending a consent request to nearby clients via beacon technology. In this context, "*consent*" refers to users' approval to engage with the system and receive commercial communications. We can send requests straight to clients' phones or other devices using beacon technology, making it easy for them to opt in if they are interested. The opt-in vs. opt-out procedure is explained in detail in the request (figure: 5.1a).

2. **Participant Response ($\delta 2$):** Participants share their answers in the second step. If a customer opts out, they will not get any more messages. Customers who opt-in, on the other hand, are noted as interested parties and get a confirmation message stating that offers will be sent to them (figure: 5.1b).

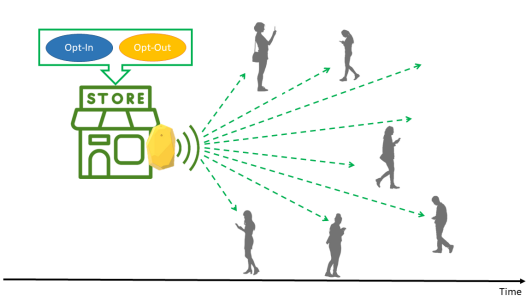
3. **Neighbor Feedback ($\delta 3$):** At this point, each user notifies neighbors—those in the vicinity who have also agreed to participate—with their evaluation of the offers. Participants can discuss the offers openly in this step, which helps to highlight their advantages and disadvantages. Feedback, both good and negative, should be shared openly and courteously (figure: 5.1c).

4. **Opinion Consolidation ($\delta 4$):** After that, users combine their own thoughts with neighbor feedback. This procedure is essential for improving the suggestions and confirming their efficacy. To make sure that the offers are as dependable and effective as possible, the input collected should be thoroughly examined to pinpoint areas that need improvement (figures: 5.1d, 5.1e).

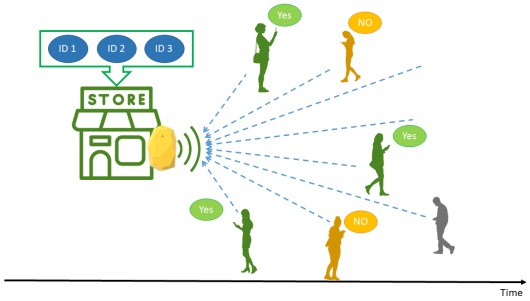
5. **Feedback to Store ($\delta 5$):** Ultimately, the store receives the aggregated participant feedback. This enables the retailer to comprehend the prevailing viewpoint and modify their offerings

as needed. Optimizing the offers being traded requires open communication of results and helpful criticism (figure: 5.1f).

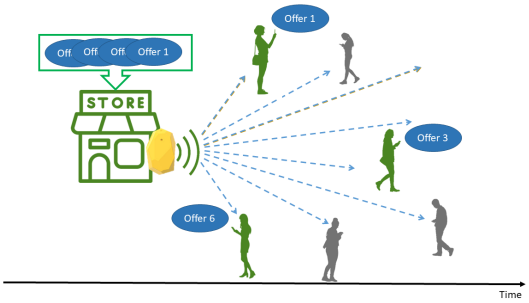
Among the many benefits that our algorithm provides, the most important one is improved user data safety. By granting users more control over their personal data, this is accomplished. Our cooperative relationships with companies, which let them interact with user data and get frank feedback on their offers, are another significant benefit. Businesses can use this feedback to better evaluate the impact of their offers and make the required changes. We achieve the ideal synergy that benefits both users and businesses by striking a balance between the distribution of personalized offers and strong privacy measures. Furthermore, the CA encourages transparency by communicating in an understandable and direct manner. Users and retailers alike stand to gain in the long run from this transparency's ability to foster confidence and trust among users.



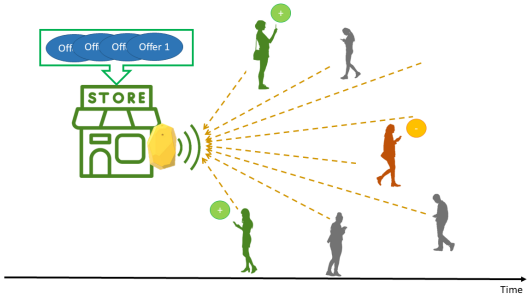
(a) Step 1 - Request for Consent



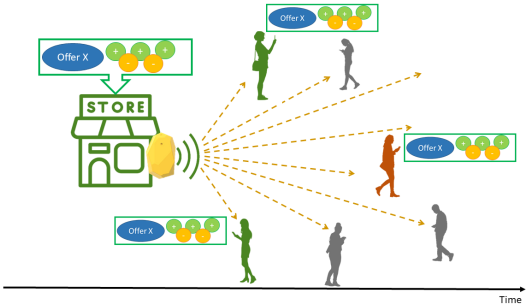
(b) Step 2 - Participant Response



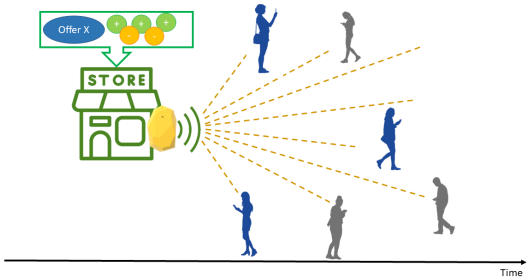
(c) Step 3 - Send the offers



(d) Step 4 - Opinion Consolidation



(e) Step 5 - Feedback to Neighbors



(f) Step 6 - Feedback to Store

Figure 5.1: CA Steps

5.3.4 Advantages and Challenges

Advantages of CA

- **Improved Security of Data:**
  - User Control: Users are in charge of what information they share and with whom, giving them more power over their personal data.
  - Privacy: The algorithm protects and upholds users' privacy through the use of opt-in and opt-out procedures.
- **Enhanced Interaction with Users:**
  - Personalization: Based on user input and preferences, the algorithm enables the delivery of tailored material.
  - Transparency: Users' confidence and trust are increased when communications are unambiguous.
- **Important Business Knowledge:**
  - Feedback Mechanism: Companies get candid comments on their offerings, which helps them gauge their effect and make the required adjustments.
  - User-Centric offerings: Companies can better satisfy the requirements and preferences of their customers by customizing their offerings based on user feedback.
- **Harmonious Combination:**
  - Benefits to Both Parties: By striking a balance between user privacy and the company requirement for data, the algorithm produces the ideal synergy.
  - Building Trust: Open and honest business methods help consumers and companies feel more trusted, which increases customer loyalty and long-term involvement.

Challenges of CA

- **Complex Implementation:**
  - Technical Difficulties: To guarantee seamless operation and interaction with current systems, the CA's implementation may call for a substantial investment of time and resources in technical know-how.
  - Maintenance: To keep the algorithm operating safely and successfully, regular upgrades and maintenance are required.
- **User Participation:**
  - Adoption Rates: User involvement is essential to the algorithm's performance. Should consumers be reluctant to consent, the algorithm's efficacy may be jeopardized.
  - User Education: Businesses may need to put in more effort to educate users about the features and advantages of the CA.
- **Resource Intensive:**
  - Cost: Creating and implementing the CA may be expensive, particularly for startups or smaller companies with tighter resources.
  - Time-consuming: Gathering, evaluating, and putting input into practice can take a lot of time, which could hinder company operations.

5.3.5 Simulation and Results

This section will offer a thorough description of the simulation and testing procedures used to assess and verify our algorithm's performance. We shall describe our methods and approaches to guarantee accurate and reliable results.
We took advantage of the *Raspberry Pi 4*'s capabilities as a proximity-based technology to put our algorithm into practice. We were able to deliver messages to neighboring mobile devices and provide location-based and context-aware experiences by utilizing beacon technology. To further establish a secure connection environment that prioritizes client privacy and market benefits, we further built a *Python* code that includes *socket* and *thread* libraries. The client-side actions are the main emphasis of Algorithm 1. Its primary objective is to use Socket technology to create a secure connection and enable customers to comment on the offers they get. Furthermore, the algorithm allows customers to read anonymous customer reviews, providing a thorough understanding of the deals that are offered. This algorithm's ultimate goal is to give consumers a seamless, secure experience while giving neighboring stores insightful data to enhance their offerings. On the other hand, Algorithm 2 is intended to make offers and gather scores in an exclusive way. We successfully implemented the procedures covered in the preceding part (section 5.3) by making use of both thread and socket libraries. We employed Thread technology to handle the many algorithmic phases, ensuring efficiency and organization all along the way. In order to guarantee a secure connection and prioritize data security and privacy at every turn, socket technology was also utilized. All in all, these algorithms are designed to give customers a smooth and safe experience while giving neighboring merchants insightful input that helps them improve their products.

Algorithm 1 Client

```
socket.connect()
message = socket.receive()
response = input()
socket.send(response)
if response ==' No'||'Quit' then
    socket.close()
else
    ad = socket.receive()
    score = socket.send(input())
end if
```

A thorough assessment of our program is given in Table 5.2, with an emphasis on important network and security criteria. This evaluation attempts to measure our algorithm's performance in a number of areas, such as data privacy, network performance, and security robustness. We can determine our algorithm's advantages and disadvantages by examining these factors and making the required modifications as needed. Our analysis directs future research and development efforts and provides insightful information on the efficacy of our methodology. The measurements that are being presented highlight how effective the algorithm is in various sectors. Its ability to address critical security issues and guarantee the security and privacy of client data is essential. Furthermore, the algorithm's intuitive architecture makes it simple to apply in a variety of corporate settings, reducing the need for significant changes. The evaluation of resource requirements, where the algorithm makes use of hardware resources already in place to streamline implementation and lower total costs, is very important. This leads to increased advantages and cost savings for the firms using the algorithm. Beyond its technological benefits, the algorithm has benefits for client relationships as well. Businesses can build stronger customer loyalty and trust by exhibiting a dedication to consumer security and comfort, which will ultimately improve the bottom line of

Algorithm 2 Server

▷ This function aims to gather clients who arrived at the same time slot by utilizing threads to divide them into groups.
procedure TIMER(τ, df):
    threading. Timer($\tau, timer, [\tau]$).start()
    $avg_score = df$.groupby('ad_id')['$score$'].mean()
    print(avg_score)
end procedure
▷ The purpose of this function is to manage the client's experience, ensuring their consent is obtained and obtaining their score of the offer.
procedure HANDEL_CLIENT($server_socket, address$):
                                                                ▷ Ask for consent.
    if $response ==' No'||'Quit'$ **then**
        $server_socket$.close()
    else
        $id = temporary_id()$
        $Ad_x = Ads[random]$
        $server_socket$.send(Ad_x)
        $score = server_socket$.receive()
        if $0 \leq score \leq 10$ **then**
            add all
        else
            ask for the score again
        end if
    end if
end procedure
                                    ▷ The goal of this function is to initiate the server.
procedure START():
    $server_socket$.connect()
    $client_thread$ = threading.Thread(target = handle_client))
    $client_thread$.start()
end procedure
start()

the organization. To sum up, the combined influence of these measures highlights the algorithm's benefits and effectiveness, making it an invaluable resource for businesses looking to improve infrastructure and network security while building client loyalty and trust.

Table 5.2: Evaluating

Criteria	Characterization
Scalability	As the number of users increases, our system's performance gets better. The client can manage a lot of data and users without sacrificing security or network performance if it stays close to the area.
Authentication	We guarantee that there is no need to worry about sensitive data or data breaches because our algorithm does not verify users—rather, it merely provides them with a temporary ID.
Encryption	Our technique protects data at rest and in transit using encryption socket connections.
Compilation	Our algorithm complies with the GDPR and other relevant security and data protection legislation. As rules change, mechanisms for opting in and out are in place to ensure continued compliance.
Redundancy	Our algorithm's network architecture includes redundancy to ensure high availability and low downtime in the event of a network or security issue.
Monitoring	There is a mechanism in place to monitor the network and identify any potential issues at the connection level.
Speed	Our algorithm is efficient and fast enough to provide recommendations in real time.
Integration	It is quite easy to combine this strategy with existing marketing platforms and may be implemented without any modifications.
Maintenance	The algorithm is easy to maintain and upgrade over time as customer needs and technological advancements change.
Cost-effectiveness	This approach is incredibly cost-effective when compared to other marketing strategies and technology, especially when it comes to security.

In contrast, we measured the **Speed** at which our algorithms reached consensus and the **Convergence** to determine if clients reached the majority decision quickly. In order to do this, we made offers to customers and watched to see what would happen in terms of features and cost. We changed the time interval (τ) to 60, 180, 300, or 600 seconds in Figure 5.2 and tracked the time until agreement was attained. To ensure that every participant received the same offers, we defined consensus as the choice made by the majority on the best offer. Interestingly, we saw that most had generally taken part, and a decision was essentially made after 65% of the entire duration had passed. This emphasizes how crucial it is to choose the right time frame for the consensus approach because making the wrong decision could cause needless delays in coming to a decision.

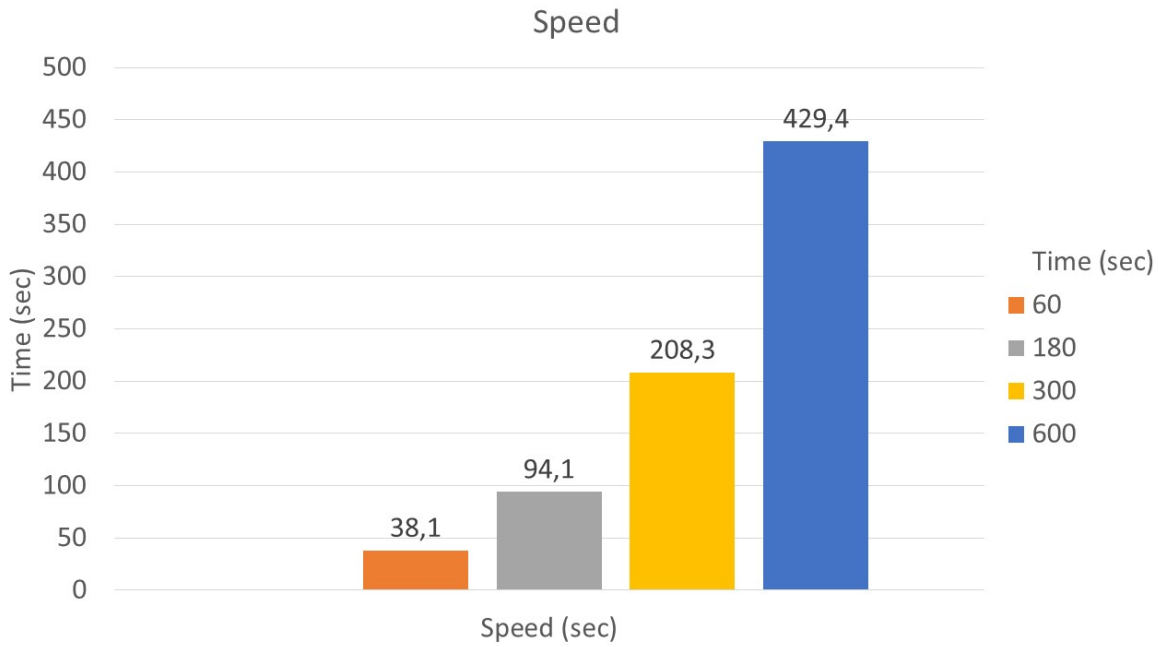


Figure 5.2: Speed

We assessed the convergence of the algorithm as the number of participants rose, as shown in Figure 5.3. More specifically, we examined the percentage of participants who, as we increased the number of participants to 25, 50, 75, 100, and 150, made selections based on price and quality comparable to the final selection. The results demonstrated the algorithm's excellent convergence and effectiveness in bigger groups, with an average of 76.58% of participants agreeing with the outcome. The algorithm's performance could be investigated further with a wider range of participants and alternative test parameters.

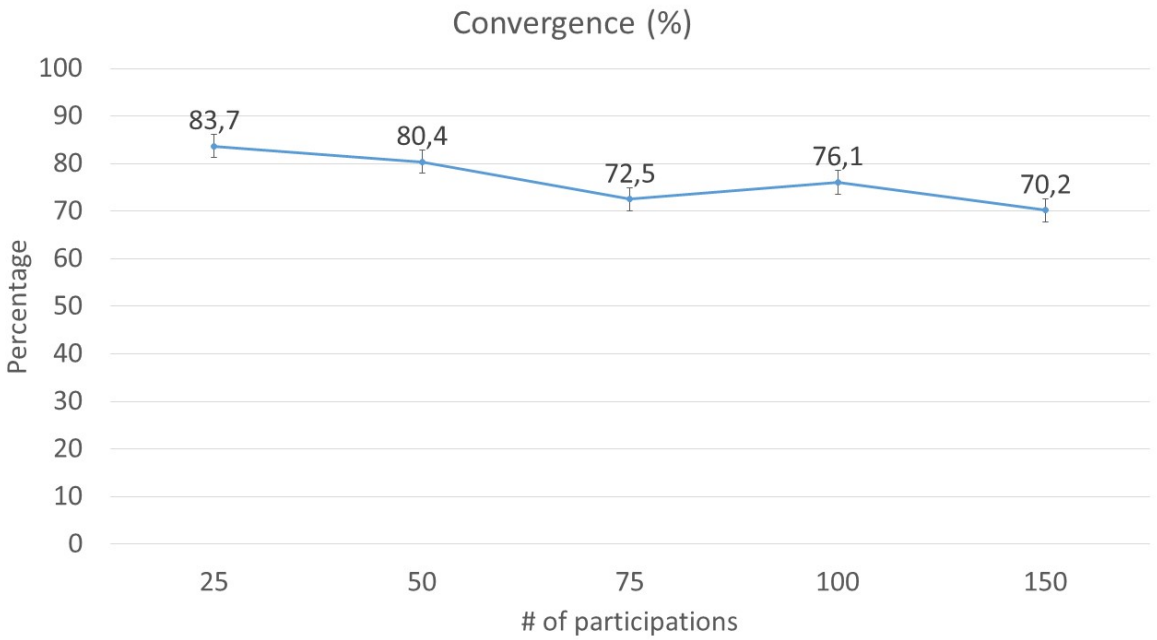


Figure 5.3: Convergence

5.4 Conclusion

5.4.1 Objectives achieved

1. We have looked at a variety of consensus algorithms used in various industries throughout this chapter, from the energy-intensive PoW, PoS, PoB, PoI, and PoC in cryptocurrencies to the PoL, PBFT, PoAh, and PoE in V2X communication and the simplified Paxos and Raft algorithms in commerce. Every algorithm has distinct features that are suited to the particular requirements of its field and represent different trade-offs between security, scalability, and decentralization. These revelations highlight how crucial it is to choose consensus algorithms that are in line with the goals and operational specifications of decentralized systems, opening the door to improved dependability and performance across a range of sectors.

2. The exploration of consent management solutions revealed significant challenges in proximity marketing, where traditional opt-in/opt-out mechanisms often fall short of meeting stringent privacy regulations and user expectations. The introduction of the CA represents a paradigm shift towards user-centric data management, integrating consent mechanisms with consensus algorithms to empower users with unprecedented control over their data interactions. By addressing these challenges, the CA not only enhances transparency and trust but also navigates complex regulatory landscapes, offering opportunities for more personalized and compliant marketing strategies across sectors.

3. Consensus algorithms provide valuable insights that open up new possibilities for creating reliable, user-focused methods of data management and privacy protection in decentralized networks. Through the integration of sophisticated consent mechanisms with consensus principles, the CA demonstrates this evolution and promotes a culture of data sovereignty and customized interaction. Through the utilization of these insights, companies can encourage more meaningful consumer connections while complying with strict data protection requirements. This will propel innovation and promote sustainable growth in the digital age.

5.4.2 Summary of the chapter

This chapter's last section emphasizes how important consensus algorithms are to decentralized systems. Although the Control Algorithm has the potential to revolutionize proximity marketing, it also recognizes the persistent difficulties and constraints that these fields entail. By combining a consensus system with an opt-in/opt-out mechanism, the Control Algorithm presents a novel strategy with the goal of giving users unparalleled control over their data exchanges with marketing campaigns. In addition to improving data security and transparency, this user-centric approach is in line with the changing legal frameworks intended to protect consumers' rights in the digital era. The Control Algorithm offers significant improvements despite resource restrictions and implementation complexity. It promotes more engaged user experiences through tailored interactions, improves data security by letting users set terms of data usage and consent, and provides insightful information about consumer behavior that may be used to expand a business and develop targeted marketing campaigns. In the long run, the Control Algorithm can be seen as a driving force behind innovation in consensus mechanism creation and study. Researchers and practitioners can further improve user interaction, data privacy, and business intelligence in proximity marketing and other domains by continuously improving its functions. The Control Algorithm is a monument to invention that guides us through the ever-changing terrain of decentralized systems and points us in the direction of a future where user empowerment is enhanced and digital interactions are more private.

Chapter 6

Contribution 3: Classifying Proximity Marketing Actors and Establishing Interaction Levels through Consensus

This chapter presents a consensus framework that categorizes consumers, merchants, and proxy devices and defines levels of interaction in order to improve trust and collaboration in proximity marketing. The paradigm emphasizes user permission and data control while striking a balance between privacy concerns and engagement. It addresses both technical integration and concerns by fostering more individualized, transparent, and trustworthy proximity marketing encounters through the establishment of clear roles and safe communication.

6.1 Introduction

Businesses are under more and more pressure in today's dynamic economy to change quickly in order to satisfy customers' changing needs and preferences. Customized experiences and on-demand services are driving a redefining of classic marketing methods in consumer behavior. In this context, proximity marketing has become a vital tool that uses location-based technologies to target consumers with promotions and messaging during crucial decision-making times. With proximity marketing, the one-size-fits-all strategy of mass marketing is replaced with a more intricate and customized interaction model. Businesses may send customized content and promotions at the exact moment and area where they are most likely to impact customer decisions by leveraging the power of mobile devices and location data. In addition to improving consumer engagement, this quick, context-aware approach makes it easier for meaningful interactions to occur at critical times, including in-store visits or close to a point of sale [108, 148].
Proximity marketing has the potential to transform marketing tactics, but it faces a number of significant obstacles that prevent it from being widely used and optimized across industries. The difficulty of efficiently utilizing location-based data and technologies to provide personalized information is one of the biggest obstacles. Preciseness and contextuality are necessary in proximity marketing, as opposed to broad methods to mass marketing that aim to draw in customers. To do this, one must possess a thorough comprehension of consumer behavior patterns, real-time data analytics skills, and the capacity to provide content that speaks to the unique needs and preferences of each individual. The quick speed at which technology is developing presents another difficulty. Since proximity marketing platforms and tools are always changing, it can be challenging for companies to stay up to date on the newest developments and incorporate them easily into their marketing plans. In addition to driving up implementation costs, this technological complexity necessitates ongoing training and adaptability for marketing teams.

6.1.1 The Impact of Uncategorization

One major obstacle compounding these difficulties is the lack of a scientifically accepted classification system for proximity marketing tactics. A disjointed foundation obstructs advancement in several ways:

1. **Design and Optimization of Strategies:** In the absence of a well-defined taxonomy, companies find it difficult to develop focused proximity marketing strategies that complement certain customer categories and corporate goals. This restricts the efficacy of marketing campaigns and causes inefficiencies in the distribution of resources.

2. **Evaluation and Benchmarking:** Comparing performance metrics from various proximity marketing campaigns is made more difficult by the lack of established categories. This makes it more difficult to assess campaign success objectively and makes it more difficult to find best practices.

3. **Scholarly and Practical Research:** In terms of academia, the lack of a classification system inhibits scholarly investigation and thorough research on proximity marketing. It restricts the creation of theoretical models and empirical research that could deepen knowledge and spur innovation in the area. In practical terms, this limits companies' capacity to derive valuable insights from scholarly research and utilize them to enhance their marketing tactics.

6.1.2 Addressing the Gap with a New Framework

This study presents a novel paradigm that is intended to systematically classify proximity marketing tactics in response to these problems. The framework, which consists of three different scales

(**GlobHub, ZoneLink, and NearbySync**), attempts to give the complicated world of proximity marketing interactions some structure and clarity. Each scale offers a thorough method for formulating and assessing strategies by concentrating on distinct elements of the marketing ecosystem, such as merchant-proxy connections and prospect engagement. This framework aims to enable organizations to more skillfully manage the complexity of proximity marketing by providing explicit categories and evaluation criteria. It seeks to improve campaign effectiveness measurement, encourage innovation in proximity marketing techniques, and help better align marketing strategies with consumer preferences. We will examine each scale of the framework in detail in the sections that follow, describing its elements, approaches, and real-world applications. We will illustrate the framework's usefulness in resolving the issues raised by proximity marketing's existing lack of classification through empirical analysis and case studies, opening the door for improved strategic decision-making and customer interaction.

6.1.3 Research Questions

The following research questions are addressed in this chapter to help direct the investigation and analysis:

1. How can the main players in proximity marketing interactions be properly categorized, and who are they?
2. In what ways may proximity marketing initiatives be organized in organized manner to help with strategy design, benchmarking, and effectiveness assessment in various scenarios?
3. Which classification schemes are suggested for real-world proximity marketing uses and limitations?

6.2 Key Players in Proximity Marketing

This section explores the hierarchy of proximity marketing and the main characters in the Proximity Marketing domain to give a comprehensive understanding of its structure. Essentially, proximity marketing uses location-based **technologies** to create direct, contextually relevant connections between **brands** and their **target audience** at the intersection of physical spaces and digital interactions.

Prospects Level:

These companies or groups use proximity marketing strategies in an effort to interact with **possible clients**. This interactive canvas allows users to actively customize their proximity marketing experience. Customers choose products based on their preferences, which leads to lively exchanges. By giving customers more choices and providing businesses with valuable data to personalize offers, this level promotes collaboration and long-lasting partnerships.

Intermediate Level:

The platforms and technology known as "**proxy tools**" are those that enable proximity marketing interactions. Businesses can interact with customers depending on their physical proximity using *beacon technology*, *geofencing*, *Bluetooth Low Energy (BLE) devices*, *mobile apps*, and other technologies.

Merchants Level:

This layer serves as the strategic center and shapes broad marketing goals and objectives. It acts as a decision-making furnace where businesses mold their strategies to maximize the possibilities of proximity marketing. The Business Level directs proximity marketing toward harmonious integration with business goals, crafting a persuasive story that balances short-term customer satisfaction with long-term brand advancement.
Like different threads, these three levels skillfully tell the proximity marketing tale, producing an amazing symphony that, as Figure 6.1 showed, represents the dynamic dance of elements needed to forge lasting connections in the ever-evolving market.

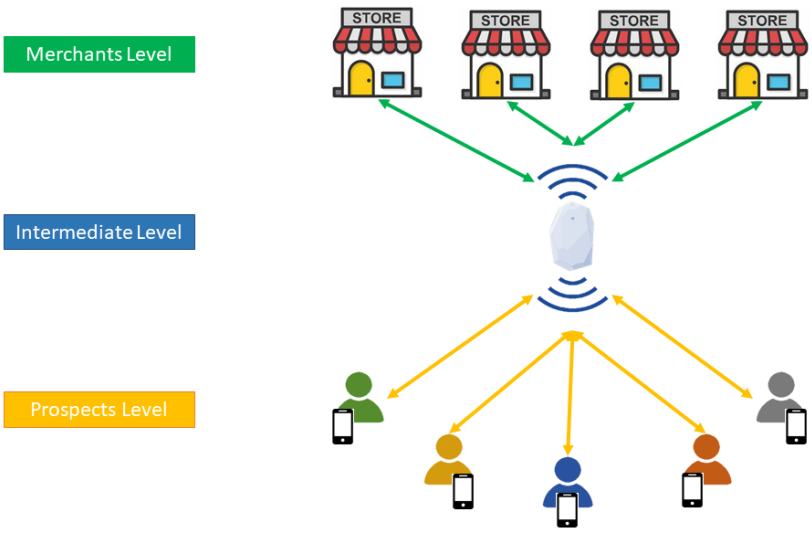


Figure 6.1: Implementation of Proximity Marketing Levels

6.3 Proximity Marketing Category Criteria

We outline the basic principles that underpin our classification of proximity marketing based on layers of the industry and emphasize the critical elements that impact how distinct classes are distinguished from one another. These criteria serve as the assessment metrics that help us categorize and assess proximity marketing strategies effectively. In addition to drawing on established theoretical frameworks, the developed criteria are specially tailored to address the unique challenges and opportunities inherent in the contemporary marketing landscape. Like the brushstrokes on a beautiful painting, we meticulously lay out a set of guidelines while creating the theoretical framework for our proximity marketing framework to capture the subtleties of this dynamic landscape. These criteria provide a guide for our research and categorization of proximity marketing strategies, which are firmly grounded in both existing theoretical frameworks and the unique challenges of the contemporary marketing environment.

Localization:

Localization, which captures the intrinsic spatial targeting and regional distinctiveness of proximity marketing, is one of the main requirements. Our paradigm prioritizes three distinct levels of localization:

- **Local:** adapting interactions to the existing context and adding a personal, small-scale touch.

- **Regional:** operating on a broader regional scale while addressing a particular geographic clientele.
- **Global:** using proximity marketing to interact with a range of international communities and reach a larger audience globally.

Temporal Aspect:

A dynamic metric that looks at the temporal facets of proximity marketing strategies is the temporal component. It evolves over three distinct time horizons:

- **Real-Time:** Including immediate, suitably contextualized encounters where businesses speak with clients directly.
- **Batch-Time:** concentrating on specific groups within set time constraints in order to maximize interactions for specific time-sensitive initiatives.
- **Strategic-Time:** adhering to key business timelines and ensuring that proximity marketing campaigns complement overarching business goals.

Audience Scope:

In proximity marketing, the audience scope criteria become critical since they look at the specificity and depth of the target market. It classifies audience involvement into three groups:

- **Individual:** identifying and meeting the unique needs of every client; tailoring interactions to provide unique experiences.
- **Group:** fostering a sense of camaraderie among specific clientele groups that share characteristics or passions.
- **Community:** identifying and addressing the wants and preferences of a larger audience by extending one's reach into more facets of the community.

Communication Technologies:

The communication technology requirements specify the channels and methods used for proximity marketing engagements. This criterion for communication technologies separates three levels:

- **Direct:** By using Bluetooth Low Energy (BLE) for tailored communication, businesses may communicate directly with consumers in the vicinity.
- **Edge:** delivering targeted, efficient interactions that ensure prompt and precise communication at the edge of the network through the use of edge computing.
- **Network:** interacting with a larger audience and expanding the reach and scope of proximity marketing efforts by utilizing network technologies like WiFi, 5G, etc.

Criteria Volume:

Criteria volume is used to gauge the proximity marketing campaign's reach and intensity (table 6.1). It represents the number of preferences the client sets into consideration and it can distinguish between three volume levels:

- **Limited:** implementing a focused approach in specific situations, suitable for limited stores and areas.
- **Moderate:** communicating with people on a reasonable frequency and breadth to strike a balance between concentrated and wide connections, suitable to stores with branches, where the preferences of clients could be specified based on moderate criteria.
- **Extensive:** where we are talking here in hundreds of preferences since we are working with worldwide companies.

Table 6.1: Criteria of Proximity Marketing Categories

Criteria	**Options**
Localization	- Local - Regional - Global
Temporal Aspect	- Real-Time - Batch-Time - Strategic-Time
Audience Scope	- Individual - Group - Community
Communication Technologies	- Direct - Edge - Network
Criteria Volume	- Limited - Moderate - Extensive

When taken as a whole, these specifications meticulously lay the foundation for our framework, providing us with a structured lens through which to categorize and assess proximity marketing strategies. Every criterion offers a degree of precision and is theoretically sound, enabling a more in-depth analysis of the numerous and constantly evolving facets of the proximity marketing landscape. This systematic approach not only enhances our understanding but also provides a more in-depth and insightful analysis of the dynamics that are evolving within proximity marketing strategies.

6.4 Proximity Marketing Categorization

Because of the intricacies of the proximity marketing sector as we discussed before, a formal framework is necessary to comprehend all of the different ways that businesses engage with their target audience. Here, we descend the classification ladder and divide proximity marketing strategies into three distinct, useful scenarios: **NearBySync**, **ZoneLink**, and **GlobeHub**. Our categorization efforts aim to map this landscape, providing a structured view that enables us to discern the tiny differences between each strategy. Each category represents a unique facet of proximity marketing, capturing the spirit of tailored encounters in a variety of physical, temporal, and audience contexts. As we look at each sector, we throw light on the specific ways businesses utilize proximity marketing strategically to enhance customer experiences, influence consumer decisions, and support long-term brand success.

6.4.1 Among Prospects: NearBySync

NearBySync, the locally tailored variant of proximity marketing, emphasizes highly personalized, real-time advertising through direct communication methods. It concentrates on specific geographic regions and uses a consensus-building strategy that takes individual preferences into consideration to generate customized offers for each customer. It instantly adjusts offerings while operating in real-time, encouraging client consensus and ensuring adaptable responses to changing audience needs and opinions. It carefully attends to each client's unique needs using an individual-scale approach, resulting in highly customized marketing campaigns that prioritize accuracy. Direct and tailored interactions between users and the system are emphasized by the Direct Communication Scale, which makes use of technology such as mobile applications for instant consensus development. A smaller number of predetermined standards are taken into consideration when the system is functioning at the Limited Criteria Scale, which streamlines and enhances the consensus-building process. A *boutique* environment is used to illustrate the proximity marketing system (Figure 6.2-a). It sends personalized offers over secure channels and privacy-preserving features after using a consensus process to determine each customer's distinct preferences. Customers can interact with one another to express their preferences and ideas as well as to approve the best deals. Continuous refinement through customer feedback guarantees a tailored and dynamic marketing experience.

6.4.2 Between Prospects and Proxies: ZoneLink

ZoneLink is a regional player in the proximity marketing space that uses marketing strategies for client groups that rotate at set intervals, or batch periods. This scale leverages edge technologies such as WiFi, 5G, and GPS and targets larger regions such as retail complexes or car shops. Reaching an intermediate agreement at the level of an aggregation point, where a plurality of client preferences are taken into account to develop personalized products that appeal to a wider spectrum of regional consumers, is the key to successful regional localization. Operating in batches, offers are updated often, and consensus is consistently reached by considering the preferences of multiple clients. Community-scale marketing includes targeting user communities or groups with shared interests, meeting their preferences, and cultivating relationships within these groups. Focusing on user communities or groups with shared interests, accommodating their preferences, and fostering relationships within these community dynamics are all part of community-scale marketing. The optimization of local preferences at the Edge Communication Scale is highlighted by the communication made possible by edge devices like the Raspberry Pi. The algorithm on this scale ensures a convoluted process of consensus-building by carefully taking into account a fair amount of criteria on the Moderate Criteria Scale. To balance customer preferences and the overall car-buying experience, the Intermediate Level, for instance, gathers client preferences and adjusts offers based on aggregated data in Figure 6.2-b *Automobile* shops.

6.4.3 Among Marchants and Proxies: GlobeHub

GlobeHub operates on a worldwide scale in proximity marketing and strategically makes judgments over a long period using wide network technologies. This size, which focuses on large markets like real estate, requires firms or organizations to reach agreements and consider many customer points of view in order to construct complex plans that are tailored to global dynamics. On the strategic-temporal scale, priorities shift to encompass long-term planning, marketing strategy modifications, and the formation of strategic consensus over an extended period of time based on insights and trends. Consensus building at the local level for larger groups, like companies, involves adaptable marketing techniques molded by information obtained from a wider perspective. The Network Communication Scale highlights the importance of networked communication channels, which

allow for smooth information transmission amongst proximity marketing system components. At the Broad Spectrum of Components. At the Extensive Factors Scale, reaching consensus requires considering a wide range of factors, which allows the system to assess a wide range of criteria for a comprehensive understanding of complex client preferences. The proximity marketing approach, which is demonstrated by *real estate* retailers in Figure 6.2-c, is centered on using aggregated data to produce business-level insights and make strategic decisions while utilizing blockchain technology to preserve individual privacy and data transparency. This gives businesses the ability to keep control over customer data while learning important strategic information.

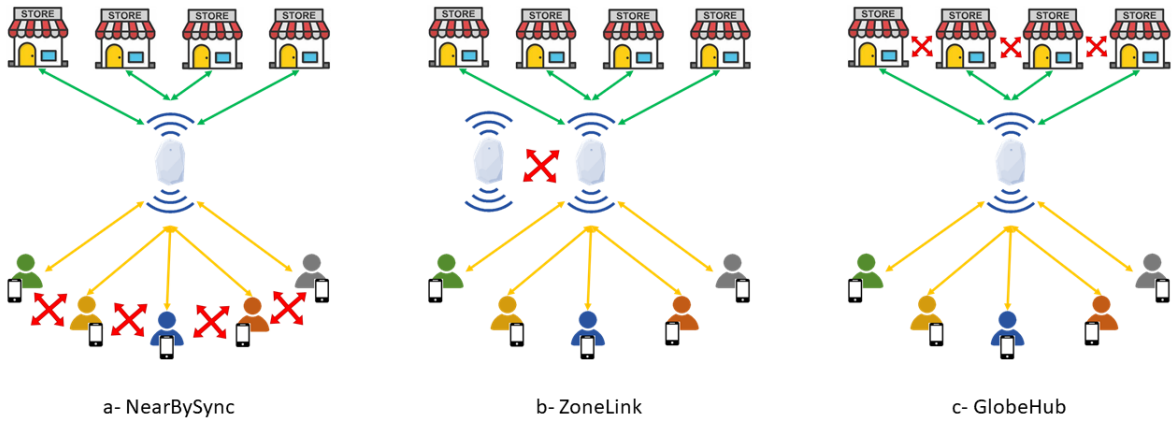


Figure 6.2: Illustrative of Proximity Marketing Scales

Table 6.2 provides a concise summary of the primary topics covered by proximity marketing strategies. A thorough description of the distinct location, temporal characteristics, audience scope, communication technology, and criterion volume associated with each of the three classes—NearBySync, ZoneLink, and GlobeHub—is provided in the table. This category offers a convenient way for businesses to quickly understand the several approaches they may take to tailor their proximity marketing strategy.

Table 6.2: Comprehensive Examination of Proximity Marketing Categories

	NearBySync	**ZoneLink**	**GlobeHub**
Localization	Local	Regional	Global
Temporal Aspect	Real-Time	Batch-Time	Strategic-Time
Audience Scope	Individual	Group	Community
Communication Technologies	Direct	Edge	Network
Criteria Volume	Limited	Moderate	Extensive
Example	Boutique stores	Automobile stores	Real estate stores

6.5 The advantages

The following are the benefits of classifying proximity marketing into these three categories:

Clear Segmentation:

Businesses can more effectively identify and target various audience categories by breaking down proximity marketing into three distinct levels: NearBySync, ZoneLink, and GlobeHub. Businesses

can more successfully adjust their marketing tactics to the unique requirements and preferences of their target audience by using each level to symbolize a distinct scale of operation and involvement.

Enhanced Personalization:

Marketing initiatives can be made more individually tailored at every level of categorization. ZoneLink uses batch-based marketing methods to target bigger area groups, while NearBySync concentrates on personalized, real-time contacts with prospects. GlobeHub is a global platform that enables companies to connect with a wide variety of consumers across the globe. Businesses can develop better audience-resonant marketing strategies that are more relevant and engaging by utilizing this hierarchy of customization.

Optimal Resource Allocation:

Businesses can manage their resources more effectively by classifying proximity marketing into distinct degrees. Businesses might, for instance, concentrate their energies and resources on NearBySync for local targeting, use ZoneLink for regional campaigns, and utilize GlobeHub for global endeavors. This methodical distribution reduces expenses and wasteful use of resources while optimizing the results of marketing initiatives.

Enhanced Consensus Building:

Various stakeholders, including prospects, proxies, and merchants, collaborate to reach a consensus at each categorization level. ZoneLink concentrates on regional consensus, GlobeHub on global consensus, and NearBySync on individual consensus development. Businesses and their target audience are able to build stronger relationships as a result of this strategy, which increases engagement, loyalty, and trust.

Scalability and Flexibility:

Companies of all sizes and sectors can benefit from the scalability and flexibility provided by the three categories. There is a level of categorization that works for a firm, regardless of how big or small it operates. Because of its scalability, proximity marketing methods may be modified by firms as they expand and change, guaranteeing that their target market will continue to be reached.
All things considered, proximity marketing's three classifications provide companies with an organized framework for organizing and carrying out their marketing campaigns, which enhances their efficacy, efficiency, and client happiness.

6.6 The restrictions:

Although the division of proximity marketing into NearBySync, ZoneLink, and GlobeHub categories has many benefits, there are certain restrictions to take into account.

Complexity:

It can be difficult and resource-intensive to implement and manage proximity marketing campaigns at many categorization levels. To effectively use proximity marketing solutions, organizations need both the technical know-how and a thorough understanding of their target demographic.

Cost:

Creating and implementing proximity marketing programs can be expensive, particularly when done at the ZoneLink and GlobeHub levels. It can necessitate spending money on marketing materials, data analytics software, and IT infrastructure, which is not always possible for smaller companies with tighter budgets.

Privacy Concerns:

In order to provide individualized experiences, proximity marketing depends on gathering and evaluating consumer data. Customers may, however, become concerned about their privacy as a result, especially in light of the gathering and use of location data. When collecting and using customer data, businesses must guarantee consent, transparency, and strict adherence to privacy standards.

Technical Difficulties:

Setting up proximity marketing campaigns may provide technical difficulties with data accuracy, device compatibility, and connectivity. These difficulties may compromise the dependability and efficiency of proximity marketing campaigns, necessitating financial investments and specialized knowledge from companies.

Limited Reach:

Compared to traditional marketing channels, proximity marketing may have a smaller reach, despite the fact that it can be very personalized and focused. Customers might not always be in close vicinity to the business's location or its gadgets, and those who do might not always choose to receive proximity-based marketing.

Competition and Saturation:

Businesses may experience heightened competition and saturation in their target areas when proximity marketing gains traction. Due to this, firms may find it more difficult to distinguish from the competition and draw in their target market, which could result in lower returns on investment.

Dependency on External Factors:

The success of proximity marketing initiatives frequently depends on outside variables like consumer behavior, industry trends, and local environmental circumstances. The success of proximity marketing initiatives may be impacted by changes in these variables, so companies must continuously assess and modify their plans as necessary. All things considered, proximity marketing has many advantages, but in order to fully realize the potential of their campaigns, companies need to be conscious of these constraints and take proactive steps to overcome them.

6.7 Privacy-Driven Consensus Mechanisms

Strong privacy protection techniques are essential in proximity marketing because of the widespread use and gathering of personal data, as covered in Chapter **??**. In response to worries about data sensitivity, businesses are progressively using cutting-edge technologies that greatly improve privacy protection by facilitating large-scale consensus among nodes and providing secure, transparent consent management [16, 76, 110]. In addition to building consumer trust, this strategy complies with changing legal constraints and moral data standards for advertising campaigns.

Explicit and secure consent management is required for proximity marketing, which uses location and other sensitive user data for tailored advertising. Despite being widely employed, standard opt-in/opt-out processes are unable to offer the required security and accountability [18, 63, 64]. Customers may become distrustful of these systems due to their lack of transparency regarding data gathering, utilization, and sharing [91, 131, 147]. Furthermore, they do not provide exact control over choices for data sharing, which is important considering how sensitive location-based data [43]. The efficacy of opt-in/opt-out procedures may be further undermined by users' perceptions of coercion to agree to data gathering in exchange for services or discounts [29, 124]. Compliance monitoring and enforcement are made more difficult by these procedures' lack of audibility and accountability, particularly in the event of data breaches or misuse [137].
Consensus algorithms must be used in order to overcome these drawbacks and create a strong foundation for controlling user permission in proximity marketing. By enabling all network users to agree on protocols, consensus techniques offer transparent, accountable, and compliant consent management [19, 104, 132]. This can support moral data practices, reduce privacy worries, and increase customer trust.
Consensus algorithm research in proximity marketing highlights the need for reliable and open solutions to protect user privacy and advance moral data practices. A transparent and safe framework for managing user data is provided by algorithms like Paxos, Raft, and PBFT, which solve the particular difficulties of proximity marketing contexts. Their benefits—reliability, transparency, and simplicity—make them a good fit for consent management in various contexts. Businesses may increase client trust and confidence in their marketing initiatives while maintaining regulatory compliance by utilizing these technologies.

6.8 Implementation in Proximity Marketing

We will experiment with several consensus processes in order to examine the efficacy of multiple consensus algorithms in proximity marketing contexts. Our proximity marketing system has selected a set of consensus algorithms for implementation based on their prospective applicability, diversity, and usefulness. Through this comparison study, we want to get valuable insights into the scalability, robustness, and performance of each algorithm in our operational setting. Putting each consensus method to use and observing its performance in our neighborhood will allow us to assess its merits, limitations, and suitability for our specific use case. We simulated clients and offers in each scenario using the Python programming language in order to accomplish this. This beneficial tactic will provide us with relevant empirical data to effectively guide our decision-making process. Through this comparison analysis, we were able to enhance the consistency and effectiveness of our proximity marketing model while providing valuable insights into the debate surrounding consensus algorithm selection and evaluation in proximity-based systems. Through the dissemination of our study, we hope to help businesses make educated decisions when they encounter similar challenges in proximity marketing and related fields.

6.8.1 Message Queuing Telemetry Transport (MQTT)

We have integrated our proximity marketing communication platform with MQTT, a lightweight, open-source messaging protocol. MQTT is designed to provide efficient device-to-device communication, particularly in environments with limited resources such as inadequate bandwidth or elevated latency. Given that MQTT employs an asynchronous client-server messaging system, it is an ideal choice for our needs [12, 127, 138]. To facilitate structured communication between businesses and clients, we have included three main topics in our MQTT framework:

- **Publish:** Offerings are introduced in this topic. In this instance, publishers market specials

and "Buy 1, Get 1 Free" days to potential clients.

- **Rate:** After receiving an offer, clients have a little window of time to determine whether or not it is relevant or desirable. Customers utilize the "rate" subject to express their level of satisfaction with the offer within a predetermined window of time.
- **Decision:** Based on the majority rating, a choice is made regarding whether to accept or reject the offer. If a consensus is established, the offer is accepted. However, if it does not meet the cutoff, the offer may be revised or reassessed in light of feedback from the customer.

By leveraging MQTT in proximity marketing, we hope to reach a consensus over offers without needing to pursue individual clients. By leveraging the efficient messaging features of MQTT and the well-established topics of publish rate and decision, we can facilitate seamless communication between businesses and their customers while protecting customer privacy [7, 135, 141]. The consensus algorithms that can be used to ensure fair and efficient decision-making processes are Paxos, Raft, and PBFT. These algorithms take into account the ratings that customers submit throughout the designated period while deciding whether to approve an offer overall. By applying consensus algorithms, we can adapt to various scenarios and customer preferences, which will improve the effectiveness of our proximity marketing initiatives (figure 6.3).

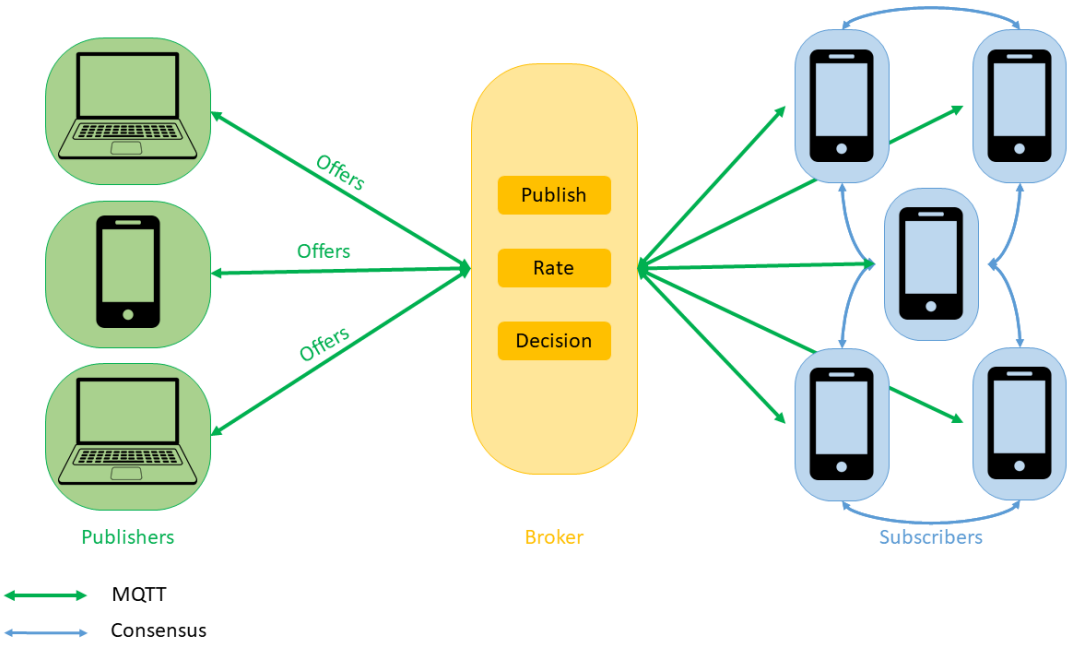


Figure 6.3: MQTT with consensus

To sum up, MQTT serves as the cornerstone of our proximity marketing communication protocol, enabling transparent, efficient, and confidential communication between companies and their customers. Our objective is to get permission over offers in a trustworthy and fair manner without compromising individual privacy by employing a variety of consensus mechanisms.

6.8.2 Paxos

In order to ensure consensus among businesses and customers and to speed up decision-making processes, we have included the Paxos consensus algorithm into our proximity marketing system.

Paxos is well known for being resilient and fault-tolerant, making it the perfect choice for distributed systems like ours where several entities must agree on a single value even in the case of network outages or partitions. To initiate the proposal phase, publishers broadcast offers to potential customers using the "publish" topic provided by the MQTT architecture. These offers, which could also contain details about specials or discounts, function as proposals in the Paxos protocol. Publishers promote the acceptance of specific offerings in their capacity as proposers.
Within a certain period of time after receiving an offer, clients evaluate its desirability. Consumers express their level of satisfaction with the transaction using the "rate" subject. These ratings serve as approvals or rejections of the proposal, much like the acceptor role does in the Paxos protocol. At the conclusion of the rating period, the Paxos consensus procedure is used to determine whether the offer is widely accepted or rejected. This phase is covered under the "decision" topic. This is the usage of Paxos: Stage of preparation: Depending on the ratings they have received, clients acting as proposers begin the consensus process by preparing messages that outline a specific offer. These messages can be sent over MQTT so that everyone is aware of the concept.

- **Promise Phase:** Acceptor clients respond to the prepared messages by acknowledging the proposal if they have not previously committed to accepting a proposal with a higher number. By guaranteeing that all acceptors are aware of the most current proposal, this step prevents disputes.
- **Accept Phase:** Following the acquisition of a quorum of commitments, the proposer client sends accept messages to signal that the proposal has been accepted by a sufficient number of acceptors. The accepted offer is now accepted as genuine, and the decision-making process is finished.
- **Learn Phase:** Lastly, clients are informed about the choice made by the Paxos algorithm. This information is distributed using the MQTT "decision" topic. This ensures that each client is aware of the chosen offer and is able to react accordingly.

To characterize the conditions for obtaining consensus inside the Paxos algorithm, we employ two fundamental formulations that encapsulate its essence:

Consensus Condition Formula:

$$\forall c, d \in \text{rounds}, \text{if chosen}(c) = v \text{ and chosen}(d) = w \text{ then } v = w$$

This formula ensures consistency across all rounds of the Paxos algorithm, stating that if a value v is chosen in round c and a value w is chosen in round d, then v must be equal to w.

Quorum Intersection Property Formula:

$$\forall Q_1, Q_2 \subseteq \text{Acceptors}, \left(|Q_1| > \frac{2}{N} \text{ and } |Q_2| > \frac{2}{N} \right) \implies Q_1 \cap Q_2 \neq \emptyset$$

The safety of the Paxos protocol depends on this formula's definition of the quorum intersection property, which guarantees that any two quorums of acceptors share at least one common acceptor. By integrating Paxos with MQTT, we enable dependable and robust decision-making in proximity marketing. The robustness of Paxos and the efficiency and portability of MQTT work together to facilitate seamless communication and agreement between companies and clients without compromising reliability or performance.

6.8.3 Raft

Every node in the system must concur on the current state of a replicated log, which is ensured using a distributed system consensus process known as Raft. Raft allows customers and businesses to decide together whether to accept or reject offers while maintaining consistency and fault tolerance in proximity marketing with MQTT. Here's an illustration of how to utilize Raft: Raft nodes can assume three different roles: leader, follower, or candidate. It is possible to think of each customer and business engaged in proximity marketing communication within the MQTT network as a node, with the ability to do these tasks. Raft employs a leader election technique to ensure that, at any given moment, only one leader node is in charge of supervising the distributed consensus procedure. To choose a new leader, nodes exchange a number of messages with one another. Consumers and companies that use the MQTT framework for proximity marketing subscribe to particular topics (publish, rate, decision), and use the Raft protocol to exchange messages with one other.
Every node in Raft maintains a duplicate log in order to maintain consistency. When a client rates an offer using the "rate" topic, the rating is appended to the log and replicated across the network. MQTT's publish-subscribe structure ensures timely updates to all nodes and facilitates rating sharing. The leader node uses the replicated log to facilitate consensus decision-making at the conclusion of the rating period. Raft ensures that all nodes eventually arrive at the same conclusion even in the event of network splits and node failures. The leader node uses Raft's consensus process to assess client ratings and determine if the offer is approved or denied by the majority of nodes. The "decision" notifies every node about this decision topic in the MQTT network.
Raft provides fault tolerance by allowing the network to continue operating even in the case of a few nodes experiencing failures or becoming unavailable. In the event that a node fails, Raft initiates the process of re-electing leaders in order to keep the consensus process going. Fault tolerance is further enhanced by MQTT's resistance to network disruptions, ensuring stable client and business communication even in difficult situations.
Raft's primary characteristics can be formally expressed to clarify its operation. Raft uses two fundamental formulas—the consistency property and the consensus condition—to maintain log consistency and agreement across the cluster.

Consensus Condition Formula:

$$\forall i, j \in \text{LogIndex}, \text{if } \log[i] = x \text{ and } \log[j] = y \text{ then } i = j \implies x = y$$

This formula ensures that for all log indices i and j, if the log entry at index i is x and the log entry at index j is y, then if i equals j, it implies that x must equal y. This ensures that each log index holds a unique command, and all nodes in the cluster replicate the same log sequence.

Consistency Property Formula:

$$\forall i \in \text{CommittedIndex}, \forall n \in \text{Nodes},$$

if $\log_n[i]$ is committed, then $\forall m \in \text{Nodes}, \log_m[i] = \log_n[i]$

The committed log index is denoted by i, the cluster nodes are represented by n and m, and the log entry at index i in node n's log is represented by $\log_n[i]$. When a log entry is committed at a specific index in a node's log, it also appears in the logs of all other nodes that have entries up to that index, thanks to this characteristic that guarantees consistency across the replicated logs.
By combining Raft's consensus approach with MQTT, we can create robust and fault-tolerant decision-making processes in proximity marketing without compromising scalability or performance.

Raft's simplicity and efficacy make it a viable choice for use cases where distributed agreement is required, such as choosing offers in proximity marketing scenarios.

6.8.4 PBFT

PBFT is designed to converge a dispersed network of nodes to consensus even in the presence of malicious or broken nodes. It works in situations where Byzantine faults, such as malicious attacks or node failures, could occur because it is predicated on the idea that a certain percentage of nodes may act erratically or malfunction. The PBFT protocol consists of several steps, including pre-preparation, preparation, commit, and execution. Network nodes cooperate to process transactions, verify their authenticity, and determine the optimal order in which to complete them. Again, MQTT serves as the foundation for communication in our proximity marketing system, promoting information exchange and customer involvement. To ensure agreement on accepting or rejecting offers without endangering client privacy, PBFT is employed in this framework.

- **Phase of Preparation (Publish):** To initiate the process, publishers broadcast offers to customers using the "publish" topic of the MQTT framework. Each offer is accompanied by a unique identity and digital signature to ensure its legality. Clients verify the validity of these offers after receiving them before proceeding to the next level.
- **Prepare Phase (Rate):** Clients utilize the "rate" issue to indicate their level of satisfaction and desirability upon receipt of an offer. In order to get a preliminary consensus about the validity of the offer and the associated rating, clients communicate with one another during this stage, using PBFT. Clients broadcast their ratings together with cryptographic evidence to prevent manipulation or tampering.
- **Commit Phase (Decision):** After the rating phase, clients confer with one another multiple times to decide whether to accept or decline the offer. PBFT ensures that clients make a final judgment about the offer's authenticity and whether or not to accept it altogether by utilizing the aggregate ratings. By broadcasting the choice via the "decision" topic, all parties can reach a synchronized state.

Let N be the total number of nodes, and f the maximum number of faulty nodes. A consensus is reached if at least $2f + 1$ nodes agree on a message or value. The system can tolerate up to f faulty nodes, where $f < \frac{N}{3}$.
In mathematical terms, the consensus condition for PBFT can be expressed as:

$$\forall m \in \text{Messages}, \exists S \subseteq \text{Nodes}, |S| \geq 2f + 1 : \forall n \in S, \text{agree}(n, m)$$

According to this formula, for every message m, there is a subset S of nodes such that S has a minimum size of $2f + 1$ and all of the nodes n in S agree on the message m. This guarantees that even in the presence of up to f faulty nodes, agreement will be obtained when a sufficient number of nodes agree on a message. In conclusion, by combining PBFT with MQTT in proximity marketing, we can ensure fair, trustworthy, and privacy-preserving decision-making processes. This will raise the overall effectiveness and legitimacy of our marketing campaigns.

6.8.5 CA

A key factor in enabling communication between the different Control Algorithm (CA) components is the MQTT framework. Through the utilization of MQTT, the system guarantees agreement among its constituents and facilitates the effective exchange of information. To handle consent communications, for example, particular subjects like "consent_request" and "consent_response" are used. These subjects encourage accountability and transparency by not just recording user

replies but also educating consumers about data gathering procedures. Important for data security, the "data_encrypt" subject makes sure that all data is encrypted before being stored, protecting user data and boosting confidence in the security mechanisms of the system.
The system's use of MQTT to manage user input is another essential component. The "feedback" subject is used to gather feedback, while the "evaluation" topic is used to share assessments of this feedback. The methodical gathering and analysis of user feedback is made possible by this structured methodology, and it is crucial for the system's ongoing improvement. Moreover, the "update" topic is used to spread real-time marketing updates. This makes it possible for marketing plans to be constantly modified in response to real-time data, improving the system's capacity to react and adjust to changing consumer preferences and behaviors.
Formal equations are utilized to define crucial components of the Control Algorithm, ensuring durable and trustworthy consensus. The Consent Consensus Formula is one such element that makes that every user's consent choice—whether to opt-in or opt-out—is appropriately documented. This formula guarantees that consent is obtained and properly documented, which is essential for protecting user privacy and data integrity. This is how the formula is expressed:

Consent Consensus Formula:

$$\forall u \in \text{Users}, c_u = \begin{cases} \text{opt-in} & \text{if } u \text{ consents} \\ \text{opt-out} & \text{if } u \text{ does not consent} \end{cases}$$

The Feedback Aggregation Formula, which correctly portrays the general sentiment by averaging individual feedback scores, is another essential element. By using this method, the system is guaranteed to be able to assess user happiness and make defensible decisions based on the information gathered. The following is the formula:

Feedback Aggregation Formula:

$$\forall f \in \text{Feedback}, A = \sum_{i=1}^{n} f_i/n$$

The individual feedback is represented by f in this formula, the number of feedback entries is indicated by n, and the aggregate feedback score is represented by A.
To summarize, the Control Algorithm's integration with the MQTT framework yields a user-centric, user-secure, and efficient proximity marketing system. Strong user consent management, safe data processing, and dynamic marketing modifications are made possible by this connection, which eventually raises user engagement and confidence. By fusing sophisticated algorithms with dependable communication frameworks like MQTT, this ground-breaking strategy raises the bar for morally sound and successful proximity marketing.

6.9 Evaluation

We used a sophisticated simulation environment written in Python to evaluate the effectiveness of consensus algorithms in the dynamic field of proximity marketing. With great attention, this environment was designed to mimic the many intricacies present in the NearBySync, ZoneLink, and GlobeHub levels. Within each tier, the consensus procedures were carefully adjusted to select and allocate offers from a pool of options to simulated clients (whose numbers varied from ten to one hundred fifty). Comprehensive experiments were carried out in a range of circumstances thanks to the flexible and durable Python-based simulation framework. Through the application of NumPy, Pandas, and Matplotlib, among other Python libraries, we were able to carefully control a multitude of variables, including client behaviors, network size, and communication latencies. This level of

detail ensured the legitimacy and depth of our assessments and allowed us to completely reflect the intricacy inherent in proximity marketing initiatives. The software for the simulation environment, analytic tools, and datasets are all publicly available on GitHub for repeatability and openness. This makes it easier for other researchers and practitioners to replicate our tests, validate our findings, and advance the design of cutting-edge consensus algorithms and proximity marketing. Throughout the simulation studies, a number of significant performance indicators were carefully monitored and investigated. These assessments included consensus time, consensus accuracy, and recovery time, among other things. These are important indicators of algorithmic efficacy and practical usefulness. We were able to gain valuable insights into the general performance characteristics, as well as the advantages and disadvantages, of each consensus method by carefully examining its performance under varied conditions and client configurations.

6.9.1 Consensus Time

Through meticulous documentation of time-stamped processes including proposal creation, message distribution, and decision-making, we were able to assess how well four consensus algorithms—Paxos, Raft, PBFT, and CA—performed in different network setups.
Our investigation showed that the consensus speed of each algorithm gradually decreased as the number of nodes in the network climbed from 10 to 150. All algorithms maintained reasonably moderate consensus speeds in spite of this decline.
With an average time of 120.2 milliseconds (ms), Paxos showed the fastest average consensus speed among the examined algorithms, especially when utilizing NearBySync technology. Raft trailed closely after at 137.4 ms, and PBFT at 145.2 ms. CA did well too, with an average time of 121.7 ms. Paxos once more attained the quickest consensus speeds in the ZoneLink and GlobeHub systems, with average times of 118.3 ms and 124.9 ms, respectively. With average times of 139.5 ms, 142.8 ms, and 118.9 ms under ZoneLink and 143.4 ms, 149.9 ms, and 126.1 ms under GlobeHub, respectively, Raft, PBFT, and CA came next (table 6.3).
These results show that, for all systems and network sizes examined, Paxos consistently performed faster in terms of consensus speed than Raft, PBFT, and CA. Even while CA had positive outcomes, it did not reach the fastest speeds. All algorithms maintained very moderate consensus speeds as the size of the network expanded, indicating their scalability for use in proximity marketing applications where network growth is expected (figure 6.4).

Table 6.3: Consensus Speed (ms)

	NearBySync	ZoneLink	GlobeHub
Paxos	120,2	118,3	124,9
Raft	137,4	139,5	143,4
PBFT	145,2	142,8	149,9
CA	121,7	118,9	126,1

6.9.2 Fault tolerance

Using the Paxos, Raft, PBFT, and CA consensus algorithms, we simulated scenarios involving node failures, message loss, and network partitions in order to evaluate fault tolerance in the NearBySync framework for proximity marketing applications. Evaluating each algorithm's resistance to various kinds of system failures was the main goal.
The outcomes showed that CA performed admirably in every situation where it failed. In particular, CA succeeded 94% of the time in managing network partitions, 96% in handling message loss, and

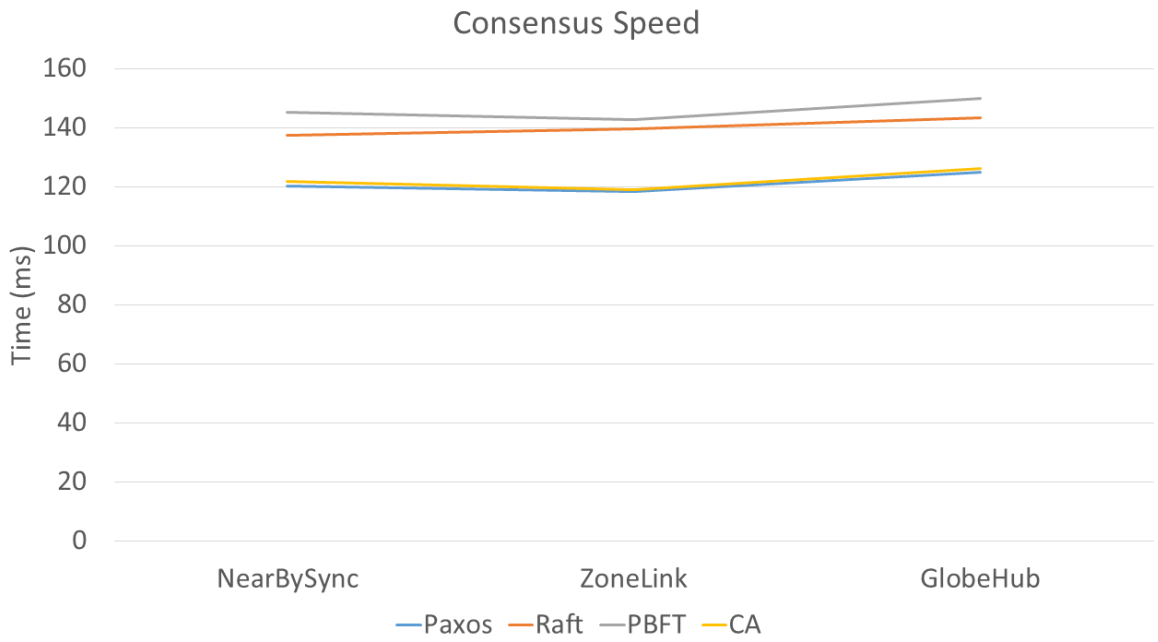


Figure 6.4: Consensus Speed

91% in addressing node failures. These results highlight CA's strong capacity to handle a variety of fault situations.
With success rates of 90% for node failures, 98% for message loss, and 90% for network partitions, Paxos also fared well overall, showing that it is still a very competitive choice. Raft and PBFT, in contrast, performed somewhat worse in each of these cases; Raft scored 95%, 94%, and 85%, while PBFT received scores of 85%, 90%, and 80
With its exceptional resilience to message loss and network partitions, CA stands out as a serious competitor for applications that demand high resilience. In settings where network conditions are dynamic and maybe unpredictable, CA offers a dependable way to guarantee data integrity and ongoing functioning. Because of its outstanding performance in all studied fault scenarios, it is the best option for proximity marketing applications where resilience and dependability are essential (figure 6.5).

6.9.3 Consistency of offers

The effectiveness of the consensus algorithms PBFT, Raft, Paxos, and CA in guaranteeing consistent acceptance and rejection of offers across a range of proximity marketing applications was assessed. The variation in offer reception rates is shown in Figures 6.6, 6.7, and 6.8. Based on the results, CA is clearly the most dependable choice for ensuring consistent offer reception in all of the circumstances that were examined. Regardless of the number of nodes or type of application, CA has demonstrated its capacity to maintain consistency by continually achieving high offer reception rates.
Raft fared well as well, frequently exhibiting offer acceptance rates that were either slightly greater than or equal to Paxos'. Raft is a good option for applications that need trustworthy offer acceptance and propagation because of its dependable performance. Even if Paxos was not as successful as Raft, it was still quite successful in terms of offer acceptance. By comparison, when it came to offer acceptance rates, PBFT constantly trailed behind CA, Raft, and Paxos. This shows that PBFT might have trouble continuing to receive offers consistently in proximity marketing environments and might use more improvement.

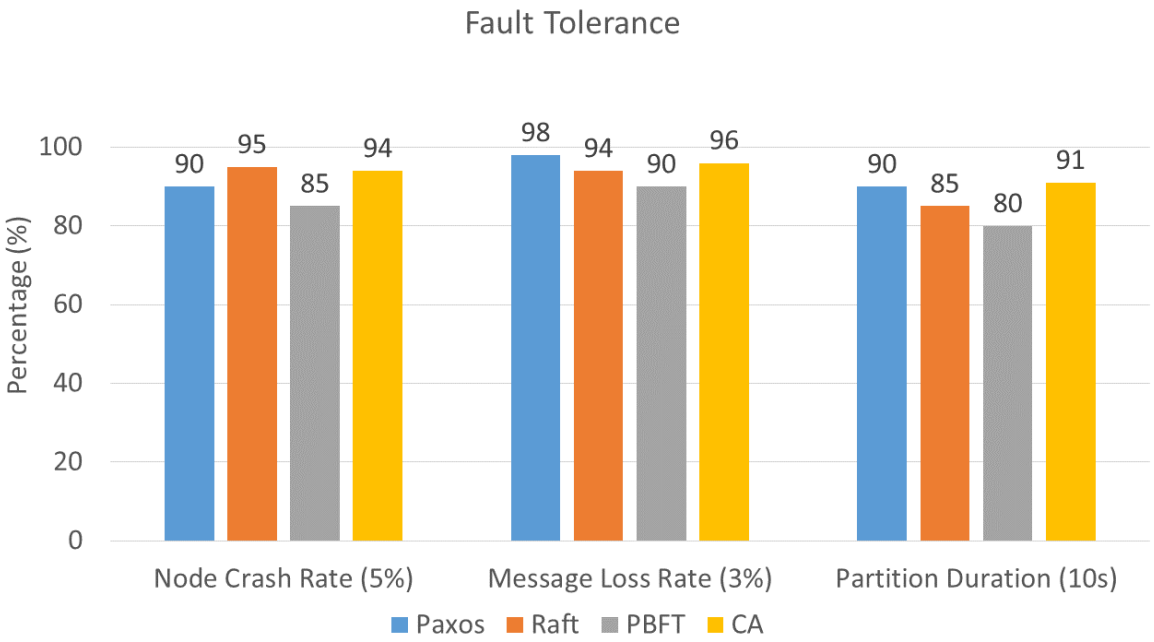
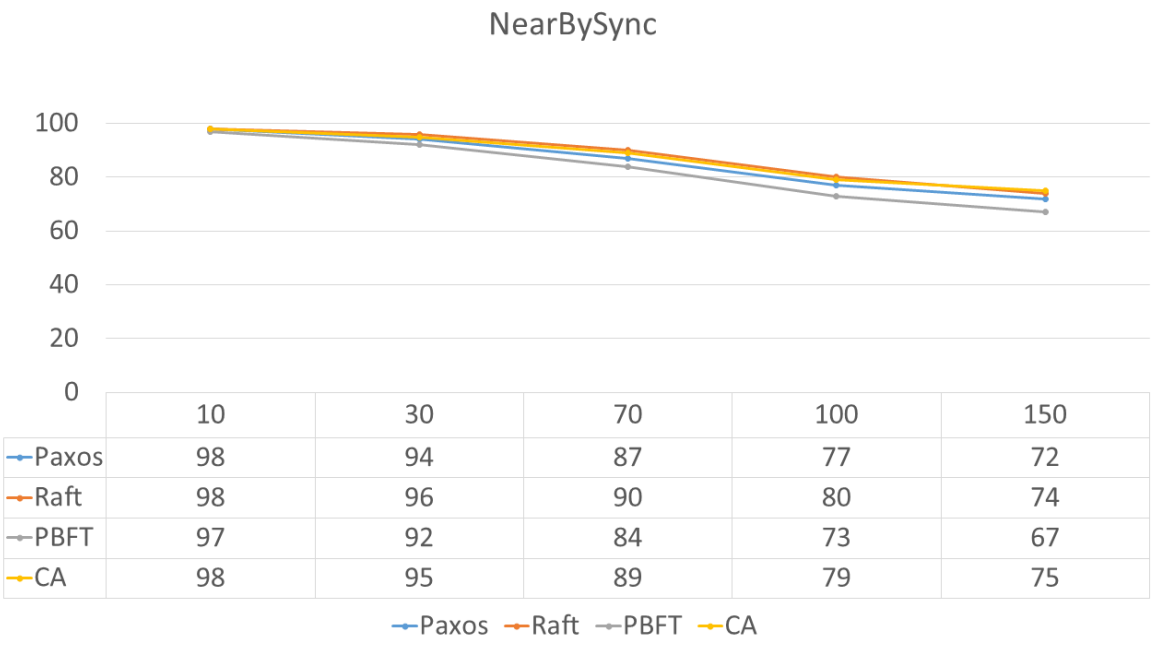


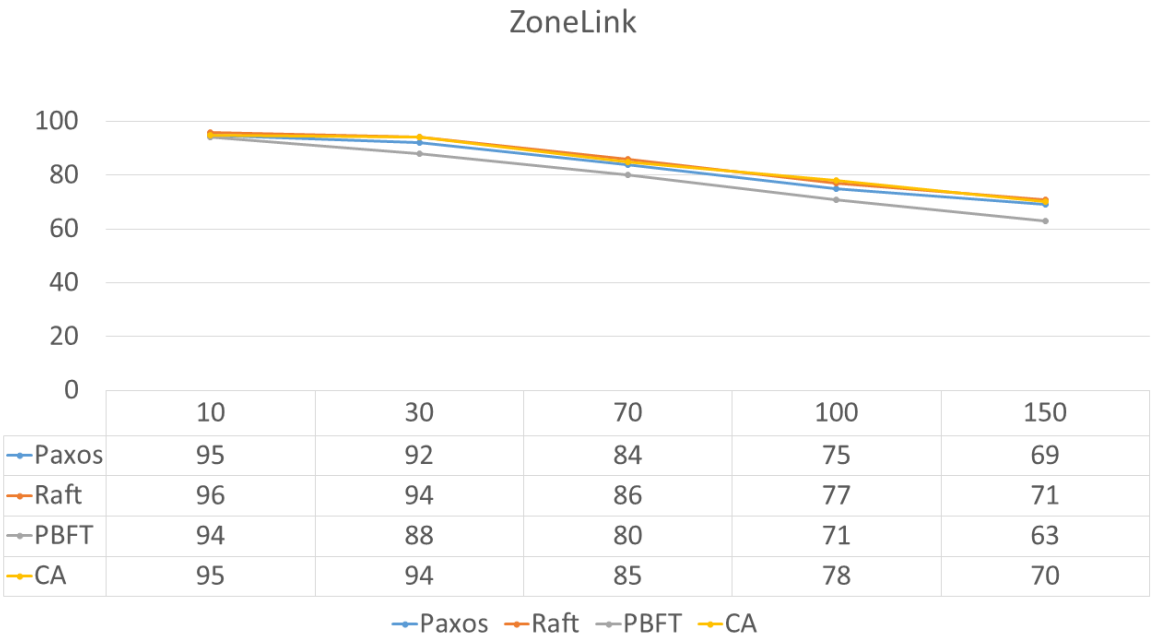
Figure 6.5: Fault Tolerance

All things considered, the results highlight how popular CA is as a consensus algorithm for proximity marketing applications because of its capacity to produce consistently high rates of offer reception under a variety of circumstances. Although Raft and Paxos are similarly efficient, CA is the most promising solution for guaranteeing dependable and consistent offer acceptance in dynamic situations due to its strong performance across a range of scenarios and node counts.



	10	30	70	100	150
Paxos	98	94	87	77	72
Raft	98	96	90	80	74
PBFT	97	92	84	73	67
CA	98	95	89	79	75

Figure 6.6: Consistency of Offer for NearBySync



	10	30	70	100	150
Paxos	95	92	84	75	69
Raft	96	94	86	77	71
PBFT	94	88	80	71	63
CA	95	94	85	78	70

Figure 6.7: Consistency of Offer for ZoneLink

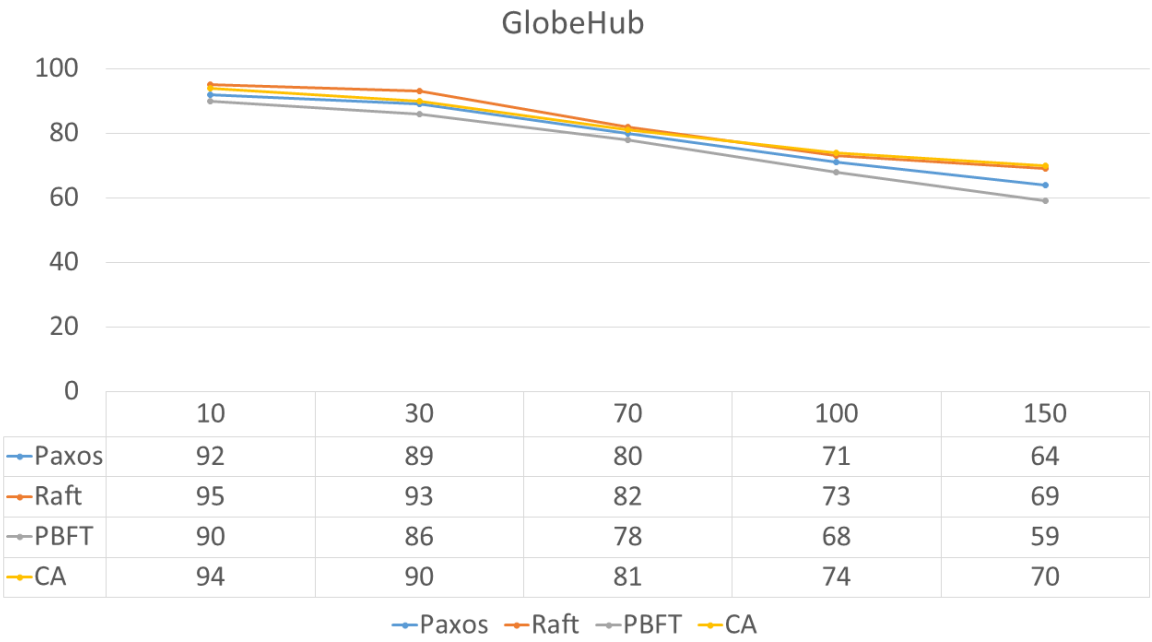


Figure 6.8: Consistency of Offer for GlobeHub

6.9.4 Composite Metric Analysis of Consensus Algorithms

In order to evaluate consensus algorithms (Paxos, Raft, PBFT, and CA) based on consensus speed, fault tolerance, and consistency of offers, we created a composite metric known as Overall Performance Score (OPS). This metric gives the three primary criteria weights in order to account for their respective relevance. The following weight sets are employed in order to calculate the Overall Performance Score (OPS):

- Set 1:
  - Consensus Speed: 50%
  - Fault Tolerance: 25%
  - Consistency of Offers: 25%
- Set 2:
  - Consensus Speed: 25%
  - Fault Tolerance: 25%
  - Consistency of Offers: 50%
- Set 3:
  - Consensus Speed: 25%
  - Fault Tolerance: 50%
  - Consistency of Offers: 25%

Before going into a detailed analysis of the consensus techniques, we first normalize the algorithmic performance metrics. The normalized value can be obtained using the following formula:

$$\text{Normalized Value} = \frac{\text{Algorithm Value} - \text{Min Value}}{\text{Max Value} - \text{Min Value}}$$

where:

- Algorithm Value is the performance value for the specific algorithm.
- Min Value is the minimum value among all algorithms for that metric.
- Max Value is the maximum value among all algorithms for that metric.

The following displays the calculated normalized values along with the OPS for each algorithm using three different weight sets. Table 6.4 presents the results of set 1, while the results of set 2 are shown in Table 6.5. The data for set 3 can be found in Table 6.6.

1. **Set 1 Weights (50% Speed, 25% Fault Tolerance, 25% Consistency)**

$$\text{OPS} = 0.50 \cdot \text{Speed} + 0.25 \cdot \text{Fault Tolerance} + 0.25 \cdot \text{Consistency}$$

Table 6.4: OPS Set 1

Algorithm	**NearBySync**	**ZoneLink**	**GlobeHub**
Paxos	0.867	0.822	0.726
Raft	0.918	0.850	0.761
PBFT	0.749	0.724	0.668
CA	0.930	0.835	0.744

2. **Set 2 Weights (25% Speed, 25% Fault Tolerance, 50% Consistency)**

$$\text{OPS} = 0.25 \cdot \text{Speed} + 0.25 \cdot \text{Fault Tolerance} + 0.5 \cdot \text{Consistency}$$

Table 6.5: OPS Set 2

Algorithm	NearBySync	ZoneLink	GlobeHub
Paxos	0.8725	0.8025	0.7375
Raft	0.9225	0.8225	0.7875
PBFT	0.8325	0.7925	0.7625
CA	0.9575	0.8375	0.8150

3. **Set 3 Weights (25% Speed, 50% Fault Tolerance, 25% Consistency)**

$$\text{OPS} = 0.25 \cdot \text{Speed} + 0.5 \cdot \text{Fault Tolerance} + 0.25 \cdot \text{Consistency}$$

Table 6.6: OPS Set 3

Algorithm	NearBySync	ZoneLink	GlobeHub
Paxos	0.792	0.743	0.680
Raft	0.873	0.823	0.732
PBFT	0.740	0.686	0.644
CA	0.934	0.817	0.719

In summary, table 6.7 illustrates that, in every case, CA consistently achieves the greatest OPS, demonstrating its superior overall performance when taking fault tolerance, consensus speed, and offer consistency into account. Raft performs admirably as well, especially in NearBySync, and is comparable to CA in a number of scenarios. While PBFT consistently scores lower than the other algorithms, Paxos performs well overall but scores lower than CA and Raft, indicating that it may struggle to effectively balance speed, fault tolerance, and consistency. By using a composite measure technique, algorithms can be compared on a balanced scale and their total effectiveness may be clearly seen. The fact that CA routinely earns the highest OPS scores supports its standing as a top option for applications needing to function well in all three dimensions.

Table 6.7: Overall Performance Scores

Algorithm	NearBySync	ZoneLink	GlobeHub
Paxos	0.875	0.8025	0.7425
Raft	0.935	0.8225	0.7875
PBFT	0.835	0.8275	0.7925
CA	**0.9675**	**0.8625**	**0.8475**

6.10 Conclusion

6.10.1 Objectives achieved

The present chapter tackled many pivotal study inquiries with the objective of augmenting our comprehension and implementation of proximity marketing tactics:

1. **Actor Identification and Categorization:** By creating the NearBySync, ZoneLink, and GlobeHub scales, we were able to effectively identify and classify the primary actors engaged in proximity marketing interactions. These scales offer a methodical framework for dissecting and comprehending the interactions that occur in proximity marketing campaigns between prospects, proxies, and merchants.

2. **Creation of a Systematic Classification Framework:** The research presented a framework for the systematic classification of proximity marketing tactics into several scales. This framework makes it easier to build strategies with clarity, conduct benchmarking studies, and assess the performance of various proximity marketing campaigns.

3. **Assessment of Real-World Use and Restrictions:** We looked at the real-world uses and restrictions of the suggested classification scales. Empirical studies and case studies yield valuable insights that showcase the framework's effectiveness in improving focused marketing campaigns, allocating resources optimally, and promoting strategic expansion over an extended period of time within various operational scenarios.

6.10.2 Summary of the chapter

In conclusion, this essay has made clear the increasing importance of proximity marketing in modern digital marketing strategies. Despite the growing popularity of proximity marketing methods, their effective implementation and improvement have been hindered by the absence of a comprehensive classification system. Consumers' persistent concerns about data privacy and the misuse of their personal information present another significant obstacle.
We have proposed a novel three-tiered classification scheme: NearBySync, ZoneLink, and GlobeHub, in answer to these pressing issues. Based on factors including audience size, communication channels, and geographic location, each tier offers tailored strategies. This framework fills in a major knowledge gap and provides businesses with a clear road map for implementing proximity marketing strategies.
Consensus algorithms play a key role in our solution since they give proximity marketing systems a dependable means of assuring consensus and data security. By utilizing algorithms like as CA, Paxos, Raft, or PBFT, businesses can protect client privacy while encouraging transparency and trust in their marketing campaigns.
Our proposed approach has two benefits: it enhances user experience by offering personalized experiences without compromising data integrity, and it protects consumer privacy by reducing the risk of data breaches and intrusive tracking. By putting consumers' privacy and comfort first, businesses may create enduring relationships founded on trust and respect.
This chapter concludes by highlighting the revolutionary potential of proximity marketing when utilized in conjunction with a customer-focused approach founded in open, moral, and privacy-conscious values. Organizations may effectively navigate the complexities of the digital landscape by using state-of-the-art technologies such as Paxos and our suggested architecture. This will promote genuine consumer relationships, foster loyalty, and support long-term expansion.

Chapter 7

Conclusion and Perspectives

The study's main results and findings are outlined in this chapter, which also provides an overview of how the dispersed techniques that have been suggested have addressed the issues of trust, privacy, and data protection in proximity marketing contexts. Furthermore, the chapter provides suggestions for further research, highlighting the necessity of investigating cutting-edge technology, broadening the range of case studies, and scrutinizing the enduring viability of proximity marketing strategies.

7.1 Conclusion

This thesis investigated how proximity marketing developed and how it became important in contemporary digital communication. Proximity marketing emerged as a rapidly growing field that utilized location-based technologies to interact with consumers in real-time through customized messaging. However, privacy, user consent, and trust were significant practical issues that needed to be addressed to ensure the successful and ethical adoption of these strategies.

The goal of this research was to create visible, unambiguous processes that promoted confidence between all parties. By offering users greater control over their personal data, such as the ability to opt-in or opt-out of data gathering and sharing, this research empowered users and established an environment of mutual trust. In order to ensure that all parties were aware of and adhered to ethical data usage standards, the study also included recommendations for clear and concise data-sharing agreements between merchants and intermediaries. We also addressed the complications of combining numerous communication technologies, such as Bluetooth, Wi-Fi, and 5G, which were essential to proximity marketing. The smooth integration of these technologies was crucial to ensure that targeted marketing messages were delivered without jeopardizing user privacy. Our study demonstrated that a commitment to user protection, effective data management, and security mechanisms was necessary to achieve this degree of integration.

This thesis introduced new ways to enhance confidentiality and trust in proximity marketing contexts, which was one of its main accomplishments. The creation of a framework for building confidence in network tools was the thesis's first contribution. Proximity marketing relies heavily on technologies such as Bluetooth, Wi-Fi, and 5G to target individuals with marketing messages based on their location. However, these tools were frequently vulnerable to privacy invasions, illegal tracking, and security lapses. To mitigate the risks of tracking users without their consent, our research proposed MAC address randomization—a technique that continuously shifted pseudonymized MAC addresses. This technique ensured that businesses could interact with customers while safeguarding personal information, thereby building greater confidence in the underlying network architecture.

The second contribution focused on using consensus-building techniques to foster trust. To prevent fraud, manipulation, and data security breaches in proximity marketing, data integrity, and marketing transaction verification were essential. In this thesis, a consensus algorithm, designed specifically for proximity marketing environments, was introduced. The algorithm secured marketing interactions and ensured that the information shared between users and businesses was authentic and trustworthy by guaranteeing that all nodes in the network agreed on the validity of transactions. This distributed approach reduced the risk of compromised transactions and eliminated single points of failure, thus strengthening the security of the entire marketing ecosystem.

The third contribution addressed the importance of trust in relationships between marketing actors—retailers, consumers, intermediaries, and technology providers. Often, users of proximity marketing were not fully aware of or in control of how their data was being collected and used. This imbalance weakened user trust and could lead to disengagement. Our study proposed new approaches to drafting clear agreements and enhancing user control over personal information. This research aimed to empower users by providing them with direct control over their privacy settings, such as the option to opt-in or opt-out of data collection. This fostered an environment where consumers could interact with proximity marketing systems with confidence and trust. Transparency among actors ensured that user interactions remained ethically and legally compliant, while also alleviating concerns about data exploitation.

In summary, proximity marketing is an effective technique for raising customer involvement, but it needs to change to satisfy consumers who are concerned about their privacy and the ever stricter regulations governing data protection. Through the examination of trust, confidentiality, and network security, this thesis makes three contributions to the advancement of user-friendly and

long-lasting proximity marketing tactics. These solutions set organizations up for long-term success in this dynamic and quickly changing industry by protecting consumer rights while simultaneously enhancing the user experience.

7.2 Perspectives

7.2.1 Short-term Perspective

The results of this thesis provide a number of readily pursued directions for future investigation. These studies would concentrate on developing the theoretical knowledge of trust mechanisms, network security, and proximity marketing in addition to improving the current approaches.

Enhanced Consensus Algorithms:

The consensus algorithms suggested in this thesis should be further developed and tested as an immediate area of research. Although the current algorithm balances security and privacy of users well, there is still room for improvement in terms of its effectiveness, scalability, and versatility in various proximity marketing settings. Studies that compare the performance of various algorithms, including Proof of Authority (PoA) and Delegated Proof of Stake (DPoS), in proximity marketing settings could potentially be carried out.

User Consent Mechanisms:

This thesis also highlighted the necessity of adhering to international data protection laws, like the GDPR, and following the law. Building trust and engagement in proximity marketing environments requires both user control over personal information and a more transparent data collection approach. Our future study will provide answers that satisfy these legal standards and point the way toward more moral and conscientious marketing strategies.

Proximity Marketing Classification Validation:

The categorization scheme described in this thesis can be verified further by means of focused case studies conducted in several sectors, including public areas, retail, and events. To investigate the practical performance of the suggested proximity marketing scales (NearBySync, ZoneLink, and GlobeHub), researchers might carry out field research. This would add to the body of empirical data demonstrating the classification framework's adaptability and efficacy.

7.2.2 Long-term Perspective

Proximity marketing relies on extensive real-world testing and implementations to be successful. Although these lengthy studies would demand a substantial financial investment, they would yield priceless insights into the operational and practical aspects of proximity marketing in large-scale settings.

Large-scale Pilot Projects:

Conducting extensive pilot projects to evaluate proximity marketing systems in real-world circumstances is one of the main long-term objectives. This can involve putting in place extensive proximity marketing installations where thousands of people interact in real-time with marketing messages in shopping centers, smart cities, or event spaces. Through data on the performance of the network integration and trust mechanisms at scale, these trials would offer fresh insights into user behavior, system robustness, and commercial outcomes.

Cross-sector Implementations:

Long-term research might also look into how proximity marketing frameworks work in a variety of industries, such as government services, transportation, and healthcare. For example, proximity marketing might be used in public transit to provide customers with targeted offers and real-time schedule changes, or in the medical field to enhance patient experiences by sending timely location-based notifications.

Proximity Marketing and IoT Integration:

Another long-term approach proposes connecting proximity marketing with the Internet of Things (IoT) to create a fully connected ecosystem. For even more dynamic and tailored encounters, proximity marketing systems could integrate wearables, smart devices, and sensors. In-depth technological research would be necessary to understand how proximity marketing works with Internet of Things (IoT) devices and how to safely handle and use the data from these devices for marketing.

Societal Behavioral Studies:

More extensive research is required to comprehend the impact of proximity marketing from a societal perspective. What reactions do people and communities have to persistent, location-based marketing? What ethical bounds apply, and how can marketing continue to be successful without going too far? In an increasingly connected environment, longitudinal studies can track customer opinions over time and provide data that will shape future tailored marketing strategies.

Impact on Consumer Trust and Brand Loyalty:

Measurements of how trust mechanisms affect consumer trust and brand loyalty can be made through real-world deployments. Long-term research ought to evaluate the ways in which users' desire to participate in marketing campaigns, contribute data, and establish enduring connections with businesses is influenced by their trust in network tools, consensus processes, and transparent data practices.

Legal and Ethical Studies:

Legal and ethical frameworks could potentially be the subject of long-term research, particularly in nations where laws governing proximity marketing are still being developed. A comparative legal research might analyze how different nations manage privacy and consent regulations, helping businesses adapt proximity marketing tactics to meet with growing worldwide norms.

To sum up, this thesis not only tackles important proximity marketing issues like trust, privacy, and network security, but it also establishes the foundation for further developments in this quickly developing industry. The suggested remedies, which range from innovative consensus algorithms to frameworks for improved user permission and privacy protection, have the power to fundamentally alter how companies interact with customers through location-based marketing in real time. The trip is far from over, though. Both the short-term and long-term views highlight how much effort needs to be done to improve these strategies and determine whether they can be scaled up in practical settings. We can get closer to a day when proximity marketing strikes a balance between innovation and ethics, providing tailored experiences while upholding users' rights, by pursuing these research options. In the end, the work showcased here acts as a first step toward user-centric, dependable, and secure marketing platforms that are advantageous to companies and customers in the digital era.

Publications List

- **Publication in International Journals (submitted)**

  Chahal, F., Fouchal, H., Gaïti, D. (2024, Octobre). Strategies for Secure Proximity Marketing: Taxonomies and Consensus Integration. In International IEEE Sensors Journal.

- **Publications in international conferences with extended articles (>3 pages)**

  - Chahal, F., Gaiti, D., Fouchal, H. (2022, June). Consensus Algorithms in Cryptocurrency and V2X-IoT: Preliminary Study. In International Conference on Innovations for Community Services (pp. 63-74). Cham: Springer International Publishing.
  - Chahal, F., Fouchal, H., Gaiti, D. (2023, February). Consensus algorithms for Opt-in/Opt-out and proximity marketing context. In 2023 International Conference on Computing, Networking and Communications (ICNC) (pp. 207-213). IEEE.
  - Chahal, F., Fouchal, H., Gaïti, D. (2023, December). User Control in Proximity Marketing: A Basic Consensus Algorithm. In GLOBECOM 2023-2023 IEEE Global Communications Conference (pp. 5931-5936). IEEE.
  - Chahal, F., Fouchal, H., Gaïti, D. (2023, October). Preserving User Privacy and Empowering Control in Proximity Marketing. In 2023 10th International Conference on Wireless Networks and Mobile Communications (WINCOM) (pp. 1-6). IEEE.
  - Chahal, F., Fouchal, H., Gaïti, D. (2024, May). Proximity Marketing: A Diverse Classification Approach. In 2024 International Wireless Communications and Mobile Computing (IWCMC) (pp. 879-884). IEEE.

- **Publications in international conferences with abstract articles (<3 pages)**

  Chahal, F., Fouchal, H., Gaïti, D. (2023, March). Data protection: Blockchain and Consensus algorithm "A use case in Proximity Marketing". In International Conference on Innovation and Connected Technology X.0 2023 (ICCITX.0-2023).

Bibliography

[1] Marketing d'influence : les challenges des marques. https://proximity.touchinnovative.com/proximity/article/75/marketing-d-influence-les-challenges-des-marques. Accessed: 2024-07-16.

[2] Passive, active, and proactive: the three stages of proximity marketing. https://www.sdggroup.com/en/insights-room/proximity-marketing-leveraging-data-high-effectiveness. Accessed: 2024-07-16.

[3] Proximity marketing: Engaging customers at the right place and time. https://mediatool.com/blog/proximity-marketing. Accessed: 2024-07-16.

[4] Proximity marketing: the privacy implications for retailers. https://www.lexology.com/library/detail.aspx?g=24f71dc6-c0c7-444e-92d2-8f013bf08f9e. Accessed: 2024-07-16.

[5] Fatemeh Akhyani, Alireza Komeili Birjandi, Reza Sheikh et Shib Sankar Sana : New approach based on proximity/remoteness measurement for customer classification. *Electronic Commerce Research*, pages 1–32, 2022.

[6] Dr Mohammed Abbas Fadhil Al-Husainy : Mac address as a key for data encryption. *arXiv preprint arXiv:1311.3821*, 2013.

[7] Jawad Ali et Mohammad Haseeb Zafar : Improved end-to-end service assurance and mathematical modeling of message queuing telemetry transport protocol based massively deployed fully functional devices in smart cities. *Alexandria Engineering Journal*, 72:657–672, 2023.

[8] Navalkrushna Allurwar, Balasaheb Nawale et Swapnesh Patel : Beacon for proximity target marketing. *Int. J. Eng. Comput. Sci*, 15(5):16359–16364, 2016.

[9] Hassan Almahdi, Shajahan Shamsudeen et K Khalufi : A study on customers' perception and marketing effectiveness of proximity marketing communications on nfc and sms-cb enabled mobile phones in usa. *Journal of Mass Communication and Journalism*, 8(6), 2018.

[10] H Alzoubi, M Alshurideh, B Kurdi, I Akour et R Aziz : Does ble technology contribute towards improving marketing strategies, customers' satisfaction and loyalty? the role of open innovation. *International Journal of Data and Network Science*, 6(2):449–460, 2022.

[11] Katia Angue, Cécile Ayerbe et Liliana Mitkova : A method using two dimensions of the patent classification for measuring the technological proximity: an application in identifying a potential r&d partner in biotechnology. *The Journal of Technology Transfer*, 39:716–747, 2014.

[12] Dheeraj Manirathnam ANNA, MN VIJAYALAKSHMI, Kota Solomon RAJU *et al.* : Enabling lightweight device authentication in message queuing telemetry transport protocol. *IEEE Internet of Things Journal*, 2024.

[13] Monika ASIJA : Mac address. *IRA-International Journal of Technology & Engineering*, 3(1):41–60, 2016.

[14] Leo Maxim BACH, Branko MIHALJEVIC et Mario ZAGAR : Comparative analysis of blockchain consensus algorithms. *In 2018 41st international convention on information and communication technology, electronics and microelectronics (MIPRO)*, pages 1545–1550. Ieee, 2018.

[15] Pierre-Alexandre BALLAND, Ron BOSCHMA et Koen FRENKEN : Proximity, innovation and networks: A concise review and some next steps. *Handbook of proximity relations*, pages 70–80, 2022.

[16] Syagnik BANERJEE, Shichun XU et Scott D JOHNSON : How does location based marketing affect mobile retail revenues? the complex interplay of delivery tactic, interface mobility and user privacy. *Journal of Business Research*, 130:398–404, 2021.

[17] Solon BAROCAS et Helen NISSENBAUM : On notice: The trouble with notice and consent. *In Proceedings of the engaging data forum: The first international forum on the application and management of personal electronic information*, 2009.

[18] Steven BELLMAN, Eric J JOHNSON et Gerald L LOHSE : On site: To opt-in or opt-out? it depends on the question. *Communications of the ACM*, 44(2):25–27, 2001.

[19] Rashmi BHARDWAJ et Debabrata DATTA : Consensus algorithm. *Decentralised Internet of Things: A Blockchain Perspective*, pages 91–107, 2020.

[20] Augustin BILOLO, Harold BOECK, Fabien DURIF et Nataly LEVESQUE : The impact of proximity marketing on consumer reactions and firm performance: A conceptual and integrative model. 2015.

[21] Felipe BOEIRA, Mikael ASPLUND et Marinho BARCELLOS : Decentralized proof of location in vehicular ad hoc networks. *Computer Communications*, 147:98–110, 2019.

[22] Miguel CASTRO et Barbara LISKOV : Practical byzantine fault tolerance and proactive recovery. *ACM Transactions on Computer Systems (TOCS)*, 20(4):398–461, 2002.

[23] Miguel CASTRO, Barbara LISKOV *et al.* : Practical byzantine fault tolerance. *In OsDI*, volume 99, pages 173–186, 1999.

[24] Fatima CHAHAL, Dominique GAITI et Hacène FOUCHAL : Consensus algorithms in cryptocurrency and v2x-iot: Preliminary study. *In International Conference on Innovations for Community Services*, pages 63–74. Springer, 2022.

[25] Elizabeth Ramírez CORREA, Erika Pulido ARJONA, Carlos OSORIO et Stefania PARETI : Factors influencing the adoption of geolocation and proximity marketing technologies. *In Information Technology and Systems: ICITS 2021, Volume 1*, pages 517–525. Springer, 2021.

[26] Mathieu CUNCHE : I know your mac address: targeted tracking of individual using wi-fi. *Journal of Computer Virology and Hacking Techniques*, 10:219–227, 2014.

[27] Martin Degeling, Christine Utz, Christopher Lentzsch, Henry Hosseini, Florian Schaub et Thorsten Holz : We value your privacy... now take some cookies: Measuring the gdpr's impact on web privacy. *arXiv preprint arXiv:1808.05096*, 2018.

[28] Ahmed Didouh, Yassin El Hillali, Atika Rivenq et Houda Labiod : Novel centralized pseudonym changing scheme for location privacy in v2x communication. *Energies*, 15(3):692, 2022.

[29] Itay P Fainmesser, Andrea Galeotti et Ruslan Momot : Digital privacy. *Management Science*, 69(6):3157–3173, 2023.

[30] Ellis Fenske, Dane Brown, Jeremy Martin, Travis Mayberry, Peter Ryan et Erik Rye : Three years later: A study of mac address randomization in mobile devices and when it succeeds. *Proceedings on Privacy Enhancing Technologies*, 2021(3):164–181, 2021.

[31] Hacène Fouchal et Zineb Habbas : Distributed backtracking algorithm based on tree decomposition over wireless sensor networks. *Concurrency and Computation: Practice and Experience*, 25(5):728–742, 2013.

[32] Lubica Gajanova, Jana Kliestikova et Margareta Nadanyiova : Application of nfc technology in proximity marketing. *In International Scientific and Practical Conference on Digital Economy (ISCDE 2019)*, pages 167–170. Atlantis Press, 2019.

[33] Lubica Gajanova, Margareta Nadanyiova, Jana Kliestikova et Judit Olah : The potential of using bluetooth-based system as a part of proximity marketing in the slovak republic. *Marketing and management of innovations*, (2):239–252, 2019.

[34] Ayush Gala, Chinmay Borgaonkar, Vaishnavi Kulkarni, Madhuri Wakode et Geetanjali Kale : Contextual flow of information in tourism using ble proximity detection to enhance the tourism experience. *In 2023 International Conference on Emerging Smart Computing and Informatics (ESCI)*, pages 1–6. IEEE, 2023.

[35] Eric Garcia Ribera : Design and implementation of a proof-of-stake consensus algorithm for blockchain. B.S. thesis, Universitat Politècnica de Catalunya, 2018.

[36] Peter Gaži, Aggelos Kiayias et Dionysis Zindros : Proof-of-stake sidechains. *In 2019 IEEE Symposium on Security and Privacy (SP)*, pages 139–156. IEEE, 2019.

[37] Cristian Geldes, Christian Felzensztein, Ekaterina Turkina et Aurélia Durand : How does proximity affect interfirm marketing cooperation? a study of an agribusiness cluster. *Journal of Business Research*, 68(2):263–272, 2015.

[38] Arthur Gervais, Ghassan O Karame, Karl Wüst, Vasileios Glykantzis, Hubert Ritzdorf et Srdjan Capkun : On the security and performance of proof of work blockchains. *In Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*, pages 3–16, 2016.

[39] Ana-Maria Giurea : Proximity market, the new trend approved by the consumer's behavior. *International Journal of Economic Practices & Theories*, 5(5), 2015.

[40] Michelle Goddard : The eu general data protection regulation (gdpr): European regulation that has a global impact. *International Journal of Market Research*, 59(6):703–705, 2017.

[41] Eric Goldman : An introduction to the california consumer privacy act (ccpa). *Santa Clara Univ. Legal Studies Research Paper*, 2020.

[42] Diksha GUPTA, Jared SAIA et Maxwell YOUNG : Proof of work without all the work. *In Proceedings of the 19th international conference on distributed computing and networking*, pages 1–10, 2018.

[43] Lenka HANÁKOVÁ : Current issues of personal data privacy in marketing. *Acta academica*, 20(2):5–20, 2020.

[44] Annmarie HANLON et Karen JONES : Ethical concerns about social media privacy policies: do users have the ability to comprehend their consent actions? *Journal of Strategic Marketing*, pages 1–18, 2023.

[45] Shihab Shahriar HAZARI et Qusay H MAHMOUD : A parallel proof of work to improve transaction speed and scalability in blockchain systems. *In 2019 IEEE 9th annual computing and communication workshop and conference (CCWC)*, pages 0916–0921. IEEE, 2019.

[46] Jason I HONG, Gaetano BORIELLO, James A LANDAY, David W MCDONALD, Bill N SCHILIT et J Doug TYGAR : Privacy and security in the location-enhanced world wide web. *In Proceedings of Fifth International Conference on Ubiquitous Computing: Ubicomp*, page 11, 2003.

[47] Heidi HOWARD, Malte SCHWARZKOPF, Anil MADHAVAPEDDY et Jon CROWCROFT : Raft refloated: Do we have consensus? *ACM SIGOPS Operating Systems Review*, 49(1):12–21, 2015.

[48] Junjie HU et Ke LIU : Raft consensus mechanism and the applications. *In Journal of physics: conference series*, volume 1544, page 012079. IOP Publishing, 2020.

[49] Dongyan HUANG, Xiaoli MA et Shengli ZHANG : Performance analysis of the raft consensus algorithm for private blockchains. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 50(1):172–181, 2019.

[50] Markus JAKOBSSON et Ari JUELS : Proofs of work and bread pudding protocols. *In Secure Information Networks: Communications and Multimedia Security IFIP TC6/TC11 Joint Working Conference on Communications and Multimedia Security (CMS'99) September 20–21, 1999, Leuven, Belgium*, pages 258–272. Springer, 1999.

[51] Eric J JOHNSON, Steven BELLMAN et Gerald L LOHSE : Defaults, framing and privacy: Why opting in-opting out. *Marketing letters*, 13:5–15, 2002.

[52] Garrett JOHNSON, Randall A LEWIS et David REILEY : Location, location, location: Repetition and proximity increase advertising effectiveness. *Available at SSRN 2268215*, 2016.

[53] Garrett A JOHNSON, Scott K SHRIVER et Shaoyin DU : Consumer privacy choice in online advertising: Who opts out and at what cost to industry? *Marketing Science*, 39(1):33–51, 2020.

[54] Kostis KARANTIAS, Aggelos KIAYIAS et Dionysis ZINDROS : Proof-of-burn. *In Financial Cryptography and Data Security: 24th International Conference, FC 2020, Kota Kinabalu, Malaysia, February 10–14, 2020 Revised Selected Papers 24*, pages 523–540. Springer, 2020.

[55] Mohammad Ayoub KHAN, Fahad ALGARNI et Mohammad Tabrez QUASIM : Decentralised internet of things. *Decentralised Internet of Things: A Blockchain Perspective*, pages 3–20, 2020.

[56] Aggelos KIAYIAS et Dionysis ZINDROS : Proof-of-work sidechains. *In International Conference on Financial Cryptography and Data Security*, pages 21–34. Springer, 2019.

[57] Seungmo KIM et Ahmed S IBRAHIM : Byzantine-fault-tolerant consensus via reinforcement learning for permissioned blockchain-empowered v2x network. *IEEE Transactions on Intelligent Vehicles*, 8(1):172–183, 2022.

[58] Sunny KING et Scott NADAL : Ppcoin: Peer-to-peer crypto-currency with proof-of-stake. *self-published paper, August*, 19(1), 2012.

[59] Jonathan KIRSCH et Yair AMIR : Paxos for system builders: An overview. *In Proceedings of the 2nd Workshop on Large-Scale Distributed Systems and Middleware*, pages 1–6, 2008.

[60] Kosuke KOMIYA et Tatsuo NAKAJIMA : Increasing motivation for playing blockchain games using proof-of-achievement algorithm. *In HCI in Games: First International Conference, HCI-Games 2019, Held as Part of the 21st HCI International Conference, HCII 2019, Orlando, FL, USA, July 26–31, 2019, Proceedings 21*, pages 125–140. Springer, 2019.

[61] Manfred KRAFFT, Christine M ARDEN et Peter C VERHOEF : Permission marketing and privacy concerns—why do customers (not) grant permissions? *Journal of interactive marketing*, 39(1):39–54, 2017.

[62] Karel KUBICEK, Jakob MERANE, Carlos COTRINI, Alexander STREMITZER, Stefan BECHTOLD et David BASIN : Checking websites' gdpr consent compliance for marketing emails. *Proceedings on Privacy Enhancing Technologies*, 2022(2):282–303, 2022.

[63] Viswanathan KUMAR, Xi ZHANG et Anita LUO : Modeling customer opt-in and opt-out in a permission-based marketing context. *Journal of Marketing Research*, 51(4):403–419, 2014.

[64] Yee-Lin LAI et Kai-Lung HUI : Internet opt-in and opt-out: investigating the roles of frames, defaults and privacy concerns. *In Proceedings of the 2006 ACM SIGMIS CPR conference on computer personnel research: Forty four years of computer personnel research: achievements, challenges & the future*, pages 253–263, 2006.

[65] Yee-Lin LAI et Kai-Lung HUI : The opt-in and opt-out debate: is it really necessary. *Online: http://www. isr. uci. edu/pep06/papers/PEP06_LaiHui. pdf [r etrieved Juli 2012]*, 2006.

[66] Leslie LAMPORT : Paxos made simple. *ACM SIGACT News (Distributed Computing Column) 32, 4 (Whole Number 121, December 2001)*, pages 51–58, 2001.

[67] Leslie LAMPORT : Generalized consensus and paxos. 2005.

[68] Leslie LAMPORT : Fast paxos. *Distributed Computing*, 19(2):79–103, 2006.

[69] Daniel LARIMER : Transactions as proof-of-stake. *Nov-2013*, 909, 2013.

[70] Luciana LAZZERETTI et Francesco CAPONE : How proximity matters in innovation networks dynamics along the cluster evolution. a study of the high technology applied to cultural goods. *Journal of Business Research*, 69(12):5855–5865, 2016.

[71] François LENGLET et Rémi MENCARELLI : Proximity in marketing: An integrating theoretical framework and research agenda. *Recherche et Applications en Marketing (English Edition)*, 35(4):99–124, 2020.

[72] Nataly LEVESQUE et Harold BOECK : Proximity marketing as an enabler of mass customization and personalization in a customer service experience. *In Managing Complexity: Proceedings of the 8th World Conference on Mass Customization, Personalization, and Co-Creation (MCPC 2015), Montreal, Canada, October 20th-22th, 2015*, pages 405–420. Springer, 2017.

[73] Nataly LEVESQUE, Harold BOECK et Marc-Antoine VACHON : Proximity marketing as a facilitator of an enhanced service experience. *In The 36th International Business Research Conference*, pages 1–13, 2016.

[74] Wenyu LI, Chenglin FENG, Lei ZHANG, Hao XU, Bin CAO et Muhammad Ali IMRAN : A scalable multi-layer pbft consensus for blockchain. *IEEE Transactions on Parallel and Distributed Systems*, 32(5):1146–1160, 2020.

[75] Marta Yuan-Chen LIN, Ben-Roy DO, Tessa Tien NGUYEN et Julian Ming-Sung CHENG : Effects of personal innovativeness and perceived value of disclosure on privacy concerns in proximity marketing: self-control as a moderator. *Journal of Research in Interactive Marketing*, 2021.

[76] Marta Yuan-Chen LIN, Ben-Roy DO, Tessa Tien NGUYEN et Julian Ming-Sung CHENG : Effects of personal innovativeness and perceived value of disclosure on privacy concerns in proximity marketing: Self-control as a moderator. *Journal of Research in Interactive Marketing*, 16(2):310–327, 2022.

[77] Marta Yuan-Chen LIN, Tessa Tien NGUYEN, Edward Ying-Lun CHENG, Angelina Nhat Hanh LE et Julian Ming Sung CHENG : Proximity marketing and bluetooth beacon technology: A dynamic mechanism leading to relationship program receptiveness. *Journal of Business Research*, 141:151–162, 2022.

[78] Dongxiao LIU, Jianbing NI, Hongwei LI, Xiaodong LIN et Xuemin SHEN : Efficient and privacy-preserving ad conversion for v2x-assisted proximity marketing. *In 2018 IEEE 15th International Conference on Mobile Ad Hoc and Sensor Systems (MASS)*, pages 10–18. IEEE, 2018.

[79] Huiye LIU, Chung-Wei LIN, Eunsuk KANG, Shinichi SHIRAISHI et Douglas M BLOUGH : A byzantine-tolerant distributed consensus algorithm for connected vehicles using proof-of-eligibility. *In Proceedings of the 22nd International ACM Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems*, pages 225–234, 2019.

[80] Aida LOUSSAIEF, Edward Ying-Lun CHENG, Marta Yuan-Chen LIN et Julian Ming-Sung CHENG : Location-based proximity marketing: An interactive marketing perspective. *The Palgrave Handbook of Interactive Marketing*, pages 753–782, 2023.

[81] Roger LUZ DA ROCHA et Paula CHIMENTI : Consumer concerns of personal data and privacy: A systematic review. 2022(1):18207, 2022.

[82] Douglas MACKAY : Opt-out and consent. *Journal of Medical Ethics*, 41(10):832–835, 2015.

[83] Elke MACKENSEN, Matthias LAI et Thomas M WENDT : Bluetooth low energy (ble) based wireless sensors. *In SENSORS, 2012 IEEE*, pages 1–4. IEEE, 2012.

[84] Sudip MAITRA, Venkata P YANAMBAKA, Ahmed ABDELGAWAD, Deepak PUTHAL et Kumar YELAMARTHI : Proof-of-authentication consensus algorithm: Blockchain-based iot

implementation. *In 2020 IEEE 6th World Forum on Internet of Things (WF-IoT)*, pages 1–2. IEEE, 2020.

[85] Manuel Adelin MANOLACHE, Sergiu MANOLACHE et Nicolae TAPUS : Decision making using the blockchain proof of authority consensus. *Procedia Computer Science*, 199:580–588, 2022.

[86] Viddi MARDIANSYAH et Riri Fitri SARI : Implementation of proof-of-work concept algorithm using simblock simulator. *In 2021 11th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, pages 1–6. IEEE, 2021.

[87] Anna MARGULIS, Harold BOECK et Michel LAROCHE : Connecting with consumers using ubiquitous technology: A new model to forecast consumer reaction. *Journal of Business Research*, 121:448–460, 2020.

[88] Anna MARGULIS, Nataly LEVESQUE et Harold BOECK : Proximity marketing in banking: lessons from retail and entertainment industries. *International Journal of Technology Marketing*, 13(3-4):401–427, 2019.

[89] Jeremy MARTIN, Travis MAYBERRY, Collin DONAHUE, Lucas FOPPE, Lamont BROWN, Chadwick RIGGINS, Erik C RYE et Dane BROWN : A study of mac address randomization in mobile devices and when it fails. *arXiv preprint arXiv:1703.02874*, 2017.

[90] Kelly D MARTIN, Abhishek BORAH et Robert W PALMATIER : Data privacy: Effects on customer and firm performance. *Journal of Marketing*, 81(1):36–58, 2017.

[91] Kelly D MARTIN et Patrick E MURPHY : The role of data privacy in marketing. *Journal of the Academy of Marketing Science*, 45:135–155, 2017.

[92] Aswathi A MENON, T SARANYA, Sheetal SURESHBABU et AS MAHESH : A comparatıve analysis on three consensus algorithms: proof of burn, proof of elapsed time, proof of authority. *In Computer Networks and Inventive Communication Technologies: Proceedings of Fourth ICCNCT 2021*, pages 369–383. Springer, 2022.

[93] Brent A MILLER et Chatschik BISDIKIAN : *Bluetooth revealed*. Prentice Hall PTR, 2001.

[94] Damion R MITCHELL et Omar F EL-GAYAR : Privacy and online social networks: A systematic literature review of concerns, preservation, and policies. *Pacific Asia Journal of the Association for Information Systems*, 14(4):1, 2022.

[95] Zanele Nicole MNDEBELE et Muthu RAMACHANDRAN : Iot based proximity marketing. *In International Conference on Internet of Things, Big Data and Security*, volume 2, pages 325–330. SCITEPRESS, 2017.

[96] Wagdy AA MOHAMED : Location-based analytics for intelligent marketing to achieve competitiveness in small business. *International Journal of Information Technology (IJIT)*, 8(1), 2022.

[97] Stefanos MOUZAS et David FORD : The mediating role of consent in business marketing. *Industrial Marketing Management*, 74:195–204, 2018.

[98] Ruchika MUDDINAGIRI, Shubham AMBAVANE, Vivek JADHAV et Santosh TAMBOLI : Implementation of proximity marketing leveraging bluetooth low energy. *In 2020 International Conference on Electronics and Sustainable Communication Systems (ICESC)*, pages 608–612. IEEE, 2020.

[99] Namita NAIR, Ankit Kumar DALAL, Abhishek CHHABRA et Nupur GIRI : Edu-coin: A proof of stake implementation of a decentralized skill validation application. *In 2019 International Conference on Nascent Technologies in Engineering (ICNTE)*, pages 1–4. IEEE, 2019.

[100] P Rajitha NAIR et D Ramya DORAI : Evaluation of performance and security of proof of work and proof of stake using blockchain. *In 2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV)*, pages 279–283. IEEE, 2021.

[101] Satoshi NAKAMOTO : Bitcoin: A peer-to-peer electronic cash system. 2008.

[102] Gabriel NICHOLAS et Aaron SHAPIRO : Failed hybrids: The death and life of bluetooth proximity marketing. *Mobile Media & Communication*, 9(3):465–487, 2021.

[103] Michael NOFER, Peter GOMBER, Oliver HINZ et Dirk SCHIERECK : Blockchain. *Business & information systems engineering*, 59:183–187, 2017.

[104] Diego ONGARO et John OUSTERHOUT : In search of an understandable consensus algorithm. pages 305–319, 2014.

[105] Diego ONGARO et John OUSTERHOUT : The raft consensus algorithm. *Lecture Notes CS*, 190:2022, 2015.

[106] Oluwakayode ONIRETI, Lei ZHANG et Muhammad Ali IMRAN : On the viable area of wireless practical byzantine fault tolerance (pbft) blockchain networks. *In 2019 IEEE Global Communications Conference (GLOBECOM)*, pages 1–6. IEEE, 2019.

[107] Keren PAKES : Can unstructured data help to create a more inclusive society? *ITNOW*, 64(1):20–21, 2022.

[108] Michela PAPANDREA, Silvia GIORDANO, Salvatore VANINI et Piergiorgio CREMONESE : Proximity marketing solution tailored to user needs. *In 2010 IEEE International Symposium on" A World of Wireless, Mobile and Multimedia Networks"(WoWMoM)*, pages 1–3. IEEE, 2010.

[109] Sunoo PARK, Albert KWON, Georg FUCHSBAUER, Peter GAŽI, Joël ALWEN et Krzysztof PIETRZAK : Spacemint: A cryptocurrency based on proofs of space. *In Financial Cryptography and Data Security: 22nd International Conference, FC 2018, Nieuwpoort, Curaçao, February 26–March 2, 2018, Revised Selected Papers 22*, pages 480–499. Springer, 2018.

[110] R PERERA et D WIJETUNGA : Do privacy concerns and intrusiveness of proximity-based sms marketing messages affect customers' intention to visit an outlet? *Faculty of Management and Finance University of Colombo Sri Lanka*, page 402, 2023.

[111] Maria Roberta PERUGINI : Cookies and consent: The new perspectives. *Eur. J. Privacy L. & Tech.*, page 82, 2021.

[112] Babu PILLAI, Kamanashis BISWAS, Zhé HÓU et Vallipuram MUTHUKKUMARASAMY : Burn-to-claim: An asset transfer protocol for blockchain interoperability. *Computer Networks*, 200:108495, 2021.

[113] B POONGODI, J Clement SUDHAHAR *et al.* : Digital transformation in retailing: Proximity marketing-influences on customer engagement. *NVEO-NATURAL VOLATILES & ESSENTIAL OILS Journal| NVEO*, pages 14845–14867, 2021.

[114] Amitai Porat, Avneesh Pratap, Parth Shah et Vinit Adkar : Blockchain consensus: An analysis of proof-of-work and its applications, 2017.

[115] Deepak Puthal et Saraju P Mohanty : Proof of authentication: Iot-friendly blockchains. *IEEE Potentials*, 38(1):26–29, 2018.

[116] Deepak Puthal, Saraju P Mohanty, Priyadarsi Nanda, Elias Kougianos et Gautam Das : Proof-of-authentication for scalable blockchain in resource-constrained distributed systems. *In 2019 IEEE international conference on consumer electronics (ICCE)*, pages 1–5. IEEE, 2019.

[117] Sara Quach, Park Thaichon, Kelly D Martin, Scott Weaven et Robert W Palmatier : Digital technologies: tensions in privacy and data. *Journal of the Academy of Marketing Science*, 50(6):1299–1323, 2022.

[118] Benjamin Rainer et Stefan Petscharnig : Challenges and opportunities of named data networking in vehicle-to-everything communication: A review. *Information*, 9(11):264, 2018.

[119] Gabriel Antonio F Rebello, Gustavo F Camilo, Lucas CB Guimaraes, Lucas Airam C de Souza, Guilherme A Thomaz et Otto Carlos MB Duarte : A security and performance analysis of proof-based consensus protocols. *Annals of Telecommunications*, pages 1–21, 2022.

[120] Mr K Manikanteswara Reddy : Proximity marketing–a game changer in retailing industry. *New Paradigms in Management, Economics & Commerce*, page 204, 2019.

[121] General Data Protection Regulation : General data protection regulation (gdpr). *Intersoft Consulting, Accessed in October*, 24(1), 2018.

[122] John Roberts, Alvin Silk, Glen Urban et Jerry Wind : Kotler on strategic marketing. *URBAN (6.20. 10). Draft.[En línea] Disponible en: http://glenurban. com/app/webroot/-files/academic/kotler. pdf*, 2010.

[123] Mariia Rodinko, Roman Oliynykov et Andrii Nastenko : Decentralized proof-of-burn auction for secure cryptocurrency upgrade. *Blockchain: Research and Applications*, 5(1):100170, 2024.

[124] Albérico Travassos Rosário et Joana Carmo Dias : How has data-driven marketing evolved: Challenges and opportunities with emerging technologies. *International Journal of Information Management Data Insights*, 3(2):100203, 2023.

[125] Sheikh Munir Skh Saad et Raja Zahilah Raja Mohd Radzi : Comparative review of the blockchain consensus algorithm between proof of stake (pos) and delegated proof of stake (dpos). *International Journal of Innovative Computing*, 10(2), 2020.

[126] Joseph W Sakshaug, Alexandra Schmucker, Frauke Kreuter, Mick P Couper et Eleanor Singer : Evaluating active (opt-in) and passive (opt-out) consent bias in the transfer of federal contact data to a third-party survey agency. *Journal of Survey Statistics and Methodology*, 4(3):382–416, 2016.

[127] Eduardo Buetas Sanjuan, Ismael Abad Cardiel, Jose A Cerrada et Carlos Cerrada : Message queuing telemetry transport (mqtt) security: A cryptographic smart card approach. *IEEE Access*, 8:115051–115062, 2020.

[128] Jawahitha SARABDEEN : Legal risks in social media marketing. *International Journal of e-Education, e-Business, e-Management and e-Learning*, 4(3):218–223, 2014.

[129] Ressy Dwitias SARI, APU SUPIYANDI, M Muttaqin SIAHAAN et Raheliya Br GINTING : A review of ip and mac address filtering in wireless network security. *Int. J. Sci. Res. Sci. Technol*, 3(6):470–473, 2017.

[130] Geoffrey SAUNOIS, Frédérique ROBIN, Emmanuelle ANCEAUME et Bruno SERICOLA : Permissionless consensus based on proof-of-eligibility. *In 2020 IEEE 19th International Symposium on Network Computing and Applications (NCA)*, pages 1–4. IEEE, 2020.

[131] Matthew J SCHNEIDER, Sharan JAGPAL, Sachin GUPTA, Shaobo LI et Yan YU : Protecting customer privacy when marketing with second-party data. *International Journal of Research in Marketing*, 34(3):593–603, 2017.

[132] David SCHWARTZ, Noah YOUNGS, Arthur BRITTO *et al.* : The ripple protocol consensus algorithm. *Ripple Labs Inc White Paper*, 5(8):151, 2014.

[133] Petchprakai SIRILERTSUWAN, Daniel EKWALL et Daniel HJELMGREN : Proximity manufacturing for enhancing clothing supply chain sustainability. *The International Journal of Logistics Management*, 29(4):1346–1378, 2018.

[134] Aimee SMITH, Rafi CHOWDHURY et Natalina ZLATEVSKA : The role of proximity dimensions in organisational transgressions: Implications for sales and marketing. *In Australia and New Zealand Marketing Academy Conference 2023: Marketing for Good*, 2023.

[135] Hannes SOCHOR, Flavio FERRAROTTI et Rudolf RAMLER : An automated evaluation of broker compatibility for the message queuing telemetry transport protocol. *Journal of Software: Evolution and Process*, 35(7):e2410, 2023.

[136] Harish SUKHWANI, José M MARTÍNEZ, Xiaolin CHANG, Kishor S TRIVEDI et Andy RINDOS : Performance modeling of pbft consensus process for permissioned blockchain network (hyperledger fabric). *In 2017 IEEE 36th Symposium on Reliable Distributed Systems (SRDS)*, pages 253–255. IEEE, 2017.

[137] Kunal SWANI, George R MILNE et Alec N SLEPCHUK : Revisiting trust and privacy concern in consumers' perceptions of marketing information management practices: Replication and extension. *Journal of Interactive Marketing*, 56(1):137–158, 2021.

[138] M SWARNAMUGI et R CHINNAIYAN : Smart and reliable transportation system based on message queuing telemetry transport protocol. *In 2019 International Conference on Intelligent Computing and Control Systems (ICCS)*, pages 918–922. IEEE, 2019.

[139] Sanjay TANEJA et VIvek SHARMA : Role of beaconing marketing in improving customer buying experience. *In Enhancing Customer Engagement Through Location-Based Marketing*, pages 176–184. IGI Global, 2023.

[140] Sujo THOMAS : Determinants of cause-related marketing participation intention: The role of consumer knowledge, cause scope and donation proximity. *Journal of Nonprofit & Public Sector Marketing*, 35(2):194–214, 2023.

[141] Archana TIWARI, Bharti MASRAM et Kritika BHARATDWAJ : Message queuing telemetry transport based data logger. *In 2023 IEEE 8th International Conference for Convergence in Technology (I2CT)*, pages 1–4. IEEE, 2023.

[142] Paul M TORRENS : Wi-fi geographies. *Annals of the Association of American Geographers*, 98(1):59–84, 2008.

[143] Robbert VAN RENESSE et Deniz ALTINBUKEN : Paxos made moderately complex. *ACM Computing Surveys (CSUR)*, 47(3):1–36, 2015.

[144] Akke VELLINGA, Martin CORMICAN, Belinda HANAHOE, Kathleen BENNETT et Andrew W MURPHY : Opt-out as an acceptable method of obtaining consent in medical research: a short report. *BMC medical research methodology*, 11:1–4, 2011.

[145] Marko VUKOLIĆ : The quest for scalable blockchain fabric: Proof-of-work vs. bft replication. *In Open Problems in Network Security: IFIP WG 11.4 International Workshop, iNetSec 2015, Zurich, Switzerland, October 29, 2015, Revised Selected Papers*, pages 112–125. Springer, 2016.

[146] Cheng Lu WANG : *The Palgrave handbook of interactive marketing*. Springer Nature, 2023.

[147] Huaiqing WANG, Matthew KO LEE et Chen WANG : Consumer privacy concerns about internet marketing. *Communications of the ACM*, 41(3):63–70, 1998.

[148] Kim WILLEMS, Malaika BRENGMAN et Stephanie VAN DE SANDEN : In-store proximity marketing: experimenting with digital point-of-sales communication. *International Journal of Retail & Distribution Management*, 45(7/8):910–927, 2017.

[149] Gavin WOOD : Polkadot: Vision for a heterogeneous multi-chain framework. *White paper*, 21(2327):4662, 2016.

[150] Daniel W WOODS et Rainer BÖHME : The commodification of consent. *Computers & Security*, 115:102605, 2022.

[151] Bingbing XIAO, Chenguang JIN, Zheng LI, Bingnan ZHU, Xiaoruo LI et Dong WANG : Proof of importance: A consensus algorithm for importance based on dynamic authorization. *In IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology*, pages 510–513, 2021.

[152] Heng XU, Xin Robert LUO, John M CARROLL et Mary Beth ROSSON : The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing. *Decision support systems*, 51(1):42–52, 2011.

[153] Fan YANG, Wei ZHOU, QingQing WU, Rui LONG, Neal N XIONG et Meiqi ZHOU : Delegated proof of stake with downgrade: A secure and efficient blockchain consensus algorithm with downgrade mechanism. *IEEE access*, 7:118541–118555, 2019.

[154] Jian YANG, Zhenhong JIA, Ruiguo SU, Xiaoxiong WU et Jiwei QIN : Improved fault-tolerant consensus based on the pbft algorithm. *Ieee Access*, 10:30274–30283, 2022.

[155] G Mustafa ZEBARI, D Assad ZEBARI et Adel AL-ZEBARI : Fundamentals of 5g cellular networks: A review. *Journal of Information Technology and Informatics*, 1(1):1–5, 2021.

[156] Yang ZHANG, Bo HAN, Zhi-Li ZHANG et Vijay GOPALAKRISHNAN : Network-assisted raft consensus algorithm. *In Proceedings of the SIGCOMM Posters and Demos*, pages 94–96. 2017.

Appendix A

Résumé de la thèse

A.1 Environnement : Marketing de proximité

Le marketing de proximité est une stratégie qui consiste à utiliser des technologies de communication, telles que le Bluetooth, le Wi-Fi et la 5G, pour diffuser des messages et des offres personnalisés aux consommateurs en fonction de leur localisation géographique en temps réel. Il vise à créer des interactions pertinentes et opportunes entre les marques et les consommateurs, afin d'améliorer l'engagement, la conversion et la fidélité, tout en exploitant les données de localisation pour optimiser les campagnes marketing et offrir des expériences individualisées.
En fournissant des informations pertinentes en temps réel, le marketing de proximité crée des opportunités d'interactions significatives entre les consommateurs et les marques qui sont les acteurs principaux de ce domaine. Cela renforce non seulement l'expérience client, mais favorise également la fidélité et les achats répétés. De plus, en proposant des offres au moment opportun, lorsque le consommateur est proche d'un produit, les chances de conversion et d'achat sont considérablement augmentées. Grâce à l'intégration de technologies telles que le Bluetooth, le Wi-Fi (norme IEEE 802.11), et la 5G, les entreprises peuvent collecter et analyser des données en temps réel sur les habitudes de consommation, offrant ainsi des informations précieuses sur le comportement des clients. Dans un marché de plus en plus concurrentiel, cette approche confère un avantage compétitif significatif, en créant des expériences uniques et personnalisées qui répondent aux attentes des consommateurs.
En résumé, le marketing de proximité offre de nombreux avantages qui améliorent l'efficacité des campagnes marketing. En se concentrant sur des communications ciblées et des données en temps réel, les entreprises peuvent renforcer l'engagement des clients et stimuler les ventes. À mesure que les comportements des consommateurs évoluent, le marketing de proximité deviendra un outil incontournable pour se démarquer dans un secteur hautement concurrentiel.

A.2 La problématique générale du marketing de proximité

Bien que le marketing de proximité offre de nombreuses opportunités aux acteurs, il présente également plusieurs défis complexes qui peuvent nuire à son application et à son efficacité. Ces défis comprennent des problématiques scientifiques telles que les préoccupations en matière de confidentialité, les questions de confiance, la sécurité des données et la réglementation, ainsi que la participation et le contrôle des utilisateurs. En outre, il existe également des enjeux politiques, économiques et écologiques. Dans le cadre du marketing de proximité, les problématiques suivantes sont particulièrement pertinentes :

A.2.1 Problèmes de Confidentialité

La collecte de données basées sur la localisation se fait souvent sans le consentement explicite des utilisateurs, ce qui soulève des préoccupations quant aux atteintes à la vie privée. Les consommateurs deviennent de plus en plus méfiants à l'égard des pratiques de marketing de proximité en raison de l'utilisation et du stockage de leurs données personnelles. Ces inquiétudes sont amplifiées par le manque de transparence concernant l'utilisation des données.

A.2.2 Problèmes de confiance

L'établissement de la confiance entre les consommateurs et les commerçants est essentiel pour une exécution réussie du marketing de proximité. Si les utilisateurs perçoivent les activités de marketing comme étant intrusives ou manipulatrices, ils risquent de se désengager et de refuser les communications personnalisées. Une communication claire concernant les politiques de données et

les avantages que les consommateurs peuvent retirer du partage de leurs informations est nécessaire pour instaurer cette confiance.

A.2.3 Sécurité des Données et Réglementation

L'augmentation du volume de données personnelles collectées dans le cadre du marketing de proximité pose de sérieux risques en matière de sécurité des données. Les systèmes doivent se conformer à des cadres juridiques stricts, tels que le Règlement Général sur la Protection des Données (RGPD), afin de protéger les informations des utilisateurs contre les violations et les abus. Le non-respect de ces normes peut entraîner une perte de confiance des consommateurs et des répercussions juridiques graves.

A.2.4 Engagement et Contrôle des Utilisateurs

Offrir aux utilisateurs un véritable contrôle sur leurs données et leurs interactions représente un défi majeur dans le marketing de proximité. Les utilisateurs doivent avoir la possibilité de modifier leurs préférences et de choisir la manière dont ils reçoivent les communications marketing. Sans ce contrôle, les consommateurs peuvent se sentir dépassés ou aliénés, rendant les tentatives d'engagement plus difficiles.

En résumé, bien que le marketing de proximité ouvre des perspectives prometteuses pour les commerçants, il est confronté à des défis fondamentaux liés à la confidentialité, la confiance, la sécurité des données, et l'engagement des utilisateurs. La réussite de son intégration repose sur la capacité à relever ces enjeux tout en respectant les cadres réglementaires et en favorisant une participation active des utilisateurs.

A.3 Motivation derrière le problème de recherche

Le développement rapide du marketing de proximité, facilité par les technologies Bluetooth, Wi-Fi et 5G, offre de nouvelles opportunités aux entreprises pour interagir avec leurs clients en temps réel. Cependant, plusieurs obstacles technologiques, liés à la confidentialité et à la confiance, limitent son plein potentiel.

A.3.1 Manque de Classification Claire

Le marketing de proximité manque d'un cadre cohérent pour classer les différents contextes d'utilisation et les technologies employées. Cette absence de standardisation complique la mise en place de stratégies efficaces et cohérentes, ce qui entraîne des expériences utilisateur incohérentes et des opportunités manquées pour les entreprises.

A.3.2 Mécanismes de Consentement et Confiance des Utilisateurs

Le consentement des utilisateurs et la transparence dans la collecte des données sont insuffisants. Les solutions actuelles offrent peu de contrôle granulaire aux utilisateurs, ce qui nuit à la confiance. Ce manque de clarté, notamment vis-à-vis du RGPD, pose des risques juridiques et sape l'engagement des consommateurs.

A.3.3 Manque de Confiance Entre Acteurs

La méfiance entre consommateurs et commerçants reste un frein majeur. Les consommateurs craignent l'exploitation abusive de leurs données, tandis que les commerçants peinent à rassurer sur

la sécurité des informations collectées. Ce manque de confiance entraîne une baisse d'engagement et des taux élevés de refus de participation.

A.3.4 Contrôle Insuffisant des Données par les Utilisateurs

Les utilisateurs ont un contrôle limité sur leurs données personnelles, notamment sur leur collecte et leur usage. Cette absence de gestion des données personnelles nourrit la méfiance et soulève des questions sur la propriété et l'usage des informations.

A.3.5 Intégration Incohérente des Technologies Réseaux

L'intégration des technologies Bluetooth, Wi-Fi et 5G est inégale, provoquant des expériences utilisateur irrégulières. Les anomalies dans la performance des réseaux entraînent des frustrations et réduisent l'efficacité des initiatives de marketing de proximité.

Ces défis soulignent l'importance de solutions distribuées pour améliorer la confidentialité, la confiance et l'intégration technologique, tout en offrant une expérience utilisateur plus cohérente et sécurisée.

A.4 Orientations de la Recherche et Contributions

Cette recherche a visé à améliorer la confiance et la confidentialité dans les contextes de marketing de proximité en examinant la confiance sous trois angles distincts : les technologies de réseau, les mécanismes de consensus et les interactions entre les acteurs du marketing.

A.4.1 Échange des adresses MAC pour améliorer la confidentialité

Les outils réseau jouent un rôle crucial dans le marketing de proximité, car ils permettent la transmission des messages marketing ciblés et la collecte de données utilisateur. Cependant, ces technologies ne sont pas sans risques. Les problèmes de confidentialité des données et le suivi non autorisé des utilisateurs demeurent préoccupants. En effet, le marketing de proximité utilise souvent des technologies basées sur la localisation pour profiler les clients, ce qui peut entraîner des pratiques de surveillance illégales. Le suivi des adresses MAC sans le consentement explicite des utilisateurs soulève d'importantes inquiétudes, pouvant ainsi amener les clients à perdre confiance dans les entreprises. Cette situation pose non seulement des défis moraux, mais également des implications juridiques significatives.
Notre étude s'est penchée sur des solutions visant à sécuriser ces technologies. Une proposition consiste en l'échange d'adresses MAC aléatoires, permettant de protéger la confidentialité des utilisateurs tout en offrant aux entreprises un accès à des informations essentielles pour leurs initiatives de marketing de proximité. Cette approche innovante réduit le risque de surveillance et de profilage en changeant régulièrement les adresses MAC pseudonymes, ce qui complique les tentatives de suivi. Par ailleurs, des technologies cryptographiques telles que l'échange de clés Diffie-Hellman et le cryptage AES sont mises en œuvre pour garantir la sécurité des données. Ces méthodes ajoutent une couche supplémentaire de protection, assurant que les informations sensibles restent confidentielles et que les utilisateurs sont mieux protégés contre les atteintes à leur vie privée.
Des simulations ont également été réalisées pour évaluer l'efficacité de la méthode proposée. Les résultats de ces simulations ont révélé que l'algorithme maintenait un haut niveau de précision dans la sélection des meilleures offres, tout en préservant l'anonymat du consommateur. Ce niveau de

performance souligne la résistance accrue aux attaques par corrélation d'adresses MAC, améliorant ainsi la sécurité de l'identité de l'utilisateur tout au long du processus de consensus.

A.4.2 Un nouveau mécanisme d'accord dans le marketing de proximité

Les mécanismes de consensus jouent un rôle fondamental dans la préservation de l'intégrité des données dans les systèmes distribués. Pour répondre aux enjeux spécifiques du marketing de proximité, cette recherche a développé un nouveau mécanisme de consensus, nommé Algorithme de Contrôle (CA), conçu pour valider les transactions de données de manière décentralisée. Ce mécanisme garantit qu'aucun acteur ne peut altérer ou manipuler les données sans l'accord des autres participants, créant ainsi un environnement où la confiance et la transparence sont prioritaires.
L'algorithme de contrôle (CA) apporte une contribution en plaçant la confidentialité des utilisateurs au cœur du processus marketing. Contrairement aux méthodes traditionnelles, CA donne aux utilisateurs la possibilité de contrôler efficacement les interactions marketing en leur permettant de choisir d'accepter ou de refuser les offres publicitaires. Ce système de consentement et retrait de consentement améliore la capacité des utilisateurs à gérer leur consentement conformément aux réglementations telles que le RGPD. Ainsi, les utilisateurs sont non seulement protégés contre une exploitation de leurs données personnelles, mais gagnent également en autonomie dans la gestion de leurs interactions marketing. On a abordé aussi les différentes techniques de gestion du consentement, en soulignant l'importance des systèmes qui permettent aux utilisateurs d'accorder ou de révoquer leur consentement à tout moment. Ces outils, intégrés dans l'algorithme, créent un cadre propre et responsable pour le traitement des données personnelles. En impliquant activement les utilisateurs dans ce processus, le CA renforce la confiance et encourage une participation éclairée, où chaque utilisateur est conscient des conséquences de ses choix sur la collecte et l'utilisation de ses données.
Le CA fonctionne à travers plusieurs phases : la réaction des participants aux offres, la soumission des décisions, l'agrégation des avis, et les retours des commerçants. Chaque phase est essentielle pour assurer une interaction fluide et transparente entre les utilisateurs et les entreprises. En recueillant les évaluations des utilisateurs sur les offres, CA permet une amélioration continue de l'efficacité des campagnes marketing. Les simulations effectuées ont montré une forte convergence des résultats et une efficacité croissante avec l'augmentation du nombre de participants. Ce processus souligne l'importance cruciale de sélectionner un délai optimal pour parvenir à un consensus.

A.4.3 Classification des acteurs du marketing de proximité et établissement des niveaux d'interaction par consensus

Les interactions entre les consommateurs, commerçants, et intermédiaires dans le cadre du marketing de proximité sont souvent caractérisées par un déséquilibre, notamment en termes de contrôle des données personnelles et de transparence. Ce déséquilibre nuit à la confiance des utilisateurs envers les entreprises et les intermédiaires technologiques, particulièrement lorsque ces derniers exploitent les données à des fins commerciales sans que les utilisateurs en aient pleinement conscience ou ne puissent exercer un contrôle direct. Cette recherche s'est efforcée de penser à cette situation en proposant un cadre structuré et transparent pour favoriser la confiance entre tous les acteurs impliqués.
Un des objectifs a été de développer un système de classification qui segmente les différents types d'interactions en fonction du niveau d'engagement et de personnalisation, tout en renforçant la transparence et le contrôle des utilisateurs sur leurs données personnelles. Trois échelles ont été introduites pour répondre à ce besoin : NearBySync, ZoneLink, et GlobeHub. Chaque échelle correspond à un niveau distinct d'engagement et permet aux entreprises de personnaliser leurs

stratégies marketing en fonction des préférences des clients, tout en assurant une interaction plus ciblée.

- **NearBySync :** favorise les interactions en temps réel avec des clients individuels dans des zones géographiques restreintes, permettant ainsi un marketing de proximité instantané et personnalisé.
- **ZoneLink :** s'adresse à des groupes de clients plus larges à travers des techniques de marketing par lots, offrant un équilibre entre personnalisation et efficacité à plus grande échelle.
- **GlobeHub :** fonctionne sur une échelle mondiale, permettant aux entreprises de mener des campagnes sophistiquées qui prennent en compte des facteurs globaux tout en conservant une approche personnalisée.

Ces trois niveaux permettent ainsi une segmentation plus efficace des prospects, intermédiaires et détaillants, optimisant ainsi l'efficacité des campagnes marketing. Ce cadre a pour but d'accroître la pertinence des interactions tout en respectant la vie privée des clients, ce qui est essentiel pour renforcer la confiance.

En résumé, cette recherche a permis de concevoir et de proposer des approches novatrices qui renforcent la confidentialité, la sécurité et la transparence dans les environnements de marketing de proximité. En abordant les problématiques liées au suivi non autorisé et à la protection des données, des solutions telles que la commutation d'adresses MAC ont été mises en place, permettant de préserver l'anonymat des utilisateurs tout en respectant les législations internationales. L'intégration de l'Algorithme de Contrôle a également montré son potentiel en améliorant à la fois la rentabilité des entreprises et la confiance des consommateurs, créant ainsi un cadre plus sécurisé et éthique. Enfin, ces efforts ont contribué à la construction d'un écosystème où la confiance, la transparence et le respect de la vie privée sont désormais au cœur des interactions, favorisant des relations durables entre les entreprises et leurs clients, ainsi qu'une fidélisation à long terme.

A.5 Structure de la thèse

La thèse est divisée en sept chapitres, chacun abordant différents aspects du marketing de proximité, avec un accent sur les approches distribuées et leurs implications. Les premiers chapitres posent les bases en explorant le concept, l'importance et les défis du marketing de proximité, suivis d'une analyse approfondie de l'état actuel de la recherche, en particulier en ce qui concerne la confidentialité et le consentement des consommateurs. Les chapitres suivants présentent des contributions novatrices, notamment des mécanismes comme le changement d'adresse MAC pour améliorer la confidentialité, un algorithme de contrôle pour l'autonomisation des utilisateurs dans la gestion des données, et un cadre de consensus pour classer les acteurs du marketing de proximité, visant à établir la confiance et la transparence. La conclusion synthétise ces approches distribuées, soulignant leur potentiel pour remodeler les environnements de marketing de proximité :

- **Chapitre 1 Introduction** - Ce chapitre introduit le marketing de proximité et la justification de l'étude, en énonçant les défis du secteur, notamment l'absence de catégories formalisées, les problèmes de confidentialité et la nécessité de mécanismes de consensus. Il présente également les objectifs et les contributions majeures de la recherche.
- **Chapitre 2 Contexte : Marketing de proximité** - Ce chapitre élargit le contexte du marketing de proximité, décrivant les concepts fondamentaux et les technologies sous-jacentes

(Bluetooth, Wi-Fi, 5G). Il présente divers exemples d'utilisation, en mettant en évidence les problèmes de confidentialité des données, de confiance et de suivi réseau.

- **Chapitre 3 État de l'art** - Ce chapitre examine la recherche actuelle sur le marketing de proximité, en se concentrant sur le consentement des consommateurs et la confidentialité. Il aborde les défis liés à l'utilisation des données, ainsi que les développements technologiques qui peuvent améliorer le marketing de proximité.
- **Chapitre 4 Contribution 1 : Échange de MAC pour améliorer la confidentialité** - Ce chapitre propose une méthode de changement dynamique d'adresse MAC pour protéger la confidentialité des utilisateurs dans le marketing de proximité, améliorant ainsi la confiance des utilisateurs sans compromettre la qualité du service.
- **Chapitre 5 Contribution 2 : Un nouveau mécanisme d'accord dans le marketing de proximité** -Ce chapitre introduit l'algorithme de contrôle (CA), qui met l'accent sur la confidentialité et le contrôle des utilisateurs, permettant aux consommateurs de gérer leurs données et leurs interactions avec les efforts marketing.
- **Chapitre 6 Contribution 3 : Classification des acteurs du marketing de proximité et établissement des niveaux d'interaction par consensus** - Ce chapitre présente un cadre de consensus pour catégoriser les acteurs du marketing de proximité, favorisant la confiance et la collaboration tout en équilibrant les préoccupations en matière de confidentialité et d'engagement.
- **Chapitre 7 Conclusion** - Le dernier chapitre résume les principales conclusions de l'étude et comment les approches proposées ont abordé les questions de confiance et de confidentialité dans le marketing de proximité. Il propose également des suggestions pour des recherches futures à court et à long terme.

Appendix B

Regulatory Framework in Proximity Marketing

B.1 General Data Protection Regulation (GDPR)

B.1.1 Principles and Requirements

One of the most extensive data privacy rules in the world was put into effect in *May 2018* with the General Data Privacy Regulation (GDPR). It is applicable to all organizations, regardless of location, that handle the personal data of citizens of the EU. A number of fundamental guidelines and regulations for data processing are established under the GDPR:

- Lawfulness, Fairness, and Transparency: The processing of personal data must be done so in a way that is both fair and lawful. Companies need to be transparent about how they use personal information.
- Limitation on Purpose: Information can only be gathered for clear, explicit, and legal purposes. It cannot be processed in a way that is inconsistent with those goals.
- Minimization of Data: Only information required to fulfill the stated objectives should be gathered about an individual.
- Accuracy: Personal information must be true and, if updated, kept current.
- Storage Restrictions: Personal information should not be stored longer than is necessary in a format that makes it possible to identify specific individuals.
- Integrity and Confidentiality: Processing of personal data must be done in a way that provides suitable security, including defense against improper or illegal processing as well as against unintentional loss, damage, or destruction.
- Accountability: Businesses are in charge of adhering to the GDPR standards and must be able to prove it.

Furthermore, prior to processing an individual's personal data, companies must acquire the individual's express consent under the GDPR. People also have the right to access their data, have it corrected when it is inaccurate, ask for the deletion of their data, and limit or object to data processing. Additionally, data protection impact assessments (DPIAs) for high-risk processing operations, data protection by design and default implementation, and 72-hour reporting of data breaches are requirements for organizations.

B.1.2 Impact on Proximity Marketing

The GDPR significantly affects proximity marketing strategies. Businesses operating in the EU or aiming to do business with EU citizens are required to abide by stringent data privacy regulations. Important consequences for proximity marketing encompass:

- Informed Consent: Before collecting and using a person's location data, proximity marketing initiatives must get that person's express consent. This entails giving people access to accurate and thorough information about the data being gathered, its intended uses, and their rights.
- Transparency: Companies must make sure that all of their data processing operations are transparent. This entails telling customers about the usage of their data as well as the existence of beacons, Wi-Fi tracking, and other location-based technology.
- Reducing the amount of data collected and limiting its intended use are key components of proximity marketing strategies. Information cannot be used for other purposes without further permission. This limits the amount of data that may be collected and highlights the need of having precise, well-defined goals.
- Strong security measures must be put in place to guard the gathered data from breaches, illegal access, and other security threats. This entails putting access controls in place, encrypting data, and routinely checking security procedures.
- The rights of users, including access, rectification, and deletion of personal data, must be made easier by businesses. To do this, systems enable people to simply manage their consent and data preferences must be put in place.
- Accountability and Compliance: Businesses need to be able to show that they are adhering to GDPR regulations. This entails keeping thorough records of all data processing operations, carrying out frequent audits, and making sure third-party service providers follow GDPR regulations as well.

Businesses using proximity marketing techniques can reduce privacy concerns and maximize the advantages of location-based marketing methods by complying with the GDPR. This will help them build consumer confidence and transparency.

B.2 California Consumer Privacy Act (CCPA)

B.2.1 Principles and Requirements

With effect from January 1, 2020, the California Consumer Privacy Act (CCPA) is a historic privacy law in the US that aims to improve consumers' rights and privacy for Californians. The following are important CCPA requirements and principles:

- Right to Know: Customers have the right to know what personal information is being gathered about them, why it is being used, and if it will be sold or shared with outside parties.
- Right of Access: Customers have the right to request free access to the personal information that has been acquired about them from enterprises.

- Right to Deletion: With some limitations, such as information required to finish transactions or fulfill legal requirements, consumers are entitled to request that their personal data be deleted.
- Right to Opt-Out: Customers have the option to prevent third parties from purchasing their personal information. To make this procedure easier, businesses need to have a prominent "Do Not Sell My Personal Information" link on their websites.
- Right to Non-Discrimination: Companies are prohibited from treating customers unfairly if they use their CCPA rights, such as by refusing to provide services or imposing alternative fees.
- Disclosure Requirements: Companies' privacy policies must include information about their data collecting, usage, and sharing procedures. This entails defining the types of personal information that are gathered, where they come from, why they are being collected (business or commercial), and which categories of third parties are shared with.
- Security Measures: In order to prevent unauthorized access, destruction, use, alteration, or disclosure of personal data, businesses must put in place and uphold adequate security processes and practices.

Businesses that meet specific requirements are subject to the CCPA. These requirements include having gross annual revenues of more than $25 million, purchasing, receiving, or selling the personal information of at least 50,000 consumers, households, or devices, or generating at least 50% of annual revenue from the sale of personal consumer data.

B.2.2 Impact on Proximity Marketing

In California, proximity marketing strategies are greatly impacted by the CCPA. Important ramifications consist of:

- Transparency in Data Collection: Consumers must be made fully aware by proximity marketing campaigns of the kinds of personal information that is being gathered, including location data, and the reasons behind its usage. This frequently entails giving real-time notifications when data collecting takes place and revising privacy regulations.
- Consumer Consent: Businesses must accept consumer requests to opt out of data sales and provide means to facilitate these requests, even if the CCPA does not need express opt-in consent for data collection (except from the sale of personal data for children).
- Requests for Access and Deletion: Companies need to be ready to respond to inquiries from customers seeking access to and deletion of their personal information. For the purpose of tracking and managing personal data across several touchpoints, comprehensive data management solutions are needed.
- Opt-Out Mechanisms: To ensure that consumers can readily opt out of data sales, proximity marketing campaigns that involve the selling of personal data must contain obvious opt-out mechanisms, such as a "Do Not Sell My Personal Information" link.
- Non-Discrimination: Companies are required to make sure that customers who use their CCPA-protected privacy rights do not encounter any discriminatory treatment, such as not being able to access certain marketing offers or getting subpar service.

- Data Security: To safeguard the private information gathered via proximity marketing, stronger security measures are required. To stop data breaches and unwanted access, this entails putting encryption, access limits, and frequent security assessments into place.

Businesses using proximity marketing can increase consumer trust and show that they are committed to preserving privacy by adhering to the CCPA. In addition to reducing legal concerns, compliance with this policy improves the credibility and dependability of proximity marketing campaigns, strengthening bonds with customers.

B.3 Colorado Privacy Act (CPA)

B.3.1 Principles and Requirements

Colorado individuals' rights to privacy are intended to be strengthened by the comprehensive data privacy law known as the Colorado Privacy Act (CPA), which was ratified on July 7, 2021. Commencing on July 1, 2023, the CPA closely resembles both the CCPA and the GDPR, placing strict obligations on companies that manage personal data. The following are the fundamental ideas and criteria of the CPA:

- Application: The CPA is applicable to organizations that either: conduct business in Colorado; or provide goods or services that are specifically aimed at Colorado people:
  - Manage or handle the personal information of one hundred thousand or more Colorado citizens in a given year, or
  - Control or handle the personal data of at least 25,000 Colorado residents, and profit from the selling of personal data or obtain discounts.
- Right to Opt-Out: Customers may choose not to have their personal data processed for the following reasons:
  - Personalized advertising.
  - The transfer of personal information.
  - Profiling in support of choices that have substantial legal or other ramifications for a customer.
- Right of Access: Customers may ask to see the categories and particular personal data that a company has gathered about them, as well as the personal data itself.
- Right to Correction: Customers may ask that inaccurate personal data about them be corrected.
- Right to Deletion: Customers are entitled to ask that their personal information be deleted.
- Right to Data Portability: Customers have the right to request and obtain their personal data in a format that is easily reusable and portable, as long as it is technically possible, so they can transfer the data to another organization without difficulty.
- Consent for Processing Sensitive Data: Before processing any sensitive data, including information about a person's race or ethnicity, religious beliefs, physical or mental health conditions, sexual orientation, citizenship or status, genetic or biometric information, or personal information gathered from a known child, businesses must get consent from customers.

- Data protection assessments: For processing operations that pose a greater risk of harm to customers, data controllers are required to carry out and record data protection evaluations. This covers processing sensitive data, selling personal information, and running targeted advertisements.
- Transparency: Companies need to provide privacy notifications that are thorough, easily readable, and explain all of the ways in which they process customer data. This covers the types of personal information that are gathered, the reasons behind data processing, the methods by which customers can use their rights, and the kinds of third parties that receive the data.
- Data Security: In order to protect personal data from unauthorized access, accidental loss, or destruction, controllers must put in place the necessary organizational and technical safeguards.

B.3.2 Impact on Proximity Marketing

The strict guidelines set by the CPA have a significant effect on proximity marketing tactics and force companies to implement strong privacy policies. Important ramifications consist of:

- Improved Transparency and Consumer Rights: Proximity marketing campaigns need to be open and honest about how they gather and use consumer data. Companies are required to notify customers about the use of location-based technologies (including GPS, Wi-Fi tracking, and beacons), the kinds of data that are gathered, and the reasons for the processing of that data. Businesses must also give customers easy ways to exercise their CPA rights, which include the ability to access, update, and delete their data.
- User-friendly opt-out procedures are vital for businesses to adhere to consumers' rights to refuse targeted advertising and the sale of their personal information. This can entail giving users of mobile apps or websites clear and simple ways to adjust their choices and refuse data collection and sharing.
- Approval for Sensitive Data: Businesses must get customers' express approval before collecting or processing sensitive data (such as exact geolocation data) as part of proximity marketing efforts. This might necessitate modernizing consent management procedures and making sure that consent is acquired in an unambiguous and positive way.
- Data Protection evaluations: When using proximity marketing techniques that could put customers at greater danger, including location-based profiling, organizations must carry out data protection evaluations. These evaluations assist in identifying possible privacy issues and guarantee that the right safeguards are in place to lessen those risks.
- Data Minimization and Purpose Limitation: Organizations must follow these guidelines, gathering just the information required for particular marketing campaigns and refraining from utilizing it for unrelated reasons without further authorization. To guarantee adherence to these standards, meticulous planning and design of data-gathering procedures are necessary.
- Data Security: To prevent unwanted access and breaches, proximity marketing initiatives need to include strong security measures. This entails encrypting data while it's in transit and at rest, putting robust access restrictions in place, conducting frequent audits of security procedures, and making sure that third-party service providers follow strict security guidelines as well.

- Accountability and Documentation: Companies that process data must keep thorough records of all of their operations, especially when it comes to high-risk processing like profiling and targeted advertising. This entails securing and maintaining consents, recording data protection evaluations, and proving compliance with CPA regulations.

Businesses using proximity marketing can increase consumer confidence and maintain regulatory compliance by following the CPA. In addition to lowering legal concerns, this upholds the moral standards of marketing techniques, cultivates a favorable rapport with customers, and shows a dedication to maintaining their privacy.

B.4 California Privacy Rights Act (CPRA)

B.4.1 Principles and Requirements

In November 2020, the California Consumer Privacy Act (CCPA) was strengthened by the California Privacy Rights Act (CPRA), sometimes referred to as Proposition 24. The CPRA aims to further secure personal data and provide consumers greater control over how their information is gathered and used. It does this by expanding existing obligations and introducing new ones. The following are the main tenets and specifications of the CPRA:

- Extension of the Definition of Personal Information: Under the CPRA, the term "personal information" is defined to encompass additional categories, including precise geolocation data, sensitive personal information (such as passport, social security, and driver's license numbers), racial and ethnic origin, and biometric data.
- Rights to Access and Correction: Customers are entitled to see the personal data that companies gather about them and to have any errors in it corrected. Companies are required to give comprehensive information regarding the types of personal data they gather, why they collect it, and the kinds of third parties they share it with.
- Right to Opt-Out of Sale and Sharing: The CPRA makes it easier for customers to choose not to have their personal information sold or shared. To give customers the option to refuse the sale of their data to third parties, businesses must prominently display an opt-out link on their website or mobile application.
- Sensitive Personal Information: Before collecting or processing sensitive personal information, including exact geolocation data, businesses must get the express agreement of consumers. This rule is applicable to proximity marketing initiatives that gather location-based information through Bluetooth beacons and GPS, among other technologies.
- Data minimization and purpose limitation: Companies are required to only gather the minimum amount of personal data required for the purposes stated at the time of collection. Without getting extra authorization from customers, they are not allowed to use personal information for purposes that are incompatible with the stated purposes.
- Enhanced Data Security Requirements: The CPRA places more stringent obligations on companies to put in place appropriate security measures to safeguard the personal data of their customers. This includes precautions against data breaches, frequent security audits, and encryption of personal information.
- Accountability and Transparency: Organizations must show that they are accountable for the data they use by keeping track of the data processing operations they carry out, regularly auditing their privacy policies and procedures, and giving customers clear and understandable information about the data they collect and handle.

B.4.2 Impact on Proximity Marketing

Businesses that use proximity marketing, especially those who gather and use location-based data for customized marketing campaigns and targeted advertising, will be greatly impacted by the CPRA. The CPRA has the following effects on proximity marketing:

- Increased Openness Requirements: Companies using location-based technology (such as GPS or Bluetooth beacons) for proximity marketing must give customers thorough disclosures about these uses. Customers must be informed about the different kinds of data that are gathered, why they are gathered, and which categories of third parties receive the data.
- Opt-Out Procedures: The CPRA makes it easier for customers to choose not to have their personal information—including that obtained by proximity marketing technologies—sold or shared. In order for customers to exercise their rights, businesses must give them simple ways to opt-out, which may include avoiding targeted advertising based on location data.
- Sensitive Data approval Requirements: Companies using proximity marketing that collect precise geolocation data must have customers' express approval. This entails getting consent in writing before collecting sensitive personal data, as well as being transparent about the kinds of data that are gathered and why they are processed.
- Proximity marketing initiatives must follow the guidelines of data minimization and purpose limitation, gathering only the minimal quantity of personal data required for certain marketing objectives. Without further consent from customers, businesses must make sure they do not utilize gathered data for uses that are incompatible with the stated aims.
- Data Security Requirements: Companies who want to safeguard the private information of customers obtained through proximity marketing campaigns must put strong data security procedures in place. To stop illegal access and data breaches, this involves frequent security assessments, access limitations, and data encryption.
- Accountability and Record-Keeping: Businesses are required to keep thorough records of all their proximity marketing operations, including data processing procedures, consent administration, and adherence to CPRA regulations. This guarantees transparency and accountability in data management procedures.

Businesses can increase consumer trust, reduce legal risk, and improve the overall performance of their proximity marketing initiatives by adhering to the CPRA's principles and requirements. Following these rules promotes an open and moral approach to data collecting and processing for proximity marketing campaigns in addition to protecting customer privacy.

B.5 Lei Geral de Proteção de Dados (LGPD)

B.5.1 Principles and Requirements

Brazil's General Data Protection Law, or Lei Geral de Proteção de Dados (LGPD), was passed in order to control how personal data is processed there and to comply with international data protection standards. The LGPD, which goes into effect in September 2020, sets guidelines and standards that businesses must adhere to while gathering, using, and preserving personal data. The following are the main tenets and prerequisites of the LGPD:

- Lawful Basis for Processing: The LGPD, like the GDPR, mandates that companies have a legitimate reason for processing personal data. This entails getting consent from data

subjects, carrying out contractual duties, abiding by the law, preserving people's health and safety, and pursuing legitimate interests.

- Purpose Limitation: Organizations that collect personal data must do so for precise, justifiable, and legitimate objectives and must inform data subjects of those purposes in a clear and understandable manner. Any further processing of personal information must be consistent with the initial reason it was gathered.
- Data Minimization: Under the LGPD, organizations must only gather the bare minimum of personal information required to fulfill their designated goals. Data controllers have to refrain from gathering and processing too much or needlessly.
- Transparency: Data controllers are required to notify data subjects about their data processing activities in a clear, correct, and freely accessible manner. This includes information regarding the rights of data subjects, the categories of data processed, the objectives of processing, and recipients of the data who are not third parties.
- Rights of Data Subjects: The LGPD gives data subjects a number of rights, such as the ability to access and update their personal information, remove consent-processed data, anonymize or block unnecessary or excessive data, transfer data to other service providers, and find out which public and private organizations the controller has shared data with.
- Security Measures: In order to prevent unauthorized access, accidental or unlawful data destruction, loss, alteration, communication, or any other type of inappropriate or unlawful processing, organizations must put in place technological and administrative security measures.
- Accountability: Data controllers are required to exhibit adherence to the principles and guidelines of the LGPD, which includes keeping track of all data processing operations, completing impact analyses, and putting in place privacy policies and procedures that comply with legal requirements.

B.5.2 Impact on Proximity Marketing

The LGPD has important ramifications for proximity marketing initiatives that gather and handle personal data, especially location-based data used for customer engagement and targeted advertising. The LGPD has the following effects on proximity marketing:

- Requirements for Consent: Before collecting and processing any personal data from data subjects—including location-based data gleaned from technologies like Bluetooth beacons, Wi-Fi signals, or GPS—organizations participating in proximity marketing must have their express consent.
- The rules of purpose limitation and data reduction must be followed by proximity marketing campaigns in order to guarantee that the personal information gathered by these technologies is only utilized for authorized and specified purposes. Businesses should refrain from gathering excessive or pointless data that is unrelated to their marketing goals.
- Transparency Requirements: Companies that engage in proximity marketing are required to give people easy access to information about their data collecting procedures, including the kinds of data they gather, why they process it, and the rights of data subjects under the LGPD. Transparency fosters trust and empowers people to make knowledgeable decisions about their personal information.

- Data Security: To safeguard the confidentiality, integrity, and availability of personal information gathered through proximity marketing campaigns, organizations need to have strong security measures in place. To reduce data breaches, security measures can include data encryption, access controls, routine security assessments, and incident response protocols.
- The LGPD grants data subjects additional rights, such as the ability to see their personal information, make correction requests, have unneeded data deleted, and withdraw their permission to process. Companies have to make it easier for people to exercise these rights and have to answer requests from data subjects right away.
- Accountability and Compliance: Companies have to show that they are responsible for processing personal data, keeping track of consent, processing personal data, and adhering to LGPD regulations. Putting privacy policies into place and carrying out frequent evaluations and audits are crucial for maintaining legal compliance.

Organizations can improve consumer trust, reduce legal risk, and promote ethical data management practices in proximity marketing campaigns by adhering to the principles and criteria of the LGPD. Following these rules fosters ethical data handling, openness in marketing techniques, and customer privacy protection.

B.6 Personal Information Protection and Electronic Documents Act (PIPEDA)

B.6.1 Principles and Requirements

Canada's federal privacy law, known as the Personal Information Protection and Electronic Documents Act (PIPEDA), regulates how private sector businesses gather, use, and disclose personal data. Organizations must abide by the guidelines and standards set forth by PIPEDA to guarantee the security of persons' personal data. The following are the main tenets and specifications of PIPEDA:

- Consent: Unless otherwise allowed by law, organizations are required to acquire individuals' meaningful consent before collecting, using, and disclosing their personal information. Clear, intelligible consent must be obtained before or at the time of collection, and it must be obtained for defined reasons.
- Purpose Limitation: Except in cases where the individual's consent is obtained or as mandated by law, personal information may only be gathered for specific, lawful purposes. It may not be used or shared for purposes other than those for which it was originally obtained.
- Data minimization: Companies should only gather the minimum amount of personal data required to achieve the stated goals, and they should only keep that data for as long as is required to complete those goals.
- Accuracy: To the degree required for the purposes for which it is to be used, organizations must make sure that personal information is accurate, full, and up to date.
- Safeguards: To prevent loss, theft, unauthorized access, disclosure, copying, use, or alteration of personal information, organizations must put in place the necessary organizational, technological, and physical safeguards.

- Openness: Businesses need to be open and honest about their privacy rules, practices, and methods for handling personal data. People must be able to obtain information regarding the organization's privacy practices and rules.
- Individual Access: People are entitled to view their personal data that is stored by an organization upon request. They can also contest the data's completeness and correctness and request that it be corrected as necessary.
- Accountability: It is the responsibility of organizations to adhere to the guidelines and regulations set forth by PIPEDA. This includes designating a privacy officer, putting policies and procedures in place, educating employees about privacy concerns, and attending to people's questions and grievances.

B.6.2 Impact on Proximity Marketing

When it comes to proximity marketing, PIPEDA governs the gathering, use, and sharing of personal data about persons, including location-based information gleaned via Bluetooth, Wi-Fi, and GPS devices. PIPEDA has the following effects on proximity marketing:

- Requirements for Consent: Before collecting and using people's personal information for marketing reasons, organizations that use proximity marketing must have their informed consent. People must be aware of the reasons why their data will be used and give their voluntary consent.
- Purpose Limitation and Data reduction: In order to guarantee that personal data gathered by proximity technology is utilized exclusively for designated and legal objectives, proximity marketing campaigns must abide by the principles of purpose limitation and data reduction. Companies should refrain from gathering an excessive amount of data that is not directly related to their marketing initiatives.
- Security and Safeguards: Companies need to put in place the right measures to prevent illegal access, use, or disclosure of personal data obtained through proximity marketing. To reduce the danger of data breaches, this entails frequent security assessments, access controls, secure data encryption, and secure storage techniques.
- Individual Access and Correction: People are entitled to see the personal data that businesses using proximity marketing are holding on them. Additionally, they are entitled to request that any incomplete or erroneous information be corrected. Companies are required to guarantee that people can access their personal data and to reply to these requests in a timely manner.
- Accountability and Compliance: It is the duty of organizations to exhibit adherence to the guidelines and regulations set forth by PIPEDA. When introducing new proximity marketing campaigns, entails keeping track of consent, recording data processing operations, and performing privacy effect analyses.
- Cross-Border Data Transfers: Under PIPEDA, companies must notify individuals if their personal data is going to be processed or moved outside of Canada or to third parties. When transmitting sensitive data over international boundaries, organizations need to be sure that sufficient security measures are in place to protect it.

Organizations can demonstrate appropriate data management practices in proximity marketing initiatives, reduce legal risks, and gain consumer trust by abiding by PIPEDA's principles and regulations. Respecting people's right to privacy, being transparent, and using personal information for marketing purposes in an ethical manner are all encouraged by PIPEDA compliance.

B.7 Personal Data Protection Act (PDPA)

B.7.1 Principles and Requirements

Singapore's comprehensive data protection law, known as the Personal Data Protection Act (PDPA), regulates how private sector firms gather, use, and disclose personal data. In order to guarantee that companies manage personal data in an ethical and transparent manner, the PDPA lays out important guidelines and standards. The following are the PDPA's fundamental ideas and specifications:

- Consent: Before collecting, using, or revealing an individual's personal information, an organization must get that individual's consent. For certain purposes, informed consent must be sought.
- Limitation on Purpose: Personal information may only be gathered, utilized, or shared for reasons that a reasonable person would find acceptable under the circumstances and that the person has been made aware of.
- Notification Organizations are required to notify individuals at the time of collection or prior, to the reasons for which their personal data is being collected, used, or disclosed.
- Access and Correction: People are entitled to ask for access to the personal information that is kept on them by an organization, as well as the correction of any information that is incorrect.
- Organizations that collect personal data that is likely to be used in making decisions that may have an impact on the individual or that will be disclosed to another organization are required to take reasonable steps to ensure that the data is accurate and complete.
- Protection Obligation: Organizations are required to take adequate security measures to guard against unauthorized access, collection, use, disclosure, copying, modification, disposal, and other hazards involving personal data that they own or control.
- Limit on Retention: No personal information may be kept around for longer than is required to achieve the goals for which it was gathered. It is imperative for organizations to create and execute rules and protocols for the storage and disposal of personal information.
- Move Limitation: Companies need to make sure that any personal information they move outside of Singapore is safeguarded to a level that is on par with the PDPA.
- Openness Requirement: Organizations must create and put into effect the policies and procedures required to fulfill their PDPA duties. They also have to provide information upon request regarding their data protection policies, procedures, and complaints procedures.
- Data Breach Notification: When there is a possibility that a data breach may cause the impacted individuals substantial harm, organizations are required to notify both the Personal Data Protection Commission (PDPC) and the affected individuals.

B.7.2 Impact on Proximity Marketing

The Personal Data Protection Act (PDPA) has a substantial impact on proximity marketing activities in a number of ways, particularly with regard to the gathering, utilizing, and sharing of personal data acquired via proximity technologies such as Bluetooth, Wi-Fi, and GPS. The PDPA has the following effects on proximity marketing:

- Getting agreement: Before collecting a person's location data for proximity marketing purposes, organizations must get that person's explicit and informed agreement. This entails making certain that people are aware of the types of data being gathered, how they will be used, and with whom they will be shared. Consent procedures can not be taken for granted and need to be made clear.
- Transparency and Notification: Individuals must be made fully aware of the reasons behind the collection of their location data by organizations. This could entail providing thorough alerts or privacy policies that outline the precise goals of proximity marketing and are accessible at data-gathering locations.
- Data Purpose Limitation and Minimization: Only information required for the proximity marketing campaign ought to be gathered. Businesses need to make sure that the information they gather is only utilized for the reasons disclosed to individuals and not for other purposes.
- Data Quality and Accuracy: Businesses need to make sure that the location data they utilize for proximity marketing is current and correct. This is essential for producing pertinent marketing content and identifying the correct audience to target.
- Data Security: To safeguard personal information, proximity marketing initiatives need to put strong security measures in place. This entails safe data access rules, encryption of data while it's being transmitted and stored, and routine security audits to stop breaches or unwanted access.
- Retention standards: To make sure that personal information obtained through proximity marketing is not retained longer than necessary, organizations need to set explicit standards for the retention of data. This entails going over data on a regular basis and securely discarding information that is no longer required.
- Data Transfer to Third Parties: Organizations must make sure that any transfers of personal data to third parties or outside of Singapore abide by the PDPA's regulations. The data must be adequately protected, and people must be made aware of any transfers of such information.
- Individual Rights: Businesses must support people's requests to view and amend their personal data. This entails setting up systems that make it simple for people to submit these kinds of requests and guarantee prompt replies.
- Data Breach Management: Procedures for locating, handling, and disclosing data breaches are essential for proximity marketing initiatives. Organizations are required to promptly notify the PDPC and impacted parties in the event of a breach, providing a detailed account of the breach's nature and the actions being taken to minimize its impact.
- Accountability and Compliance: Data Protection Officers (DPOs) are designated by organizations to supervise adherence to the Data Protection Act (PDPA), provide recurring training for personnel handling data, and keep thorough records of data protection procedures.

Organizations using proximity marketing can show their dedication to data privacy, avoid fines from the law, and increase consumer trust by adhering to the PDPA. Privacy concerns must be incorporated into proximity marketing efforts at every stage, from data collection and processing to storage and disposal, in order to ensure compliance.

The table B.1 offers a thorough summary of the many data protection laws that apply in various jurisdictions, emphasizing their main tenets and prerequisites as well as how they specifically affect proximity marketing strategies. The basic tenets, legal requirements, and geographic applicability of each regulation are explained. The chart also lists each regulation's consequences for proximity marketing, including the necessity of explicit consent, openness in data collecting and processing procedures, rights of data subjects, and the implementation of data protection laws. This comparison draws attention to the differences in regulatory frameworks and emphasizes how companies using proximity marketing must adjust to various legal requirements in order to maintain compliance and safeguard customer privacy.

Regulation	Region	Key Principles and Requirements	Impact on Proximity Marketing
General Data Protection Regulation (GDPR)	European Union	▪ Lawfulness, fairness, and transparency ▪ Purpose limitation ▪ Data minimization ▪ Accuracy ▪ Storage limitation ▪ Integrity and confidentiality ▪ Accountability	▪ Requires explicit consent for data collection ▪ Strict regulations on data processing and storage ▪ Right to access and erasure (Right to be forgotten) ▪ Heavy fines for non-compliance
California Consumer Privacy Act (CCPA)	California, USA	▪ Right to know about the personal data collected ▪ Right to delete personal data ▪ Right to opt-out of the sale of personal data ▪ Non-discrimination for exercising privacy rights	▪ Must provide clear notices about data collection practices ▪ Enable opt-out mechanisms for consumers ▪ Increased transparency and consumer control over data ▪ Penalties for non-compliance

Regulation	Region	Key Principles and Requirements	Impact on Proximity Marketing
California Privacy Rights Act (CPRA)	California, USA	▪ Enhances and amends CCPA ▪ Creates the California Privacy Protection Agency (CPPA) ▪ Introduces the concept of "sensitive personal information" ▪ Data minimization and storage limitation	▪ Stricter requirements for handling sensitive personal information ▪ Greater consumer rights to correct inaccurate personal data ▪ Mandatory risk assessments and cybersecurity audits
Colorado Privacy Act (CPA)	Colorado, USA	▪ Data rights similar to CCPA/CPRA ▪ Right to opt-out of targeted advertising ▪ Data protection assessments ▪ Transparency and purpose specification	▪ Requires controllers to conduct data protection assessments ▪ Enhanced consumer rights to access, correct, and delete data ▪ Obligations to disclose data processing activities
Lei Geral de Proteção de Dados (LGPD)	Brazil	▪ Lawfulness, necessity, and transparency ▪ Purpose specification ▪ Data quality ▪ Security measures ▪ Accountability	▪ Requires explicit consent for data collection ▪ Data subject rights to access, correction, and deletion ▪ Mandatory data breach notification ▪ Penalties for non-compliance

Regulation	Region	Key Principles and Requirements	Impact on Proximity Marketing
Personal Information Protection and Electronic Documents Act (PIPEDA)	Canada	▪ Accountability ▪ Identifying purposes ▪ Consent ▪ Limiting collection ▪ Limiting use, disclosure, and retention ▪ Accuracy ▪ Safeguards ▪ Openness ▪ Individual access ▪ Challenging compliance	▪ Requires consent for data collection and use ▪ Obligates organizations to protect personal data ▪ Provides individuals with rights to access and correct data ▪ Mandatory breach notification under certain circumstances

Regulation	Region	Key Principles and Requirements	Impact on Proximity Marketing
Personal Data Protection Act (PDPA)	Singapore	▪ Consent ▪ Purpose limitation ▪ Notification ▪ Access and correction ▪ Accuracy ▪ Protection ▪ Retention limitation ▪ Transfer limitation ▪ Accountability	▪ Requires consent for data collection ▪ Obligates organizations to disclose purposes for data collection ▪ Provides rights to access, correct, and withdraw consent ▪ Obligates data protection measures and breach notifications

Table B.1: Comparison of Regulatory Frameworks

Fatima CHAHAL

Doctorat : Systèmes SocioTechniques

Année 2024

Approches distribuées pour les environnements de commerce de proximité

Le marketing de proximité consiste à communiquer des messages ciblés et adaptés aux consommateurs en fonction de leur localisation géographique, en temps réel. L'envoi d'offres pertinentes en fonction de la localisation des utilisateurs permet aux entreprises d'interagir efficacement avec eux et de renforcer l'interaction client. Cependant, ce domaine fait face à des défis : les problèmes de sécurité des données, de confidentialité et de confiance freinent l'adoption généralisée. De plus, les mécanismes de consentement actuels sont souvent inadéquats, offrant aux utilisateurs un contrôle limité sur leurs données. De nombreux clients se méfient de la manière dont leurs informations sont collectées et utilisées, soulevant des inquiétudes en matière de transparence. Les solutions en place demeurent limitées et ne répondent pas pleinement aux préoccupations des utilisateurs. Pour combler ces lacunes, Nous proposons des stratégies distribuées axées sur l'instauration de la confiance dans le domaine. Nous examinons la confiance sous trois angles : protocoles, processus de consensus et interactions entre acteurs. En améliorant la sécurité des protocoles, nous visons à protéger les utilisateurs contre le suivi non autorisé. Nous proposons également une nouvelle méthode de consensus pour garantir l'intégrité des données et la transparence dans la prise de décision. Enfin, un nouveau mécanisme de classification donne aux utilisateurs plus de contrôle sur leurs données, renforçant la confiance entre consommateurs et détaillants.

Mots clés : marketing de proximité – traitement réparti – confiance numérique – réseaux locaux sans fil – consensus – système de communication sans fil – consentement.

Distributed Approaches for Proximity Marketing Environments

Proximity marketing involves communicating targeted messages tailored to consumers based on their geographic location, in real-time. Sending relevant offers based on users' locations allows companies to effectively engage with them and boost customer engagement. However, this field faces challenges: Data security, privacy, and trust issues are hampering widespread adoption. Additionally, current consent mechanisms are often inadequate, providing users with limited control over their data. Many customers are worried about how their information is collected and used, raising transparency concerns. Existing solutions remain limited and do not fully address user concerns. To address these gaps, our research proposes distributed strategies focused on building trust in proximity marketing. We examine trust from three perspectives: protocols, consensus processes, and actor interactions. By improving the security of network protocols, we aim to protect users from unauthorized tracking. We also propose a new consensus method to ensure data integrity and transparency in decision-making. Finally, a new classification mechanism gives users more control over their data, strengthening trust between consumers and retailers.

Keywords: proximity marketing – electronic data processing, distributed processing – digital trust – wireless LANs – consensus – wireless communication system – consent.