Kingdom of Saudi Arabia
Ministry of Education
Qassim University
College of Computer
Information Technology Dept.

المملكة العربية السعودية
وزارة التعليم
جامعة القصيم
كلية الحاسب
قسم تقنية المعلومات

# SecureJoin: Web-based Platform for Secure Group Access

*Students:*

| | |
|---|---|
| **Fai Alrasheed** | **391202139** |
| **Hanan Alshoshan** | **412205599** |
| **Sarah Almuzaini** | **421202238** |
| **Shaden Alawaji** | **421202289** |

*Supervisor:*

**Dr. Ahmad Reeves**

*A project report submitted in partial fulfillment of the requirements for B.Sc. degree in Information Technology. Qassim-Saudi Arabia*

*1446 (2024/2025)*

# Certificate

It is certified that the project report has been prepared and written under my direct supervision and guidance. The project report is approved for submission for evaluation.

**Dr. Ahmad Reeves**

# Dedication

﴿ وَآخِرُ دَعْوَاهُمْ أَنِ الْحَمْدُ لِلَّهِ رَبِّ الْعَالَمِينَ ﴾
الحمد لله ما انتهى درب، ولا خُتِم جهد، ولا تمَّ سعيٌ إلا بفضله وكرمه.

We dedicate this work with deep gratitude to those who supported us throughout our journey. To our beloved parents, whose unwavering love, prayers, and encouragement have been the foundation of our strength and perseverance.

We thank our families for their constant support, patience and belief in our abilities, which inspired us to move forward even during challenging times.

We thank our esteemed professors, who provided invaluable knowledge, guidance, and mentorship, shaping not only our academic paths, but also our professional futures.

And to our beloved country, for giving us the opportunity, resources, and pride to pursue our education and strive for excellence.

This achievement is not ours alone; it belongs to all those who believed in us, supported us, and made this journey possible.

**The SecureJoin Project Team**

# Abstract

The rise of digital communication platforms like WhatsApp and Telegram has revolutionized connectivity but also introduced significant challenges, including spam, unauthorized access, and the lack of robust user verification in public chat groups. Studies highlight how messaging platforms, despite implementing end-to-end encryption, remain vulnerable to threats such as metadata exploitation and unauthorized group entry Rastogi and Hendler et al. [1], SecureJoin addresses these vulnerabilities with an innovative web-based platform designed to enhance group access security through customizable, multilayered verification mechanisms.

SecureJoin empowers group administrators by integrating features such as one-time use credentials, including email verification, SMS verification, and customized verification questions. These functionalities prevent unauthorized entry, reduce spam, and ensure that only legitimate members gain access. The platform also prioritizes usability, offering an intuitive interface for seamless management and integration with popular messaging platforms.

Through user feedback and rigorous testing, the project aims to establish a scalable, reliable, and user-friendly solution to manage group access in various contexts, including educational, professional, and community settings.

This report presents a comprehensive overview of the SecureJoin project, covering all key phases including research, design, implementation, testing, and result analysis. By targeting critical security gaps, SecureJoin supports the goals of the **Saudi Vision 2030 digital transformation initiative**, contributing to a safer and more efficient digital ecosystem. The platform development process, features, and potential to redefine secure group communication standards are discussed in detail.

# Table of Contents

# List of Figures

# List of Tables

# Chapter 1

# INTRODUCTION

# CHAPTER ONE INTRODUCTION

## 1.1 Introduction

In today's digital age, communication platforms such as WhatsApp and Telegram have become integral to daily life, facilitating instant interaction among users across the globe. However, the rise of public chat groups on these platforms has led to significant challenges, particularly with regard to security and user integrity. The ease of sharing group-join links has opened the door to spam, unauthorized access, and the proliferation of unwanted content, creating environments where genuine users often find themselves overwhelmed and frustrated.

Building on previous research that highlighted security vulnerabilities and privacy risks in messaging platforms such as Rastogi and Hendler [1] and in broader social network environments as noted by Nawaz et al. [2], the SecureJoin project proposes a web-based platform designed to enhance the security of group access by implementing a comprehensive verification system. This system verifies the authenticity of users before they join chat groups and improves the overall quality of interactions within these groups. Using a multilayered approach that includes custom verification questions, verification messages by email or SMS, and one-time-use credentials, SecureJoin aims to provide a robust solution tailored to the unique needs of various group contexts, including educational institutions and professional organizations.

## 1.2 Problem Statement and Motivations

Public chat groups face critical vulnerabilities that undermine the user experience and the integrity of group interactions. The primary problem lies in the ease with which unauthorized users can access these groups. This unrestricted access often results in the influx of spam, irrelevant advertisements, and harmful content, detracting from the purpose of the group and causing frustration among legitimate members. Additionally, group administrators struggle to maintain control over membership, leading to challenges in fostering a safe and engaging environment.

Recent literature emphasizes that traditional verification and authentication practices on social media platforms are often inadequate, relying on weak user validation methods that expose groups and users to heightened risks of spam, unauthorized access, and identity misuse

Herath et al. [3]. The motivations behind the SecureJoin project stem from the urgent need to create a secure, user-friendly solution that empowers group administrators while protecting genuine users. By offering a customizable verification process that adapts to the specific needs of each group, SecureJoin aims to enhance security and significantly reduce the risk of unauthorized access.

Moreover, the platform's proposed features—such as one-time-use credential verification (via email, SMS, and custom verification questions) and seamless integration with popular messaging applications—underscore its potential to set a new standard in group access management. In a landscape where digital interactions are increasingly scrutinized for security, SecureJoin not only addresses current challenges but also lays the groundwork for a more secure and collaborative online community.

## 1.3 Goals and Objectives

The primary goal of the SecureJoin project is to develop a web-based platform that enhances the security and integrity of group access on popular messaging applications like WhatsApp and Telegram. This goal will be achieved through a multi-layered verification process designed to authenticate users before granting them access to chat groups. The specific objectives of the project are as follows:

i. **Custom Verification Questions:** Implement a feature that allows group administrators to create tailored verification questions specific to their group's context. This will improve security by ensuring that only users who possess relevant knowledge or credentials can join the group.

ii. **Verification Messaging System:** Develop a robust verification messaging system where users receive unique verification codes via email or SMS. Users must enter these codes to confirm their identity, adding an extra layer of security to the joining process.

iii. **Prevent Credential Reuse:** Design the platform to ensure that once a user has been admitted to a group, their access credentials (such as email or phone number) cannot be reused for future entries. This measure will prevent unauthorized sharing of credentials and enhance overall group security.

iv. **Seamless Integration with Messaging Platforms:** Ensure that SecureJoin can be seamlessly integrated with popular messaging applications. This integration will allow for automated group membership control based on the verification process established by the platform.

v. **User-Friendly Interface:** Develop an intuitive and user-friendly interface that simplifies the process for group administrators to manage verification questions and authorized user verifications, facilitating ease of use and accessibility.

vi. **Alignment with Vision 2030:** Support the "Digital Transformation" initiative of Vision 2030 by promoting cybersecurity and digital innovation, contributing to a more secure and user-friendly digital ecosystem.

These objectives collectively aim to provide a comprehensive solution to the challenges posed by unauthorized access and spam in public chat groups, ultimately fostering a safer and more productive online community.

## 1.4 Study Scope

The scope of the SecureJoin project includes the design, development, and implementation of a web-based platform for secure group access on popular messaging applications like WhatsApp and Telegram. The project will cover the following key areas:

i. **Target User Groups:** The platform will cater to educational institutions, professional organizations, and community groups that require secure and controlled access to their messaging environments.

ii. **Verification Methods:** SecureJoin will implement custom verification methods, including tailored verification questions and unique verification codes sent via email or SMS. This multifaceted approach aims to enhance user authentication and reduce unauthorized access.

iii. **Integration and Compatibility:** The project will focus on integrating SecureJoin with existing messaging platforms, ensuring seamless compatibility and operational efficiency.

iv. **Usability and User Experience:** A primary goal is to create an intuitive user interface that facilitates easy navigation for group admins and members, prioritizing a positive user experience.

v. **Security Features:** The platform will implement robust security measures, including preventing credential reuse and ensuring data protection, aligning with best practices in cybersecurity.

**Limitation:** The study will also address certain limitations, such as:

- Platform Dependency: SecureJoin's effectiveness may vary depending on the specific APIs and functionalities provided by different messaging platforms.
- User Adoption: The success of the platform relies on user acceptance and willingness to adopt new verification practices, which could vary across different demographics.

By clearly delineating these aspects, the project aims to provide a focused solution that meets user needs while acknowledging the challenges and limitations inherent in the development and implementation of SecureJoin.

## 1.5 Study Plan and Schedule

The study plan for the SecureJoin project outlines a structured approach to ensure the timely completion of key phases, based on the Work Breakdown Structure (WBS) and accompanying Gantt chart. This plan details tasks, duration, and the timeline for the project's various components.

**Work Breakdown Structure (WBS)**

1. Project Planning and Research

   1.1. Define project objectives and scope

   1.2. Research similar platforms, technologies, and security practices

   1.3. Identify user requirements and target platforms (messaging/communication)

   1.4. Gather information on APIs (WhatsApp, Telegram, etc.)

   1.5. Identify databases for user authentication and verification

2. Report Drafting (Introduction, Literature Review, Methodology)

    2.1. Draft Chapter 1: Introduction

        2.1.1. Define the problem statement

        2.1.2. Outline project goals and significance

    2.2. Draft Chapter 2: Literature Review

        2.2.1. Research existing solutions, methodologies, and technologies

        2.2.2. Review verification and security methods for messaging platforms

    2.3. Draft Chapter 3: Methodology

        2.3.1. Define technical implementation (frontend, backend, database, APIs)

        2.3.2. Identify tools and technologies (e.g., Node.js, React, MySQL)

        2.3.3. Outline testing strategies and security measures

3. Platform Design and Development (The second stage)

    3.1. Design User Interface

        3.1.1. Design admin dashboard for creating verification questions

        3.1.2. Design user registration and verification screens

    3.2. Backend Development

        3.2.1. Set up authentication system using one-time-use credentials (email/SMS and custom questions)

        3.2.2. Develop API integration with messaging platforms

    3.3. Database Implementation

        3.3.1. Configure and test basic user data storage

    3.4. Testing and Debugging

        3.4.1. Perform unit testing for each module

        3.4.2. Conduct user acceptance testing

4. Final Presentation

    4.1. Prepare project slides

        4.1.1. Summarize problem statement, objectives, and research findings

4.1.2. Present preliminary design concepts

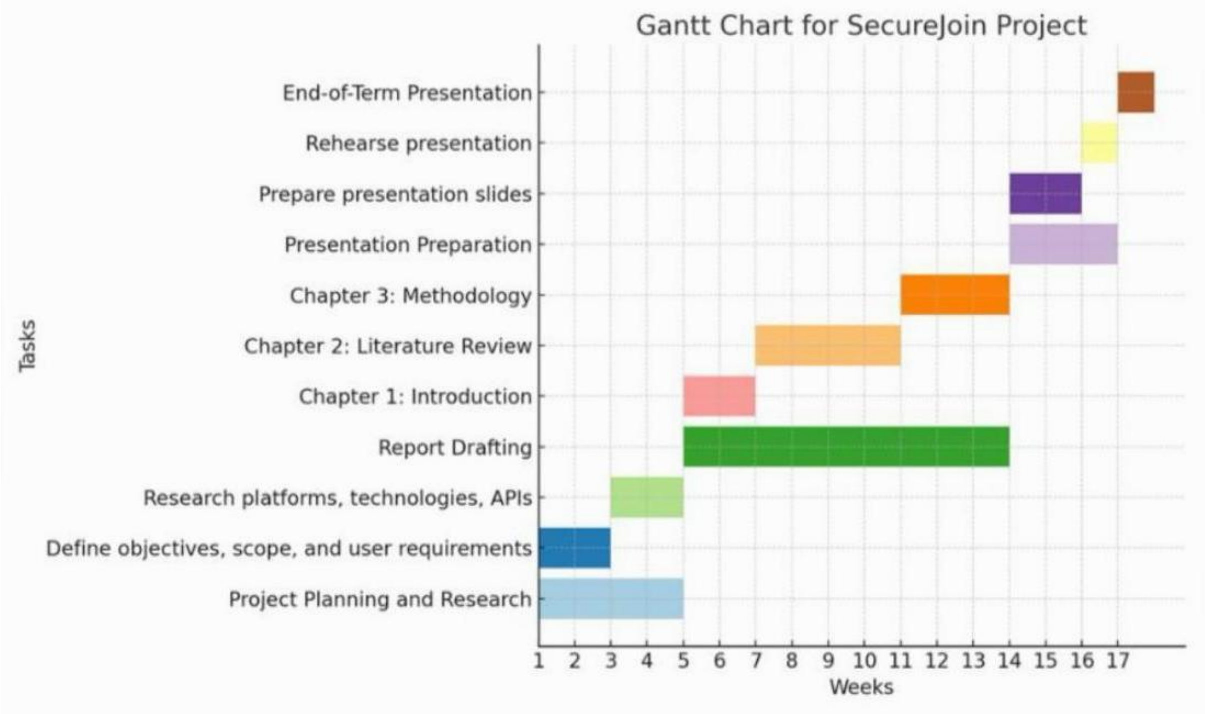
4.2. Rehearse presentation

**Gantt Chart (First Stage)**

Table 1.1: First Stage

| Task | Duration (Weeks) | Timeline |
|---|---|---|
| **Project Planning and Research** | 4 | Week 1-4 |
| - Define objectives, scope, and user requirements | 2 | Week 1-2 |
| - Research platforms, technologies, APIs | 2 | Week 3-4 |
| **Report Drafting** | 9 | Week 5-13 |
| - Chapter 1: Introduction | 2 | Week 5-6 |
| - Chapter 2: Literature Review | 4 | Week 7-10 |
| - Chapter 3: Methodology | 3 | Week 11-13 |
| **Presentation Preparation** | 3 | Week 14-16 |
| - Prepare presentation slides | 2 | Week 14-15 |
| - Rehearse presentation | 1 | Week 16 |
| **End-of-Term Presentation** | 1 | Week 17 |

Figure 1.1: First Stage Gantt Chart



This study plan provides a clear roadmap for the SecureJoin project, detailing the tasks to be accomplished, their respective duration, and the overall timeline. Each phase of the project is carefully structured to ensure thorough research, effective drafting, and successful presentation of findings. By adhering to this schedule, the team aims to achieve its objectives efficiently and effectively.

## 1.6 Organizing of the Chapters

This section provides an overview of the report's structure, highlighting the content and objectives of each chapter in the SecureJoin project.

The **Introduction** chapter serves as the foundation of the report, presenting the SecureJoin project and outlining the context of digital communication and its associated security challenges. It begins with an overview of the vulnerabilities faced by public chat groups, followed by a detailed exploration of the motivations behind developing SecureJoin as a solution. This chapter establishes the project's goals and objectives, clarifies the study's scope, and introduces the study plan and schedule, including a Work Breakdown Structure (WBS) and Gantt chart.

The **Literature Review** chapter provides crucial context by examining existing research related to the project. It introduces four key themes—security in social media, authentication in group chats, rule-based spam detection, and usability in security systems—offering a comprehensive understanding of the challenges SecureJoin addresses. It concludes by identifying gaps in the current literature that the SecureJoin platform aims to fill.

The **Methodology** chapter articulates the research approach adopted for the study. It defines the type of study conducted, details the survey findings used to inform platform development, and outlines the methodology used for requirements gathering, data collection, data analysis, system design, and prototyping. This chapter also explains how feedback and iterative development were used to refine the platform throughout its creation.

The **Implementation** chapter presents the technical realization of SecureJoin. It describes the tools, technologies, and programming languages utilized, outlines the system architecture and design, and explains the development of core components and interfaces. Additionally, it highlights the security measures incorporated to ensure the protection and integrity of group access.

The **Testing and Results** chapter evaluates the performance and usability of the SecureJoin platform. It discusses the system testing and software usability testing methodologies, presents the key findings from these tests, analyzes user feedback, and offers recommendations for future improvements based on the results.

The **Conclusion and Future Work** chapter summarizes the project's major achievements, reflecting on key accomplishments, challenges encountered, and lessons learned during the project. It also proposes future enhancements for the SecureJoin platform, including advanced security features, improved accessibility options, and broader platform expansions.

Finally, the **Appendices** provide supplementary materials relevant to the project, while the **References** section lists all sources cited throughout the report, ensuring thorough academic documentation.

This organized structure ensures a logical, coherent flow of information throughout the report, making it accessible and comprehensive for the readers.

# Chapter 2

# LITERATURE REVIEW

# CHAPTER TWO
# LITERATURE REVIEW

## 2.1 Introduction

The literature review for the SecureJoin project is organized around four central themes that reflect key areas of research in developing secure group access solutions for digital communication platforms. This thematic structure provides a focused examination of the current landscape, highlighting essential insights, prevailing trends, and identifying gaps in existing solutions that SecureJoin aims to address.

### 2.1.1 Security in Social Media

The security challenges inherent in social media and digital communication platforms form the basis of this theme. Studies here examine a range of threats, from identity theft to data privacy issues, which are often exacerbated by the public nature of group links and insufficient privacy settings. These insights reinforce SecureJoin's mission to implement proactive, user-centered security measures that address broader social media vulnerabilities.

### 2.1.2 Authentication in Group Chats

This theme explores the foundational aspects of user verification and access control within group chats. With the increasing prevalence of platforms like WhatsApp and Telegram, ensuring secure and authorized access has become critical. Studies within this theme emphasize the importance of multi-layered authentication processes that enhance trust and protect group integrity, aligning closely with SecureJoin's use of customized verification questions, one-time credentials, and strong user identity verification practices.

### 2.1.3 Rule-Based Spam Detection

Addressing unauthorized access and spam, this theme delves into rule-based techniques for filtering and blocking unwanted activity in group chats. Rule-based systems provide a straightforward and adaptable approach, crucial for platforms managing dynamic user activity. Literature in this area outlines strategies such as keyword detection, user behavior analysis, and automated filtering—all elements that inform SecureJoin's spam prevention and user verification methods.

### 2.1.4 Usability in Security Systems

The final theme addresses the critical need for security systems to balance robustness with user accessibility. Research in this area shows that overly complex security features can lead to user errors, reducing system effectiveness. By incorporating user-friendly design principles, SecureJoin aims to ensure that group administrators and users can manage access seamlessly without compromising on security.

This chapter systematically reviews these themes to build a comprehensive understanding of the security, usability, and practical implications of managing group access securely. Each of these themes not only provides a distinct perspective on the challenges surrounding group chat security but also interconnects to form a holistic view of the requirements for a platform like SecureJoin. The synthesis of authentication mechanisms, spam prevention strategies, robust social media security practices, and user-centered design principles within this literature review builds a comprehensive foundation for SecureJoin's development. The insights gained from each theme will guide the development of SecureJoin, aligning the project with best practices and innovations in digital security. By integrating these diverse insights, SecureJoin will aim to provide a secure, efficient, and user-friendly solution tailored to the evolving needs of group chat users in both private and professional spheres. This chapter will delve into these themes in detail, demonstrating how they guide and inform SecureJoin's approach to creating a safer, more controlled group communication experience.

## 2.2 Related Work

### 2.2.1 Security in Social Media

The theme of security in social media has become increasingly critical as users engage more deeply with digital platforms for communication, information sharing, and networking. The vast amount of personal data exchanged on these platforms presents numerous vulnerabilities, including identity theft, phishing, and data breaches. These threats are often exacerbated by inadequate privacy settings and users' limited awareness of security risks. Consequently, ensuring the security of users on social media is essential for protecting personal information and maintaining user trust.

In response to these vulnerabilities, the literature emphasizes the need for robust security measures to effectively mitigate risks. Projects like SecureJoin aim to address these challenges by implementing proactive security mechanisms, including enhanced privacy controls, user education initiatives, and the integration of adaptable technological innovations. By focusing on user-centered designs and transparent security practices, SecureJoin seeks to empower users to manage their data securely while fostering a safer online environment.

**Key Points and Relation to SecureJoin Project Idea**

- User Awareness and Education Trust is crucial for user engagement in social media. Many users underestimate online risks and rely on perceived security rather than technical knowledge. This gap underscores the importance of educational initiatives to raise awareness about privacy settings and secure online behaviors. SecureJoin aligns with findings from Nawaz et al. [2], emphasizing the need to empower users to recognize and combat security threats effectively.

- Privacy Controls and User Trust The public nature of social media leaves users vulnerable to privacy invasions. Studies suggest that implementing visible and user-friendly security features enhances user trust. SecureJoin aims to incorporate intuitive privacy settings, allowing individuals to control their data visibility and sharing options, as supported by research Singh et al. [4].

- Technological Solutions Advanced technologies such as encryption methods present promising solutions for enhancing security in social media environments. While SecureJoin initially focuses on accessible and proven technologies like one-time-use credential verification, future work may explore more sophisticated innovations. This direction aligns with insights from Rastogi and Hendler [1], who advocate for balanced approaches that prioritize both user security and privacy.

- Impact on Mental Health The psychological effects of security breaches, particularly among vulnerable populations such as adolescents, are significant. Exposure to cyberbullying and privacy violations can lead to considerable emotional distress. SecureJoin recognizes the importance of creating supportive environments that prioritize user well-being. Lahti et al. [5] highlight the value of fostering safe online spaces to promote mental health, a principle that informs SecureJoin's design and implementation strategies.

**Conclusion** The theme of security in social media is multifaceted, necessitating a comprehensive approach that involves user education, robust privacy controls, and the integration of advanced technologies. The SecureJoin project aims to address these critical challenges by developing a platform that prioritizes user safety and enhances trust. By incorporating insights from existing research, SecureJoin can effectively tackle security vulnerabilities, promote safe online behaviors, and create a more secure digital landscape for all users.

### 2.2.2 Authentication in Group Chats

**Introduction**

Authentication in group chats has emerged as a critical focus in the development of secure communication platforms. With the rise of digital tools such as WhatsApp and Telegram, group chats have become integral to personal, academic, and professional collaboration. However, these platforms are vulnerable to security threats, including spam, unauthorized access, and breaches of privacy due to the ease with which group links can be shared. Ensuring the authenticity of users before granting them access is essential to maintaining the security and integrity of these communication spaces.

In response to these vulnerabilities, multi-layered authentication mechanisms have been proposed to prevent unauthorized access while enhancing user trust. Projects like SecureJoin aim to address these issues by implementing robust verification methods, including custom verification questions and one-time-use credentials. Future developments may explore database-linked verification for pre-approved memberships. These mechanisms are designed to ensure that only legitimate members are allowed into groups, addressing key security challenges while promoting trust among users.

**Key Points and Relation to SecureJoin Project Idea**

- **Trust and User Perception**

  Trust plays a central role in user participation within group chat environments. Research by Oesch et al. [6] highlights that users often rely on perceived security measures rather than technical knowledge to judge whether communications are secure. This perception of trust can be strengthened by implementing visible security features such as authentication mechanisms. SecureJoin's use of custom verification questions and one-time-use credentials aligns with the need to enhance user trust through transparent, user-friendly verification processes.

Oesch et al. [6] also note that many users distrust existing group chat tools despite the availability of end-to-end encryption, often due to a lack of visible security indicators. By providing a clear, multi-step authentication process, SecureJoin addresses this gap, promoting higher levels of trust among users, particularly when sensitive or confidential information is involved. This approach is further supported by findings from Chen et al. [7], who emphasize the importance of mutual authentication and secure key agreements.

- **Membership Verification and Access Control**

  Managing group membership is a significant challenge, especially where join links can be easily shared. SecureJoin tackles this issue through a multi-layered verification system, combining custom verification questions and one-time credentials. This system ensures that only verified users are granted access, significantly reducing the risk of unauthorized entry. This approach addresses concerns raised by Chen et al. [7], who argue that effective access control mechanisms are essential for maintaining privacy and security in group-based mobile chats. SecureJoin's approach directly addresses these concerns by enhancing membership verification procedures to maintain group integrity.

- **Managing Dynamic Group Membership**

  Group chat environments are often dynamic, with frequent member changes. This fluidity poses challenges in maintaining group integrity. SecureJoin addresses this by enabling administrators to create custom verification questions for new members, filtering unauthorized users based on specific knowledge relevant to the group.

  Oesch et al. [6], highlight how users often struggle to monitor group memberships, which can lead to privacy risks. SecureJoin's automated verification system offers an efficient solution, aligning with the insights from Diallo et al. [8], about managing dynamic group memberships in evolving digital spaces.

- **Preventing Unauthorized Sharing of Access Credentials**

  A key challenge is preventing unauthorized sharing of group join links. SecureJoin addresses this by implementing a one-time-use credential system, ensuring that once a user gains access, their information cannot be reused or shared. This effectively prevents unauthorized entry through shared credentials, a vulnerability common in many platforms.

  This issue is similarly addressed by Chen et al. [7] and Diallo et al. [8],emphasize the need for preventing credential reuse to maintain group security. SecureJoin's approach directly responds to these vulnerabilities, offering a more secure and controlled method of managing group access.

**Conclusion**

Authentication in group chats is central to ensuring the security and integrity of modern communication platforms. As group chats continue to grow in personal, professional, and educational settings, the need for robust authentication mechanisms becomes critical.

SecureJoin addresses these challenges through a multi-layered authentication system combining custom verification questions and one-time-use credentials. These features ensure that only legitimate users are granted access to groups, significantly reducing the risk of unauthorized entry and enhancing user trust.

By aligning its features with the key security concerns identified in the literature, SecureJoin offers a comprehensive solution to the vulnerabilities present in existing group chat systems. Its emphasis on preventing credential reuse and automating the verification process further strengthens its role as a secure, user-friendly tool for managing digital group communications.

### 2.2.3 Rule-Based Spam Detection

**Introduction**

The theme of rule-based spam detection addresses the growing challenge of spam in social media and group chats, where unauthorized users can easily join through shared links, compromising security. Rule-based systems rely on predefined rules to filter spam effectively. For SecureJoin, this approach ensures that only legitimate users gain access to groups, aligning with the project's mission to prevent spam and protect group integrity.

**Key Points**

- **Adaptability to Evolving Spam Patterns**

  Spam detection systems must adapt to the rapidly changing tactics employed by spammers. A systematic review by Kaddoura et al. [9], highlights the challenges of maintaining effective spam filters, noting that spammers continuously modify their strategies to bypass detection. Techniques such as dynamic keyword selection and frequent updates to filtering rules help systems remain resilient. SecureJoin can benefit by incorporating adaptable rule-based methods to secure group access dynamically as spam patterns evolve.

- **Rule-Based Content Filtering**

  Rule-based filters focus on detecting spam through keywords or identifiable message patterns. Sharma et al. [10] discuss how applying rule-based conditions, such as identifying commercial keywords in emails, can offer an efficient and lightweight spam detection method. While rule-based filters may not provide the learning capabilities of machine learning models, they present a straightforward preliminary screening approach suitable for SecureJoin's need to quickly and efficiently prevent unauthorized access to group chats.

- **Behavior Analysis and Spam Detection**

  Behavior analysis plays a crucial role in spam detection, especially on dynamic platforms. Kaddoura et al. [9] emphasize that behavioral characteristics, such as repetitive login attempts and malicious link sharing, can effectively signal spam activity. SecureJoin could enhance its user verification by analyzing login behaviors or interaction patterns to identify potential spammers before they gain access.

- **Automated Verification and Scalability**

  Automated rule-based systems significantly reduce the need for manual intervention, improving scalability and administrative efficiency. Sharma et al. [10] explain that automation based on IP addresses, domain patterns, and predefined behavioral rules enables platforms to focus resources on more critical management tasks. Implementing automated verification and lightweight spam detection within SecureJoin ensures a scalable and user-friendly process for group management.

- **Real-Time Detection and Prevention**

  Real-time spam detection is essential for securing dynamic environments. Kaddoura et al. [9] stress that real-time rule-based and machine learning hybrid systems can prevent spam from entering platforms by blocking suspicious activity immediately. Although SecureJoin primarily relies on rule-based verification for now, future enhancements could incorporate real-time spam detection capabilities to further secure group communication.

- **Distributed Detection for Enhanced Scalability and Reliability**

  As spam activities grow in volume and complexity, distributed frameworks for spam detection become increasingly important. Kaddoura et al. [9] propose a Distributed Large-Scale Anti-Spam System (DLSAS) for decentralized environments, demonstrating that distributed spam filtering improves system reliability and processing speeds. While SecureJoin initially adopts a centralized architecture, exploring distributed detection models could represent a future direction for scaling the platform securely.

**Conclusion**

Rule-based spam detection offers a foundational approach to preventing unauthorized access in group chats. With the rise of spam activities in digital communication, platforms like SecureJoin can leverage lightweight, adaptable rule-based systems to filter out potential spammers effectively.

By aligning its design with proven methodologies in spam detection, SecureJoin aims to implement a scalable, automated verification system that adapts to changing patterns and enhances group security. These measures will help ensure that SecureJoin remains efficient and resilient even as user activity increases, supporting the platform's mission to offer a safe and trustworthy group communication experience.

### 2.2.4 Usability

The theme of usability in security systems emerged from the need to bridge the gap between technically robust security solutions and user accessibility. Initially, security-focused tools prioritized functionality over user experience, often resulting in high error rates and low adoption as users struggled with complex requirements. This approach frequently led users to bypass or disable essential security features, creating vulnerabilities that ultimately defeated the purpose of these protections.

For example, studies such as Usability of Security: A Case Study illustrate that poorly designed systems often cause user errors that compromise security, as seen with PGP 5.0, where complex interfaces led users to misconfigure settings and undermine overall system effectiveness [11].

**Key Points and Relation to SecureJoin Project Idea**

- **Minimizing User Errors through Usable Security:** Saltzer and Schroeder [11]emphasize that security features lacking usability can significantly increase the frequency of user errors, ultimately reducing the effectiveness of overall system security. Their case study illustrates that even in technically robust systems such as PGP 5.0, complex design elements led users to misconfigure settings, undermining intended security objectives. Drawing on these insights, SecureJoin focuses on developing a user-centered interface with streamlined verification processes to ensure that users can authenticate smoothly and accurately, minimizing confusion and preventing errors that could compromise group access integrity.

- **Simplifying Authentication to Promote User Engagement:** Juels and Wattenberg [12]found that complex, multi-step authentication methods, such as Time-Based One-Time Passwords (TOTP), negatively impact user adoption due to setup difficulties and increased error rates during interactions. Their usability study demonstrated that users are more likely to abandon or misuse authentication systems that require extensive configuration or involve confusing steps. Informed by these findings, SecureJoin adopts simpler verification methods, such as SMS or email codes, which minimize setup complexity and reduce the likelihood of user errors, thereby facilitating smoother and more accessible onboarding for users joining chat groups.

- **Balancing Security with User-Friendliness:** Hong et al. [13]emphasize that achieving an effective balance between strong security measures and user-friendliness is critical to preventing users from adopting insecure shortcuts. Their study on user authentication methods revealed that when systems are overly complex or burdensome, users are more likely to bypass essential security features, thereby compromising overall system integrity. Applying these insights, SecureJoin implements a multi-layered but straightforward verification process designed to maintain high security standards while ensuring that users can navigate authentication procedures easily and without frustration, ultimately promoting stronger compliance and system trust.

- **Understanding User Perceptions to Refine Security Tools:** Schneier et al. [14] suggest that addressing user perceptions is critical for developing security systems that users are willing to adopt and trust. Their evaluation of multi-factor authentication methods highlights that systems perceived as overly complex or intrusive are often rejected, even when technically secure. Building on these findings, SecureJoin emphasizes the importance of integrating user feedback throughout the platform's development process. By continuously refining its verification methods based on user perceptions, SecureJoin aims to ensure that users feel both comfortable and secure during the onboarding process, thereby enhancing adoption and trust in the system.

- **Tailoring Security Features to User Preferences:** Clarke et al. [15] argue that user familiarity with authentication methods significantly increases both acceptance and usability of security systems. Their study on authentication preferences in eBanking environments found that users are more willing to adopt security measures that align with their previous experiences and comfort levels. Informed by these findings, SecureJoin prioritizes understanding user preferences and familiarity with different verification options. By tailoring the platform's design to offer authentication methods that users are more likely to accept and trust, SecureJoin aims to enhance both the usability and overall adoption of its secure group access solution.

### Conclusion

The reviewed studies offer valuable insights that directly inform the design principles adopted by SecureJoin. Saltzer and Schroeder [11] underscore the necessity of minimizing system complexity to prevent user errors that could compromise security objectives. Informed by this, SecureJoin prioritizes user-centered design, aiming to create an authentication experience that is intuitive and error-resistant. Similarly,Juels and Wattenberg [12] demonstrate that users are more likely to adopt simpler authentication mechanisms, supporting SecureJoin's strategy of implementing streamlined verification methods, such as SMS and email codes, to facilitate smooth user onboarding.

The importance of balancing strong security with ease of use is highlighted by Hong et al. [13] who argue that overly complicated systems often drive users toward insecure practices. SecureJoin addresses this concern by maintaining a balance between multi-layered security and user accessibility. Furthermore, Schneier et al.[14] advocate for the continuous incorporation of user feedback into security tool development. SecureJoin embraces this approach by integrating iterative improvements based on user experience, thereby enhancing trust and system usability.

Finally, the findings of Clarke et al.[15] emphasize that aligning authentication methods with user preferences significantly improves adoption and trust. SecureJoin incorporates this understanding by offering familiar, user-preferred verification options, further strengthening user engagement. By synthesizing these insights, SecureJoin aims to deliver a secure, user-friendly platform that effectively supports safe and efficient group communications.

## 2.3 Thematic Analysis

### 2.3.1 Security in Social Media

The theme of **Security in Social Media** emphasizes the need to systematically identify and analyze recurring patterns of security threats across online social networks (OSNs). As the complexity of these threats continues to evolve, understanding user experiences and perceptions becomes crucial for devising effective mitigation strategies. Research highlights several key dimensions in this area, notably user awareness, the diversity of attack vectors, and the design of response mechanisms, all of which contribute to a comprehensive understanding of the security landscape.

**User Awareness and Education** User awareness significantly impacts the effectiveness of security measures within OSNs. Numerous studies suggest that many users remain unaware of potential threats, often relying passively on built-in platform protections without fully understanding their limitations. This gap in awareness fosters complacency, making users prime targets for phishing, social engineering, and similar attacks. Enhancing user education through targeted and engaging training initiatives can empower individuals to better recognize and respond to security threats.
**- Strength:** Prioritizing user education fosters a more informed user base capable of proactively identifying and avoiding security risks.
**- Limitation:** However, designing engaging and effective educational content presents challenges, particularly as users exhibit varying levels of interest and engagement. Tailoring security messaging to different demographics may help mitigate this issue.

Another significant aspect is the **Diversity of Attack Vectors** threatening social media platforms, including malware distribution, phishing campaigns, and identity theft. Each attack vector exploits specific user behaviors or technological vulnerabilities, requiring nuanced understanding to develop effective defenses.
**- Strength:** A multifaceted approach that addresses multiple attack vectors can lead to the creation of robust, adaptable security frameworks.
**- Limitation:** Nevertheless, the continuous evolution of attack strategies demands regular updates to both technical defenses and user training, potentially stretching organizational resources over time.

Additionally, **Response Mechanisms** are essential in mitigating the impact of security incidents. Automated response systems capable of monitoring user behavior and detecting anomalies in real time offer a proactive defense strategy.

**- Strength:** Automated systems enhance an organization's ability to address threats quickly, thereby narrowing the window of exposure to potential attacks.

**- Limitation:** However, an overreliance on automated detection can result in false positives, which may desensitize users and erode trust. Balancing sensitivity and specificity in detection algorithms is critical to maintaining system credibility.

In conclusion, the thematic analysis of security in social media offers a foundational framework for understanding and addressing the challenges faced by OSNs. Insights into user awareness, diverse attack vectors, and effective response mechanisms illuminate areas ripe for improvement and innovation. By emphasizing user education, adapting to evolving threats, and implementing robust response strategies, OSNs can enhance their security posture while fostering user trust. Ongoing engagement with the user community and iterative improvements to security protocols will be vital in navigating the complex landscape of online threats.

### 2.3.2 Authentication in Group Chats

The **Authentication in Group Chats** theme examines the essential security measures needed to control access to digital group communication spaces. With platforms like WhatsApp and Telegram increasingly used for sensitive and collaborative discussions, robust authentication mechanisms have become necessary to safeguard group integrity. The reviewed literature outlines various approaches to group authentication, including custom verification questions, database-linked access control, and one-time-use credentials. Each of these approaches plays a role in the multi-layered strategy that SecureJoin adopts. In this section, we critically analyze the strengths and limitations of these approaches, providing insights into how SecureJoin can leverage and enhance existing methods to create a more secure and user-friendly group authentication system.

The first key point is **Trust and User Perception**. Research highlights that user trust in group chat environments is heavily influenced by visible security measures, with users often relying on perceived security rather than technical knowledge Oesch et al. [6]. Multi-step verification and clear, user-centered authentication steps have been shown to enhance trust, as users feel more secure when they see authentication protocols in place. SecureJoin's use of customized verification questions and visible database-linked checks strengthens this sense of security, making it transparent that only verified users can join the group.

**- Strength:** By making the authentication process visible and understandable, SecureJoin aligns with user expectations and reinforces trust.

**- Limitation:** However, balancing visibility with simplicity can be challenging; too many steps may deter users, while too few could compromise security. SecureJoin must find an effective balance between ensuring transparency and maintaining ease of use to avoid user fatigue or confusion.

Another critical aspect is **Membership Verification and Access Control**. Managing membership in group chats remains a significant challenge, especially when group links can be easily shared, leading to unauthorized access. Studies, such as those by Chen et al. [7], emphasize the need for multi-layered verification systems that incorporate tools like database-linked user lists. SecureJoin's approach aligns well with these findings, as it includes multiple verification points that collectively reduce unauthorized access. By restricting access to only verified or pre-approved members, SecureJoin mitigates risks associated with link sharing and protects group exclusivity.

**- Strength:** This multi-layered approach effectively limits unauthorized access, preserving group integrity by ensuring that only trusted individuals gain entry.

**- Limitation:** The administrative overhead for maintaining database-linked verification lists can be a challenge, particularly in large, dynamic groups where membership changes frequently. To address this, SecureJoin could consider automating updates or providing batch-upload functionalities to reduce the manual workload for administrators.

In terms of **Managing Dynamic Group Membership**, The fluid nature of group memberships—where members frequently join and leave—complicates the task of maintaining group security. This issue is particularly pronounced in open groups with no predefined member list, where the risk of unauthorized access is higher. Research by Diallo et al. [8] highlights the need for adaptive authentication mechanisms that can dynamically adjust to group changes. SecureJoin addresses this by enabling group administrators to create verification questions tailored to new members, effectively filtering out unauthorized users based on knowledge specific to the group.

**- Strength:** This flexibility is especially valuable in dynamic settings, as SecureJoin's adaptive questions allow administrators to screen users based on relevant knowledge or criteria, reducing the risk of unauthorized users entering sensitive discussions.
**- Limitation:** However, in highly dynamic environments, manual customization of questions may become cumbersome for administrators. Automating the generation of relevant verification questions based on group data could be a future enhancement for SecureJoin, reducing administrative workload while maintaining security.

Lastly, the challenge of **Preventing Unauthorized Sharing of Access Credentials** is crucial. Credential reuse and sharing of group links are recurring security risks in group chats, as noted by Chen et al. [7]. Many platforms fail to prevent users from sharing their access credentials with others, compromising group security. SecureJoin's implementation of one-time-use credentials directly addresses this vulnerability by ensuring that once a user is granted access, their information cannot be shared or reused.
**- Strength:** One-time-use credentials effectively prevent unauthorized access through shared links, providing an additional security layer that maintains group exclusivity.
**- Limitation:** A potential downside is that one-time-use credentials may create inconvenience for users if they need to re-enter the group repeatedly, such as in the case of multi-device usage. To address this, SecureJoin could consider implementing a temporary session persistence feature, allowing users to maintain access across devices within a defined timeframe before requiring re-authentication.

In conclusion, the literature on Authentication in Group Chats offers a strong foundation for SecureJoin's authentication mechanisms by emphasizing multi-layered verification, dynamic member management, and one-time-use credentials. However, there remains room for innovation to overcome existing limitations. SecureJoin's development strategy can leverage these insights by prioritizing usability alongside security, ensuring user-friendly authentication steps that do not compromise group integrity. Automating administrative tasks, incorporating user feedback, and adapting features based on group-specific needs can further enhance SecureJoin's usability and security. By addressing both the strengths and limitations of current authentication approaches, SecureJoin has the potential to set a new standard in secure group access, promoting a trust-centered, user-friendly experience that stands out in the realm of digital communication platforms.

### 2.3.3 Rule-Based Spam Detection

The **Rule-Based Spam Detection** theme aaddresses critical security challenges in social media and group chat platforms, where unauthorized users often gain access through shared links, compromising group integrity. Rule-based systems, operating with predefined criteria, provide an efficient foundation for spam detection within SecureJoin by filtering out unwanted users at entry. This approach aligns with SecureJoin's goal of restricting access to verified users and enhancing security for groups that rely on open links.

**Adaptability to Evolving Spam Patterns**
Spam detection systems must remain adaptable, as spammers frequently modify their tactics to bypass existing filters. Research by Kaddoura et al. [9] highlights the necessity of maintaining dynamic rule sets through techniques such as keyword updates and evolving detection criteria.
**- Strength:** Adaptive rule-based systems allow SecureJoin to respond swiftly to emerging spam patterns without constant manual reprogramming, maintaining a high level of security.
**- Limitation:** Frequent updates to detection rules may introduce maintenance complexity, requiring careful oversight to prevent gaps in protection or excessive false positives.

**Rule-based content filtering** provides a lightweight, efficient method for preliminary spam detection, targeting specific keywords or message structures that indicate spam activity Sharma et al [10].
**- Strength:** Rule-based filters offer a simple and resource-efficient approach for early spam screening, allowing SecureJoin to block potential threats quickly at the entry point.
**- Limitation:** Static rule-based systems may struggle to detect sophisticated spam tactics that deviate from known patterns, potentially requiring supplementary detection layers.

**Behavior Analysis for Spam Detection** Monitoring user behaviors, such as repeated login attempts or abnormal link-sharing patterns, adds a dynamic layer of spam detection. Abdo et al [16] emphasize the importance of behavior-based detection methods for enhancing platform security.
**- Strength:** Behavior analysis enables SecureJoin to detect and block suspicious users proactively, even before explicit spam content is posted.
**- Limitation:** Reliance on behavior-based scoring may lead to false positives, incorrectly flagging legitimate users whose activities resemble spam patterns under certain conditions.

**Automation for Scalability** Automating verification processes is essential to managing large user bases efficiently. Sharma et al. [10] describe how automated spam detection systems, based on IP addresses and domain patterns, minimize administrative burden.

**- Strength:** Automation allows SecureJoin to efficiently scale its verification processes, reducing the need for continuous manual oversight as user volumes grow.

**- Limitation:** Over-automation without careful monitoring can result in vulnerabilities if attackers find patterns that evade automated checks.

**Real-Time Detection and Prevention** Real-time spam detection enables immediate response to threats, preventing unauthorized users from disrupting group communications. Abdo et al.. [16] advocate for integrating real-time monitoring in dynamic digital platforms.

**- Strength:** Real-time detection allows SecureJoin to block spam activity instantly, minimizing potential disruption to group integrity.

**- Limitation:** Implementing real-time systems requires significant computational resources, and delays or misclassifications could affect user experience.

Finally, **Distributed Detection for Enhanced Scalability and Reliability** such as the Distributed Large-Scale Anti-Spam System (DLSAS) proposed by Soliman and Girdzijauskas [17] spread detection tasks across multiple nodes to enhance performance and resilience.

**- Strength:** Distributed detection improves system scalability and stability, allowing SecureJoin to handle high-volume spam filtering efficiently across diverse group environments.

**- Limitation:** Managing distributed systems adds architectural complexity, requiring robust coordination mechanisms to avoid inconsistencies between detection nodes.

In Conclusion, The thematic analysis of rule-based spam detection highlights the critical need for adaptable, real-time, and distributed security measures in digital communication platforms. By integrating these insights, SecureJoin can offer a dynamic, multi-layered spam detection solution that effectively balances automation with adaptability. Prioritizing a combination of rule-based filtering, behavioral analysis, real-time monitoring, and distributed architecture will enable SecureJoin to maintain robust group security while ensuring a seamless and scalable user experience.

### 2.3.4 Usability

The Usability theme addresses the critical relationship between system design simplicity and security effectiveness. In the context of SecureJoin, usability plays a pivotal role in ensuring that users can smoothly complete authentication processes without encountering unnecessary complexity or making security-compromising errors. Research indicates that systems with high usability not only foster better adoption but also enhance security outcomes by reducing the frequency of user mistakes.

**Relationship of Usability to the SecureJoin Project** Research consistently highlights the importance of usability in the success of secure system designs. Saltzer and Schroeder [11] demonstrate that poor usability often leads to user errors that can undermine even the strongest security protocols. In SecureJoin, a core design objective is to create a streamlined, user-friendly verification system that minimizes confusion without sacrificing security strength. Similarly, studies on two-factor and multi-factor authentication usability reveal that users frequently reject overly complex security setups, preferring straightforward verification methods instead Juels and Wattenberg [12, 14] Based on these insights, SecureJoin adopts simple yet secure verification techniques, such as SMS and email codes, to enhance user experience and foster higher adoption rates.

- **Strength:** Emphasizing usability enables SecureJoin to significantly reduce user errors and increase user engagement, promoting both security and accessibility.
- **Limitation:** Prioritizing simplicity could unintentionally weaken security if critical authentication layers are oversimplified; SecureJoin must therefore carefully balance simplicity with maintaining robust multi-layered protection.

**Gaps in Existing Research** While prior studies address usability challenges in general security mechanisms, they largely overlook context-specific security needs such as verifying users in group chat environments, where unauthorized access and spam are particularly prevalent. Research on two-factor and multi-factor authentication methods primarily focuses on banking or personal account security, rather than on dynamic group settings where link sharing and fluctuating membership introduce unique vulnerabilities Hong et al [13, 15]. The SecureJoin project addresses this context-specific gap by implementing group membership validation through custom verification questions and database-linked user lists—techniques not typically covered in existing usability research.

Additionally, although Schneier et al. [14] emphasize the value of user feedback in the usability of multi-factor authentication systems, their study does not explore how continuous feedback can be leveraged to iteratively refine security protocols specifically for group access. SecureJoin will integrate iterative feedback loops into its development process, allowing for dynamic adaptation of verification features to better align with real-world security needs and user experiences.

**- Strength:** SecureJoin directly addresses the overlooked need for context-specific usability in group communication settings, offering innovative solutions that adapt standard authentication methods to new environments.

**- Limitation:** Designing verification processes specifically for dynamic group environments introduces complexity that may not be fully addressed by existing usability frameworks; thus, SecureJoin must develop new best practices through ongoing user research and testing.

**Agreement with Existing Findings** The emphasis on balancing usability with security presented in prior studies aligns closely with SecureJoin's design philosophy. Hong et al [13] conclude that overly complex security mechanisms often lead users to bypass protective measures, ultimately reducing overall system security. Reflecting this insight, SecureJoin adopts a strategy of implementing multi-layered but straightforward verification methods that maintain robust authentication without overwhelming users. Similarly, Clarke et al. [15] find that users are more likely to adopt authentication methods that they are already familiar with, such as SMS and email-based verification. This understanding reinforces SecureJoin's choice to prioritize commonly used and widely recognized verification techniques to enhance user engagement and system adoption.

**- Strength:** SecureJoin's adherence to established usability principles supports high user adoption rates while maintaining strong security, addressing a critical challenge identified in prior research.

**- Limitation:** While relying on familiar verification methods promotes usability, it may also expose the system to common attack vectors targeting SMS and email authentication; thus, SecureJoin must supplement ease-of-use strategies with strong backend security measures.

**Areas of Improvement and Differentiation for SecureJoin** While SecureJoin builds upon established usability principles, it differentiates itself by focusing on adaptable, context-specific verification methods for group chat access. Unlike traditional two-factor authentication systems that often require repetitive verification steps, SecureJoin streamlines the onboarding process by using database-linked verification. This allows administrators to upload pre-verified user lists, automatically validating new members without requiring repeated manual checks. By minimizing redundant authentication steps while maintaining strong access control, SecureJoin addresses usability and security challenges that standard two-factor methods typically overlook.

Moreover, SecureJoin adopts an iterative design model that incorporates continuous user feedback, moving beyond the one-time usability assessments seen in existing studies. This dynamic approach allows SecureJoin to flexibly adapt its features to evolving user needs and security requirements over time.

**- Strength:** SecureJoin's streamlined onboarding and continuous refinement based on user feedback enhance both usability and security, offering a flexible system that evolves alongside user expectations.

**- Limitation:** Managing dynamic, pre-verified user lists introduces administrative complexities, and maintaining the integrity of database-linked verification requires robust update and error-handling processes to prevent unauthorized access.

In Conclusion, The SecureJoin project applies the usability insights presented in the reviewed studies to the specific context of group chat security, addressing access control needs that have been largely overlooked in existing research. By incorporating adaptable verification methods and establishing continuous feedback loops for iterative improvement, SecureJoin seeks to bridge the gaps left by traditional two-factor and multi-factor authentication systems. Its emphasis on balancing strong security with user-friendly design distinguishes SecureJoin as a unique contribution to both the usability and security fields. In particular, SecureJoin advances group communication security by preventing unauthorized access while maintaining a seamless and accessible user experience.

## 2.4 Conclusion

This chapter presented a comprehensive review of the existing literature on security and usability in digital communication platforms, with a specific focus on challenges relevant to group chat environments. Through a thematic analysis, four major areas were explored: security in social media, authentication in group chats, rule-based spam detection, and usability in security systems.

The review revealed that while significant progress has been made in enhancing individual account security and general usability principles, notable gaps remain in addressing the specific needs of group chat settings—particularly regarding dynamic membership verification, spam prevention, and user-centered authentication strategies. Studies consistently emphasized the importance of balancing robust security mechanisms with ease of use, noting that overly complex systems often lead to user errors and reduced security effectiveness.

SecureJoin addresses these identified gaps by developing an adaptable, multi-layered verification system tailored to group communication contexts. It builds upon the strengths highlighted in existing research, such as user familiarity with authentication methods and the value of continuous usability improvements, while introducing new solutions like database-linked user validation and dynamic spam filtering mechanisms.

By synthesizing these insights and applying them to a specialized context, SecureJoin contributes uniquely to both the usability and security fields, offering an innovative platform designed to enhance the safety, trustworthiness, and user experience of group chat communications.

# Chapter 3

# METHODOLOGY

# CHAPTER THREE METHODOLOGY

## 3.1 Introduction

This chapter presents the detailed methodology adopted for the development of the SecureJoin platform, a web-based solution designed to enhance the security of group access on popular messaging platforms such as WhatsApp and Telegram. The methodology outlines the systematic approach taken to address the project's objectives, ensuring the platform is both secure and well designed. A structured, iterative, prototype-based methodology was selected to guide the development process. This approach emphasizes flexibility, continuous refinement, and early validation of design decisions. The focus of this chapter is on the initial phases of the development lifecycle—specifically, requirements gathering and system design—which form the foundation for addressing the critical security challenges identified in public chat groups.

## 3.2 Type of Study

The SecureJoin project adopts a prototype-based programming approach, which emphasizes iterative development and testing. This methodology is particularly suitable for projects where continuous user feedback is essential to refine features and enhance security measures. By focusing on building and testing functional prototypes, the project team aims to rapidly iterate on the system, making adjustments based on testing results and user feedback.

This study is not purely theoretical; instead, it proposes a focus on the practical development of a secure group access system. By planning the creation of working prototypes and rigorous testing, the project aims to validate the efficacy of the proposed security measures in real-world scenarios. Additionally, the study incorporates elements of simulation-based testing to analyze how the system is expected to perform under varying conditions, such as handling high volumes of user verification requests.

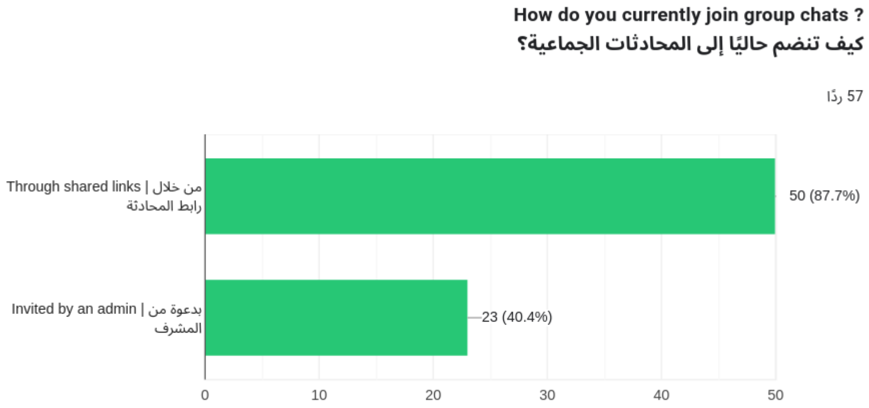
## 3.3 Survey Overview

To better understand user experiences and security challenges in group chat environments, a survey was conducted with 57 participants. The survey captured perspectives on group chat challenges, spam prevalence, security concerns, and preferences for verification methods. The data reflects a diverse range of user experiences and emphasizes the importance of implementing improved security measures in messaging platforms.

### 3.3.1 Key Finding

1. **Methods of Joining Groups** Respondents primarily joined groups through shared links (87.7%) and admin invitations (40.4%). This highlights the convenience but also the vulnerabilities of these common methods. (see Figure 3.1)

Figure 3.1: Methods of Joining Groups.



2. **Spam and Security Concerns**

   a. Spam Frequency: 54.4% of respondents encounter spam occasionally, while 31.6% experience it frequently. (see Figure 3.2)

   b. Security Perception: A striking 45.6% of participants believe that current security methods are insufficient, indicating a strong demand for enhanced measures. (see Figure 3.3)

Figure 3.2: Spam Frequency.

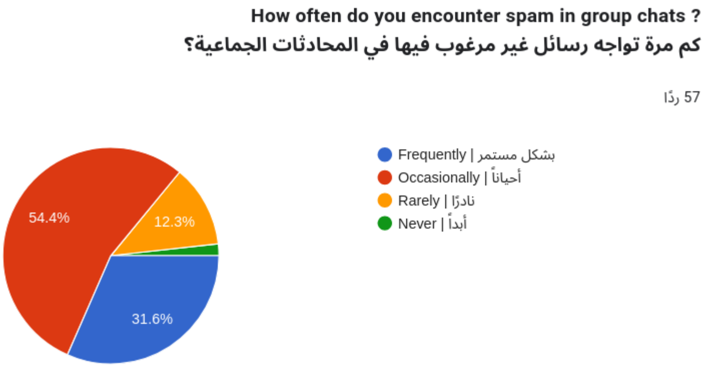
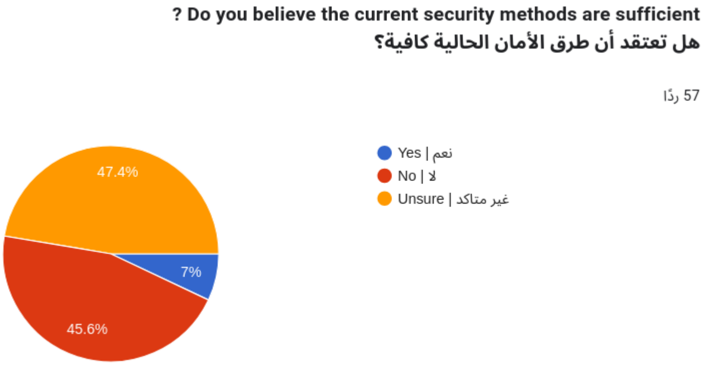


Figure 3.3: Security Perception.



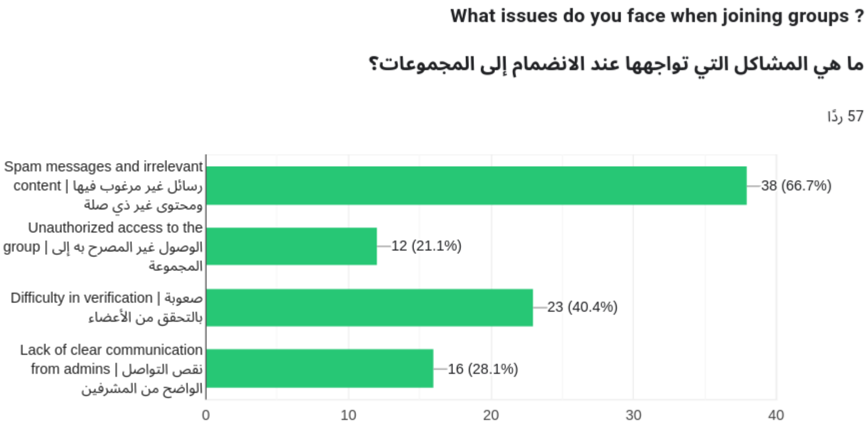
3. Challenges in Joining Groups

The most commonly reported issues include:

a. Spam messages and irrelevant content (66.7%).

b. Difficulty in verification (40.4%). (see Figure 3.4)

Figure 3.4: Spam Frequency.



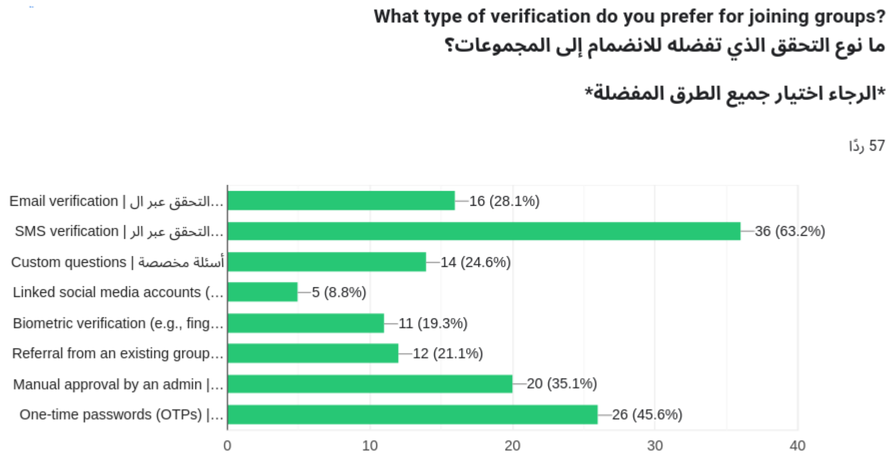
4. **Preferred Verification Methods**

   Respondents identified multiple methods for group verification, including:

   a. One-Time Passwords (OTPs): Preferred by 45.6% for their simplicity and security.

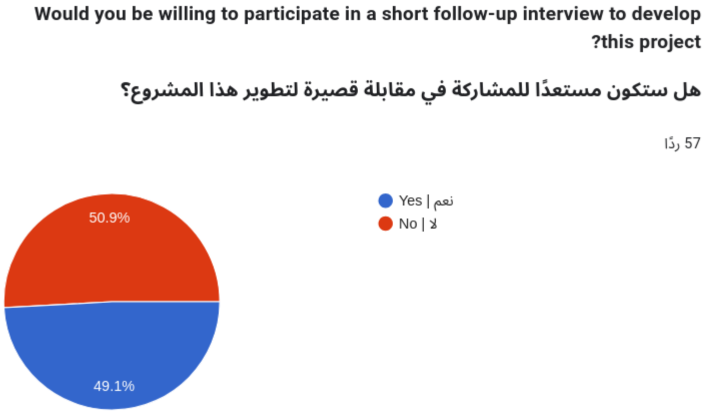
   b. Manual Admin Approval: Chosen by 35.1% for its control over group membership. (see Figure 3.5)

Figure 3.5: Preferred Verification Methods.



5. **Willingness to Engage** Approximately 49.1% of participants expressed willingness to participate in follow-up interviews, demonstrating strong interest in contributing to the development of SecureJoin (see Figure 3.6)

Figure 3.6: Willingness to Engage.



### 3.3.2 Implications for SecureJoin

The data underscores critical opportunities for SecureJoin to differentiate itself:

**Spam Mitigation**: Address spam issues by integrating robust verification mechanisms, such as combining OTP-based authentication with database-linked verification.

**User-Centric Design:** Offer multiple verification methods to accommodate varying user preferences and enhance accessibility.

**Improved Security:** Strengthen control over group membership to prevent unauthorized access and mitigate risks associated with the open sharing of group links.

### 3.3.3 Next Steps

The survey results will guide the refinement of SecureJoin's verification features. Future steps include:

- **Prototype Testing:** Implement and test OTP and manual admin approval systems based on user preferences.
- **User Feedback:** Conduct follow-up interviews to gather deeper insights into user expectations and pain points.
- **Scalability Planning:** Develop strategies to manage diverse user scenarios and support large group dynamics effectively.

By addressing these user-identified concerns, SecureJoin aims to redefine the standards of group chat security while maintaining a high level of user convenience.

## 3.4 Methodology Approach

The methodology approach for developing SecureJoin revolves around a structured software development process. This process is underpinned by the Agile methodology, which allows for flexibility and adaptability throughout the project lifecycle. Agile principles were employed to ensure that the project could quickly adapt to changes, incorporate user feedback, and improve security features in response to testing results.

### 3.4.1 Type of Selected Method

The selected method for this project combines **prototype-based software development** software development with **iterative design cycles.** This approach was chosen for several reasons:

1. **Rapid prototyping and testing:** The ability to quickly develop prototypes, test them, and make improvements based on user feedback was essential for refining security features.
2. **User-centered design:** The methodology emphasizes incorporating user feedback at each stage to ensure that the platform is intuitive and meets the needs of both group administrators and users.
3. **Focus on security and usability:** By iteratively developing the platform, the project team ensured that security features were robust without compromising user experience.

**Agile principles** also enabled the team to prioritize critical tasks—such as implementing verification systems, database integration, and frontend design—into focused sprints. This ensured that essential security features were delivered on time while allowing for continuous refinements based on testing and evaluation.

### 3.4.2 Study Procedure

The study procedure is broken down into several phases, each critical to the successful implementation of SecureJoin. These phases include requirements gathering, data collection, analysis, system design, and implementation.

#### 3.4.2.1 Requirements

To develop a robust and efficient platform, a thorough requirements analysis was conducted. This involved gathering both functional and non-functional requirements to define the project's scope and objectives clearly:

–**Functional Requirements**

| **Requirement Name** | **Requirement Description** | **Why Needed** |
|---|---|---|
| User Registration | Users must be able to register on the platform, providing essential information such as name, email, phone number, etc. | Registration is required to uniquely identify users and enable verification for secure group access. |
| Custom Verification Questions | Group administrators can create tailored verification questions that users must answer correctly to join the group. | Custom questions enhance security by ensuring that only users familiar with the group's context can join. |
| SMS/Email Verification | Users will receive verification codes via SMS or email, which they must enter to confirm their identity. | Adds an additional layer of security to confirm the identity of users and ensure legitimacy. |
| Database-Linked User Verification | Admins can upload a list of preapproved users (e.g., university students) and the system cross-checks this list. | Ensures that only authorized users can join specific groups, preventing unauthorized access. |
| One-Time Use of Access Credentials | Once a user is verified and added to a group, their credentials cannot be reused for access by another user. | Prevents credential sharing, ensuring that only legitimate users gain access to the group. |
| Group Access Management Integration | Integrates with messaging platforms like WhatsApp and Telegram to manage group membership based on verification. | Ensures automated group access management, reducing the risk of unauthorized members joining. |
| Customizable Link Expiration | Admins can set expiration times for group join links, after which the link will no longer be valid. | Limits the risk of shared links being used after the intended group access period, enhancing security. |
| Multi-Language Support | The platform supports multiple languages, allowing users to interact in their preferred language. | Increases accessibility and usability for a global user base. |

Table 3.1: Functional Requirements of SecureJoin

–**Non-Functional Requirements**

| **Requirement Name** | **Requirement Description** | **Why Needed** |
|---|---|---|
| Scalability | The platform must be able to handle a growing number of users and verification requests without performance degradation. | Ensures that the system remains efficient and usable even as user demand increases. |
| Reliability | The platform must consistently deliver verification codes and process verification requests without failure. | Builds trust among users by providing consistent and dependable service. |
| Security | The system must adhere to the latest security standards to protect user data and prevent unauthorized access. | Safeguards user information and group integrity against breaches and vulnerabilities. |
| Cross-Platform Compatibility | The platform should function seamlessly across various devices (e.g., desktops, tablets, smartphones). | Ensures users can access the platform from their preferred device, improving usability. |
| Localization | Support for multiple languages and cultural contexts to cater to a global audience. | Makes the platform more inclusive and accessible to non-English speakers. |
| Performance Optimization | The platform should provide quick response times, even during peak usage. | Improves user satisfaction by reducing delays and providing a smooth experience. |
| Compliance | Adherence to relevant legal and regulatory standards, such as GDPR for data privacy. | Ensures the platform operates within legal boundaries and protects user rights. |
| Maintainability | The system should be designed to allow easy updates and integration of new features. | Reduces long-term maintenance costs and ensures the platform remains up-to-date with evolving needs. |

Table 3.2: Non-Functional Requirements of SecureJoin

This list of functional and non-functional requirements covers the essential aspects of SecureJoin, from ensuring that only authorized users can join groups to guaranteeing the system's performance, security, and usability. By addressing both the core features and operational qualities of the platform, these requirements form the foundation for a robust, secure, and scalable solution for group access management.

#### 3.4.2.2 Data Collection

Data collection was a crucial step in the methodology to ensure that the SecureJoin platform addresses real-world challenges faced by chat group administrators. The data collection process included:

- **User Surveys and Interviews:** Conducted with potential users (group admins and members) to understand their pain points related to group management, spam prevention, and user authentication.
- **Secondary Data Analysis:** Reviewing API documentation from WhatsApp and Telegram to understand their limitations and capabilities for secure integration.
- **Competitor Analysis:** Examining existing solutions for group management to identify gaps that SecureJoin could address, especially in terms of security and usability.

#### 3.4.2.3 Data Analysis

Data analysis focused on interpreting the collected information to refine the system's design and functionalities:

- **Quantitative Analysis:** Survey data was quantitatively analyzed to identify common issues faced by group admins, such as spam, unauthorized access, and difficulty in managing large groups.
- **Qualitative Analysis:** Insights from interviews were used to prioritize features like custom verification questions and database-linked user lists.
- **Spam Prevention Techniques:** Data was analyzed to understand patterns of spam and unauthorized access attempts, which informed the rule-based filters implemented in the system.

#### 3.4.2.4 System Design Procedure

The system design phase was comprehensive, involving multiple stages to ensure that the platform was both secure and user-friendly:

- **System Architecture:**

  The platform was developed using a Model-View-Controller (MVC) architecture, which separated data management, user interface, and control logic.

  This architecture enhances modularity and scalability.

- **User Interface (UI) Design:**

  The admin dashboard was designed to be intuitive, allowing group administrators to set up custom verification questions, manage user lists, and monitor group access.

  User verification screens were optimized for mobile devices, ensuring that the process of entering verification codes via SMS or email was seamless.

- **Backend Development:**

  Implemented using Flask, the backend was designed to handle user authentication, group management, and secure communication with the database.

  The integration with Twilio API enabled automated sending of verification codes via SMS and email.

- **Database Design:**

  MySQL was used to store user credentials, verification codes, and group membership information securely.

  Tables were designed to prevent duplication of credentials and to lock user access once verified, thus preventing credential sharing.

#### 3.4.2.5 Implementation and Testing

The implementation involved developing, testing, and refining various components of the system:

- **Unit Testing:** Each module, such as user authentication, verification code generation, and database queries, was tested independently to ensure functionality.

- **Integration Testing:** Focused on ensuring that the system components (frontend, backend, and database) interacted seamlessly.

- **Usability Testing:** Conducted with a sample group of users to evaluate the ease of using the admin dashboard and verification processes. Feedback from these sessions was used to enhance the user experience.

- **Security Testing:** Rigorous testing to identify potential vulnerabilities, including attempts to bypass verification, reuse credentials, or access unauthorized data.

Continuing our exploration of the SecureJoin platform, the survey responses provided invaluable insights into user experiences and expectations surrounding group chat security. The findings from this dataset shape the foundation for refining SecureJoin's features and addressing key concerns.

## 3.5 Summary

This chapter provided a comprehensive overview of the methodology adopted for the development of SecureJoin. By employing a prototype-based, iterative approach grounded in Agile principles, the project prioritizes both security and usability throughout its lifecycle. The structured methodology ensures that each phase—from requirements analysis to system implementation and testing—aligns closely with the project's core objectives: preventing unauthorized access, mitigating spam, and enhancing user trust in group communications. Through this approach, SecureJoin is positioned to deliver a robust, user-centered solution tailored to the evolving security challenges of digital group platforms.

# Chapter 4

# Implementation

# CHAPTER FOUR
# IMPLEMENTATION

## 4.1 Introduction

This chapter documents the comprehensive process of implementing and testing the SecureJoin platform—a security-focused web application designed to control access to group chats on popular messaging platforms such as WhatsApp and Telegram. Building on the design and planning stages outlined in earlier chapters, this phase transitions the project from conceptual architecture to an operational system. The chapter details the technologies used, architectural decisions made, algorithms implemented, and strategies followed to ensure the development of a robust and user-friendly final product.

The implementation phase centered on creating a responsive and interactive user interface, a scalable backend service, and secure integrations with third-party tools, including Clerk (for authentication), Supabase (for database management), and Waha (for OTP delivery). Each component of the system was carefully selected to align with the platform's core objectives: verifying users before granting access to private groups, minimizing spam, preventing unauthorized sharing of invitation links, and maintaining a high-quality user experience.

SecureJoin was developed using modern web technologies, including React, Vite, Tailwind CSS, and TypeScript for the frontend, while Node.js, Prisma ORM, and Supabase supported the backend. The system supports multiple verification workflows, including text-based questions, multiple-choice quizzes, and OTP verification via email or phone. These workflows are configurable by group administrators to meet the specific privacy needs of their groups.

This chapter is organized into several key sections. It begins by introducing the tools, libraries, and programming languages used during development, explaining their purposes and suitability. Next, the software design is discussed in detail, including architecture diagrams, user flows, and descriptions of the core modules and components.

The source code and project repository can be accessed via: `https://github.com/SenQii/securejoin` or visit the project website at: `http://securejoin.vercel.app`.

## 4.2 Programming Languages and Tools

The development of SecureJoin utilized a modern technology stack, integrating powerful programming languages, frameworks, and external services to ensure a responsive, secure, and scalable platform. The selected tools were carefully chosen to align with the platform's requirements for security, usability, and real-time performance.

**Frontend Development**

- **React 18 (with Vite)** – Enables the creation of a responsive, component-based interface with rapid development support provided by Vite's fast build system.
- **TypeScript** – Adds static type safety to JavaScript, helping to catch potential bugs early in the development process and improving code maintainability.
- **Tailwind CSS** – A utility-first CSS framework used to design responsive, mobile-friendly, and RTL-supportive (Right-to-Left language) user interfaces efficiently.
- **shadcn/ui** – Provides A pre-styled UI component library that accelerates development and ensures a consistent visual style across the platform.
- **Clerk** – Provides authentication and session management capabilities, supporting features like JWT-based authentication and OAuth integration.

**Backend Development**

- **Node.js** – A JavaScript runtime environment used for building server-side logic and handling API routes.
- **Prisma ORM** – Facilitates type-safe database queries, schema management, and seamless interaction with the database layer.
- **Supabase (PostgreSQL)** – Acts as the main database solution, offering secure, real-time data access and management.

**External Integrations**

- **Waha API** – Used to Integrates OTP delivery services, enabling real-world validation by sending one-time passwords (OTPs) to users' mobile numbers or email addresses for verification purposes.

## 4.3 Software Design

### 4.3.1 System Architecture Overview

As illustrated in Figure 4.1, SecureJoin follows a layered, modular system architecture composed of four primary layers:

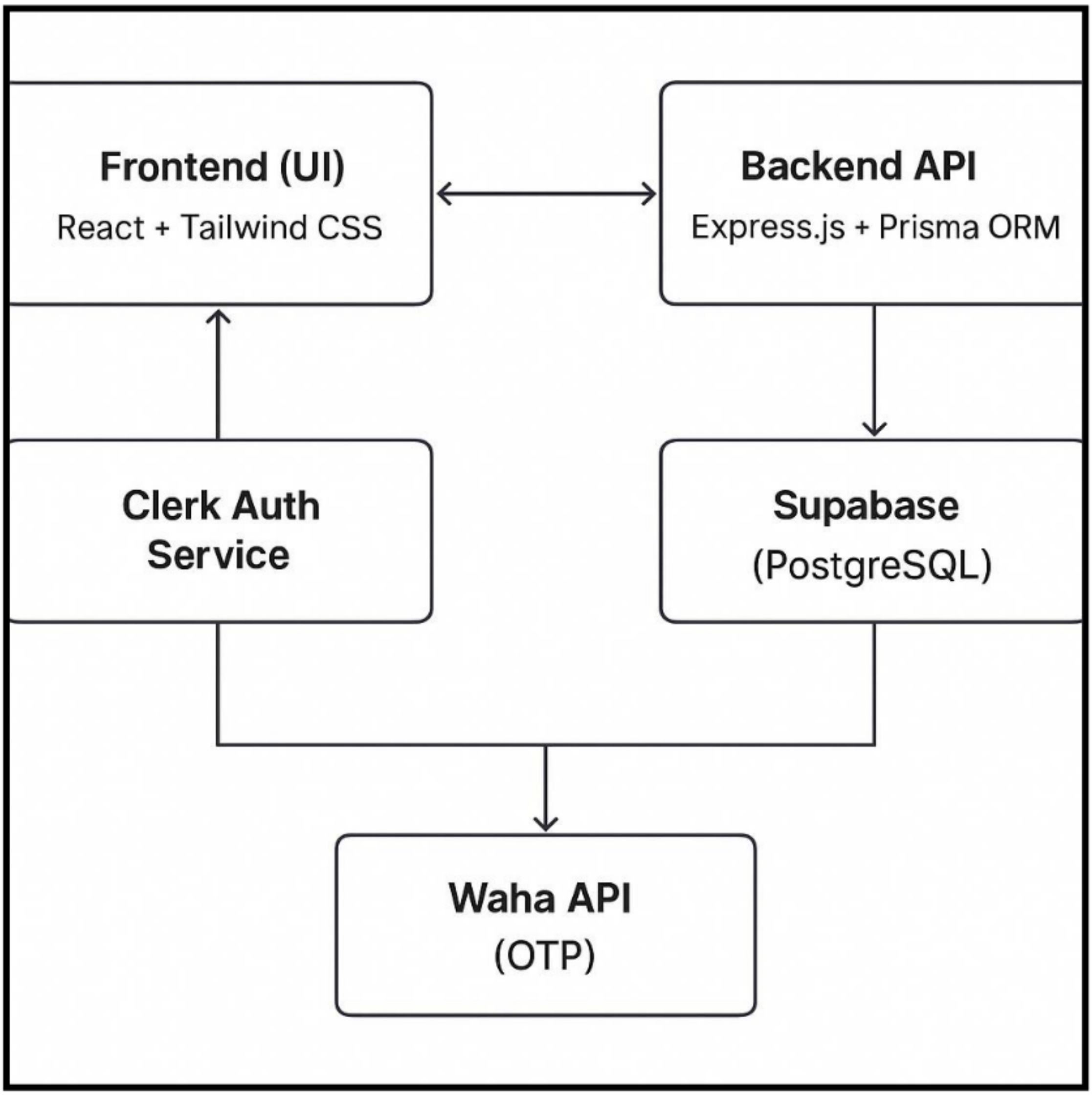


Figure 4.1: SecureJoin System Architecture Overview.

- **Frontend (UI)**: Enables administrators to create secure links and users to authenticate before joining groups.
- **Backend (API)**: Manages data storage, processes verification logic, and handles integration with third-party services.
- **External Services**: Includes Clerk for authentication, Waha for OTP delivery, and Supabase for secure real-time database management.
- **Actors**:

  **-Admins:** Create verification quizzes and secure invitation links.

  **-Guests:** Authenticate and verify identity before joining a group.

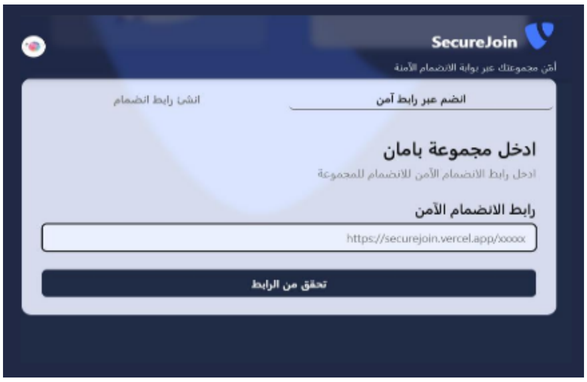
  **- Server:** Validates verification inputs and responds with access authorization.

### 4.3.2 Core Components and Interfaces

SecureJoin's software is organized around several key user-facing and system-facing components:

- **Admin Interface**: Allows signed-in administrators to choose verification methods, create quizzes, and generate secure invitation links.
- **User Interface**: Guides guests (unauthenticated users) through the verification process, controlling access to group links based on successful verification.
- **JoinForm / CreateForm**: Dynamic frontend components rendered based on authentication status to either allow users to join existing groups or enable administrators to create new verification setups.
- **Dashboard**: An administrative panel providing analytics, quiz management tools, and success/failure tracking for user verifications.

In the following are three figures that show the key components of the platform. First, a figure of the Join Form interface, which guides guests through the verification process [Figure 4.2]. Next, a figure of the admin interface after logging in, where the admin can create quizzes and manage secure links [Figure 4.3]. Finally, the Admin Dashboard Figure displays detailed analytics and data about the groups created by the admin, including success and failure metrics, [Figure 4.4].



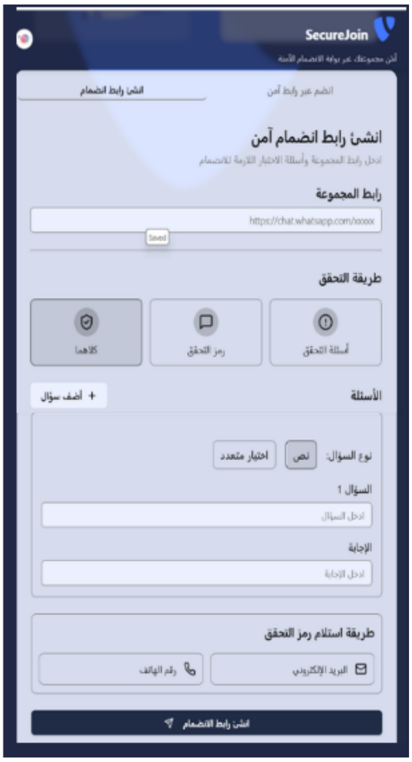
أمّن مجموعتك عبر بوابة الانضمام الآمنة

ادخل مجموعة بامان

ادخل رابط الانضمام الآمن للانضمام للمجموعة

https://securejoin.vercel.app/xxxxx

Figure 4.2: Join Form Interface.



أمّن مجموعتك عبر بوابة الانضمام الآمنة

انشئ رابط انضمام آمن

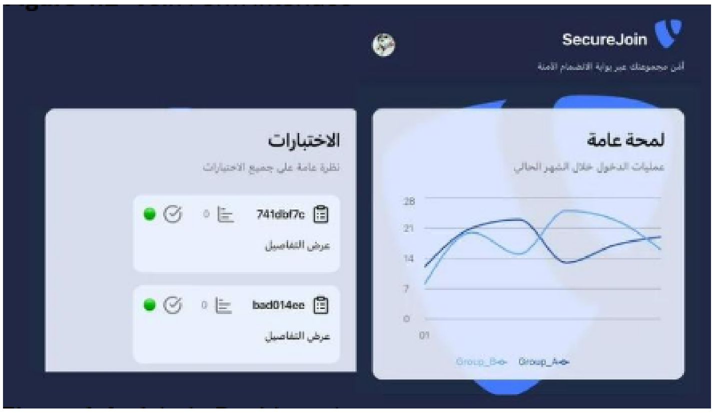
ادخل رابط المجموعة وأسئلة الاختبار اللازمة للانضمام

https://chat.whatsapp.com/xxxxx

ادخل السؤال

ادخل الإجابة

Figure 4.3: Admin Interface.



أمّن مجموعتك عبر بوابة الانضمام الآمنة

نظرة عامة على جميع الاختبارات

عمليات الدخول خلال الشهر الحالي

Figure 4.4: Admin Dashboard.

### 4.3.3 Sequence Diagram

SecureJoin's flow involves three primary actors:

- **Admin** – Creates Secure-Links and configures authentication settings.
- **Server (API)** – Handles authentication logic, security enforcement, and group access validation.
- **Member (Guest)** – Attempts to join a group via a Secure-Link by completing the authentication process.

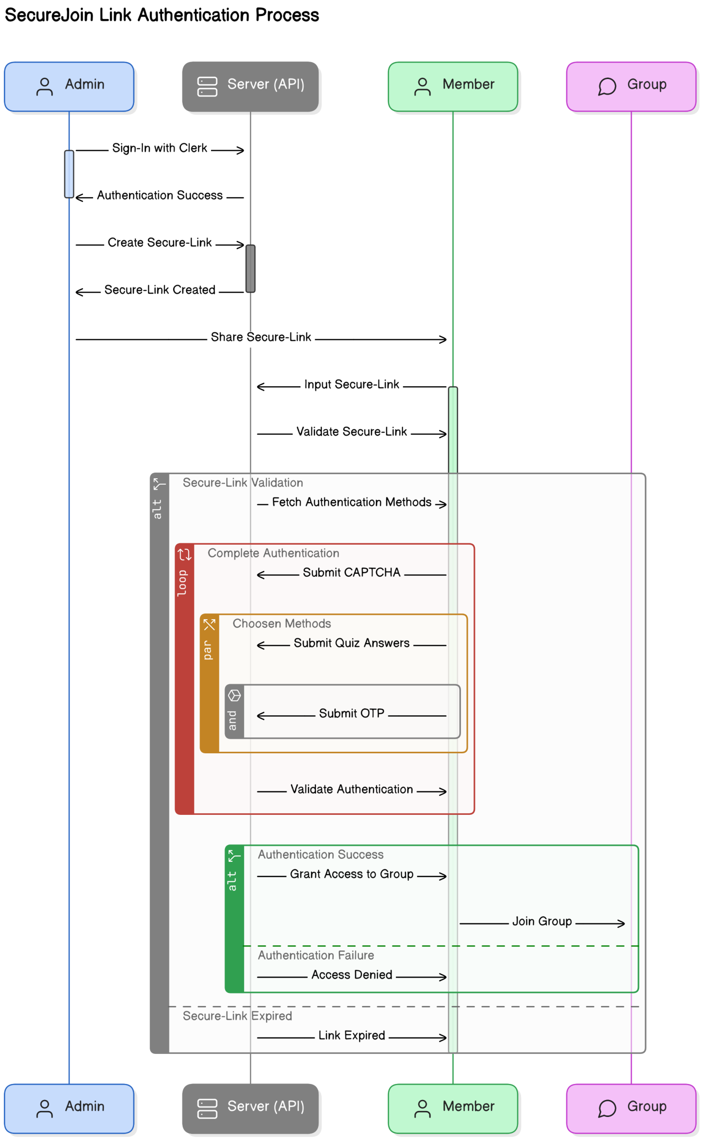


Figure 4.5: SecureJoin Sequence Diagram.

### 4.3.4 UI Design Considerations

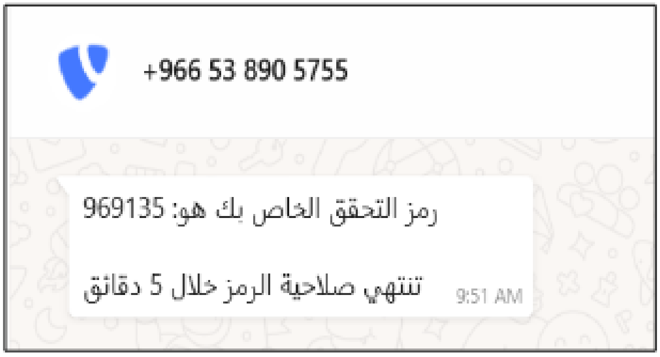
The design of SecureJoin's user interface emphasizes accessibility, ease of use, and responsiveness:

- **Responsive Layout:** The platform is designed to function seamlessly across desktop, tablet, and mobile browsers, providing a consistent experience across devices.
- **Step-by-Step Forms:** The user flows are broken into guided steps to improve learnability, reduce user errors, and make the verification process intuitive.

### 4.3.5 Security Measures

To protect the platform from unauthorized access and malicious activities, several key security measures were implemented:

- **One-time code usage**: We implemented a system where each verification code can only be used once. This prevents users from sharing access codes with others, which is crucial for maintaining group integrity and ensuring that only authorized individuals can join (Figure 4.6).



+966 53 890 5755

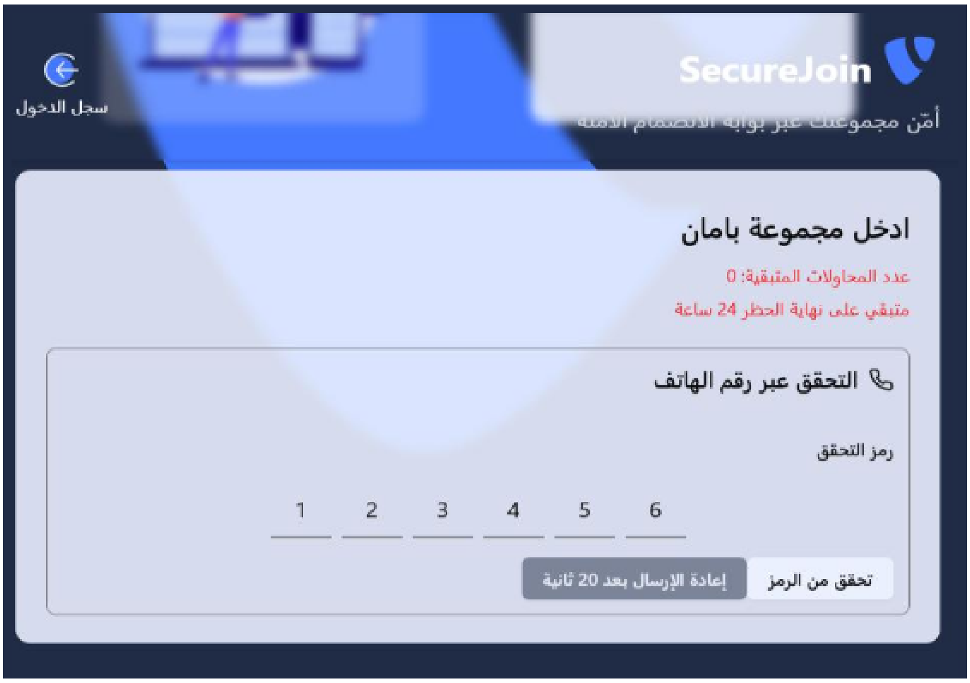
رمز التحقق الخاص بك هو: 969135

تنتهي صلاحية الرمز خلال 5 دقائق

9:51 AM

Figure 4.6: One-Time Code Enforcement.

- **Rate limiting and IP bans**: To guard against brute-force attacks where malicious users might try multiple inputs to guess verification codes or answers, we applied rate limiting on our API endpoints. After a certain number of failed attempts, requests are temporarily blocked. This protects the platform from being overwhelmed and ensures fairness and security for legitimate users, (Figure 4.7).



SecureJoin
أمّن مجموعتك عبر بوابة الانضمام الآمنة
سجل الدخول

ادخل مجموعة بامان

عدد المحاولات المتبقية: 0

متبقي على نهاية الحظر 24 ساعة

التحقق عبر رقم الهاتف

رمز التحقق

1 2 3 4 5 6

تحقق من الرمز
إعادة الإرسال بعد 20 ثانية

Figure 4.7: Temporary Access Block for Security Enforcement.

- **All verification logic handled on the server side**: All sensitive verification checks—such as matching user inputs against database records or verifying code authenticity—are handled entirely on the server. This design prevents attackers from bypassing security by manipulating client-side code, since all verification happens through secure backend API calls. Keeping the logic server-side greatly enhances the reliability and security of the verification process.

- **Secure token validation**: Every administrative action—like creating questions, managing user lists, or generating links—requires a securely generated token. These tokens are issued through our authentication provider (Clerk) and validated on the server before allowing any action. This ensures that only authenticated and authorized admins can perform sensitive tasks, protecting the system from unauthorized access or misuse.

## 4.4 Conclusion

This chapter detailed the full implementation process of the SecureJoin platform, transitioning from conceptual design to a fully operational system. The chapter covered the technology stack selection, system architecture, core functionalities, user interface design considerations, security measures, and integration with third-party services.

Through the use of modern frontend and backend technologies, combined with a layered architecture and strong server-side security practices, SecureJoin successfully addresses the core challenges of managing secure group access on messaging platforms such as WhatsApp and Telegram. The platform's modular design, user-centered verification flows, and emphasis on robust authentication mechanisms collectively contribute to a scalable, secure, and user-friendly solution.

The insights gained during the implementation phase, supported by rigorous testing and iterative refinement, have laid a strong foundation for evaluating the platform's effectiveness in real-world use cases, which will be further discussed in the following chapter.

# Chapter 5

# TESTING AND RESULTS

# CHAPTER FIVE
# TESTING AND RESULTS

## 5.1 Introduction

Following the full implementation of the SecureJoin platform, this chapter presents the testing strategies, methodologies, and results obtained through comprehensive usability evaluations and system validation procedures. The primary objective of the testing phase was to ensure that SecureJoin not only functions correctly from a technical perspective but also delivers a seamless, efficient, and intuitive user experience.

Testing activities focused on two major dimensions:
**- System Testing:** Evaluating the platform's technical functionality, performance, security robustness, and ability to prevent unauthorized access and spam.
**- Usability Testing:** Assessing the platform's user experience based on three critical usability criteria:

- **Effectiveness:** Measuring users' ability to accurately and confidently complete core tasks.
- **Efficiency:** Evaluating the time and effort required to complete verification and access tasks.
- **Learnability:** Assessing how easily new users could understand and begin using the system without external guidance or training.

Testing involved two primary user groups:

- **Administrators:** Responsible for setting up groups, creating secure verification workflows, and managing group access approvals.
- **End Users:** Individuals attempting to join groups by completing verification challenges or code-based access procedures.

The combined results from both system testing and usability evaluations provide a comprehensive assessment of SecureJoin's functionality, user experience quality, and areas for future enhancement.

## 5.2 System and Software Testing

Following system development and deployment, comprehensive testing was conducted to validate both the technical robustness and the user experience quality of the SecureJoin platform. This section presents the outcomes of technical system validation as well as structured usability evaluations. Testing activities were organized into two complementary streams:

- **System Testing:** Focused on technical functionality, performance, and security validation.
- **Software Usability Testing:** Focused on measuring effectiveness, efficiency, and learnability from a user-centered perspective.

### 5.2.1 System Testing

System testing was conducted to evaluate the technical functionality, security resilience, and performance stability of SecureJoin under realistic usage conditions.

#### 5.2.1.1 Functional Testing

Functional testing verified the core features of SecureJoin, ensuring alignment with platform specifications:

- **User Registration and Authentication:** Users could successfully register and authenticate via SMS or email verification codes.
- **Custom Verification Questions:** Administrators could create and manage custom quizzes for group access control.
- **OTP Verification:** OTPs were correctly generated, delivered, validated, and expired after use, preventing reuse.
- **Credential Reuse Prevention:** Verification credentials, once used, were immediately invalidated to prevent unauthorized reuse.

Result: All functional tests passed successfully, confirming workflow accuracy and system integrity.

#### 5.2.1.2 Security Testing

Security testing evaluated SecureJoin's ability to resist common attack vectors:

- **One-Time Code Enforcement:** OTPs were invalidated immediately after successful use.
- **Brute Force Protection:** Rate-limiting and IP blocking mechanisms effectively thwarted repeated unauthorized access attempts.
- **Server-Side Validation:** All critical verification logic was enforced securely server-side, eliminating client-side vulnerabilities.

Result: SecureJoin demonstrated strong defense against anticipated security threats

#### 5.2.1.3 Performance Testing

Performance testing assessed system behavior under increasing user load:

- **Concurrent Verification Requests:** Simulated multiple users registering and verifying simultaneously, with stable system performance.
- **Database Query Handling:**High efficiency was maintained in verification code generation, lookup, and expiration under load.

Result: SecureJoin successfully handled concurrent verification scenarios without significant latency or errors.

### 5.2.2 Software Usability Testing

In addition to technical validation, usability testing was conducted to assess user experience quality.

#### 5.2.2.1 Testing Methodology

Usability testing employed both qualitative and quantitative methods:

**Participants**: 15 total participants, divided into:

- **5 Administrators:** Focused on group setup, verification management, and approval workflows.

- **10 End Users:** Focused on accessing groups via verification challenges and OTP codes.

Participants were assigned defined tasks targeting three critical usability criteria:

- **Effectiveness:** Accuracy and confidence in task completion.
- **Efficiency:** Speed and effort involved in task completion.
- **Learnability:** Ease of understanding and using the system without external help.

Structured interviews and task performance metrics were collected for analysis.

#### 5.2.2.2 Key Findings

**Effectiveness**

- All participants successfully completed assigned tasks.
- No system malfunctions or task errors were observed.
- 100% of participants rated their task confidence a perfect 5/5.
- Participants reported that key features were easy to locate and use.

**Efficiency**

- Administrators required between 30 seconds to 4 minutes, depending on the number of verification questions configured (average 4–6 clicks)..
- End users completed verification processes in 2–4 minutes, averaging 3–4 clicks.
- Task flow was described as smooth and logical, without unnecessary steps.

**Learnability**

- Every participant, including both admins and users, was using the SecureJoin system for the first time. Despite the lack of prior experience, all users were able to begin their tasks effortlessly and without any external assistance or instructions. One user shared, “It was extremely easy to get started because the labels and icons were clear.” Another admin echoed this sentiment by saying, “The clear button labels made it very easy to begin.”

- When asked whether they needed help or relied on trial and error to navigate the platform, the answers were unanimously negative. As one admin put it, “No, the interface was intuitive enough to navigate without help.” A different admin confirmed, “I figured it out by myself.”
- Participants consistently described the design elements as intuitive. One user stated, “Everything was simple to understand,” while another added, “All buttons and labels were clear and easy to understand.”.
- On a scale of 1 to 5, all participants rated the ease of task comprehension a 5. One admin commented, “I’d rate it a 5; it was really easy,” while a user said, “I would rate this as a 5; it was very easy to understand how to proceed.”
- When asked if they felt confident repeating the same task without guidance, every participant responded positively. One admin concluded, “Yes, I’m confident I could do it again alone,” and a user said, “Yes, I feel sure I could do it again by myself.”

These responses reflect a strong degree of learnability in the SecureJoin platform, demonstrating that even first-time users can navigate and complete tasks with ease and confidence.

graphicx

| Participant | Task Completed | Errors Encountered | Confidence (1–5) | Time (min) | Clicks | Smoothness (1–5) | Repeat Task Easily |
|---|---|---|---|---|---|---|---|
| Admin 1 | Yes | No | 5 | 5.0 | 6 | 5 | Yes |
| Admin 2 | Yes | No | 4 | 4.0 | 6 | 4 | Yes |
| Admin 3 | Yes | No | 5 | 5.0 | 10 | 5 | Yes |
| Admin 4 | Yes | No | 4 | 3.0 | 5 | 5 | Yes |
| Admin 5 | Yes | No | 5 | 0.5 | 4 | 5 | Yes |
| User 1 | Yes | No | 5 | 2.0 | 3 | 5 | Yes |
| User 2 | Yes | No | 5 | 3.0 | 3 | 5 | Yes |
| User 3 | Yes | No | 5 | 3.0 | 7 | 5 | Yes |
| User 4 | Yes | No | 5 | 3.0 | 3 | 5 | Yes |
| User 5 | Yes | No | 5 | 4.0 | 4 | 5 | Yes |

Table 5.1: Usability Test Results for SecureJoin

#### 5.2.2.3 Insights and Improvements

Although SecureJoin’s usability performance was rated highly, several opportunities for refinement were identified:

- **Tooltips for New Admins:** Adding contextual tooltips could provide helpful micro-instructions during group setup.
- **Step-by-Step Onboarding Wizard:** A guided setup process could reduce time spent configuring group settings for first-time administrators.

- **Click-Tracking Implementation:** Analyzing user click paths could help identify any hidden friction points in the interface, allowing for targeted UX optimizations.

These improvements aim to make the platform even more user-friendly, particularly for new administrators. Full participant feedback and interview responses are available in Appendix D.

## 5.3 Results and Analysis

The testing results confirmed that the SecureJoin platform successfully achieves its primary objectives: securing group access, minimizing spam, preventing unauthorized link sharing, and maintaining a seamless user experience. Both technical system testing and structured usability evaluations demonstrate that the platform performs reliably, efficiently, and intuitively across its intended use cases.

Key findings include:

### 5.3.1 Effectiveness

All participants completed their assigned tasks successfully, without errors or system malfunctions. Confidence ratings were uniformly high, demonstrating that the platform's core functionalities are intuitive and reliable.

### 5.3.2 Efficiency

Both administrators and end users completed tasks rapidly with minimal steps, highlighting an optimized user flow. System responsiveness remained consistently high during testing.

### 5.3.3 Learnability

First-time users were able to navigate and complete tasks independently, without requiring external assistance. Participants praised the intuitive design, clear labels, and logical task progression.

**Common feedback included:**

- "Everything was simple to understand."
- "The interface made it clear what to do next."
- "I didn't need any guidance—everything just made sense."

The results validate SecureJoin's strength in balancing robust security measures with a high-quality user experience. The platform's effectiveness in enforcing secure group access, combined with its efficient and learnable interface, positions it as a strong candidate for broader adoption. Minor improvement areas, such as enhanced onboarding support for new administrators, were identified through participant feedback and will guide future iterations.

### 5.3.4 Summary of User Feedback

| **Criterion** | **Score (1–5)** | **Summary** |
|---|---|---|
| Effectiveness | 5 | All tasks completed accurately without issues. |
| Efficiency | 5 | Quick task completion with minimal clicks and no delays. |
| Learnability | 5 | Clear interface and confident usage by first-time users. |

Table 5.2: Performance Evaluation Table

## 5.4 Recommendations and Future Improvements

While testing confirmed the overall usability, functionality, and security of the SecureJoin platform, several enhancements were identified to further refine the user experience and system performance:

### 5.4.1 Admin Onboarding Enhancements

- **Tooltips for New Administrators:** Introduce contextual tooltips that explain key features during setup and configuration.

- **First-Time Setup Wizard:** Implement a guided onboarding process to walk administrators through essential steps when creating groups and setting verification workflows.

### 5.4.2 Interface Analytics

- **Click-Tracking and Interaction Monitoring:** Enable click-tracking mechanisms to collect data on user interactions, helping identify workflow bottlenecks and opportunities for interface optimization.

### 5.4.3 Accessibility Enhancements

- **Keyboard Navigation Support:**Expand keyboard operability to ensure that all platform functions can be accessed without a mouse, enhancing accessibility.
- **Screen Reader Compatibility:** Improve compatibility with screen readers to provide a more inclusive experience for visually impaired users.

## 5.5 Conclusion

The testing phase confirmed that SecureJoin is a robust, intuitive, and user-centered platform that effectively meets its functional and usability objectives. All participants—regardless of their role as administrators or end users—were able to complete their tasks confidently, efficiently, and with minimal effort. The positive feedback collected during testing provides a strong foundation for future iterative enhancements, ensuring that SecureJoin continues to evolve in line with user needs and technological advancements. Overall, the platform demonstrates a strong balance between security, usability, and scalability, positioning it as a promising solution for secure group access management across digital communication platforms.

# Chapter 6

# CONCLUSION

# CHAPTER SIX<br>CONCLUSION

## 6.1 Conclusion

This chapter provides a comprehensive conclusion to the SecureJoin project, summarizing its objectives, major achievements, challenges encountered, contributions made, and outlining key recommendations for future development. It reflects on the project's outcomes relative to its initial goals and highlights opportunities for further refinement and expansion.

## 6.2 Project Summary

SecureJoin was conceived as a solution to address significant security vulnerabilities and usability challenges associated with group access in popular messaging platforms such as WhatsApp and Telegram. The project aimed to build a web-based platform that empowers group administrators to manage membership securely, using multi-layered verification techniques while maintaining a seamless and intuitive user experience.

This project involved:

- **Problem Identification and Objectives:** Defining the vulnerabilities faced by public chat groups and establishing goals centered on improving access control, reducing spam, and enhancing usability.
- **Literature Review** Analyzing prior research on security challenges in social media, group authentication methods, spam detection techniques, and the role of usability in system security.
- **Methodology and System Design:** Applying a prototype-based, user-centered Agile development approach to build a scalable, secure, and accessible platform.
- **Implementation and Testing:** Successfully developing, deploying, and validating SecureJoin through systematic system testing and user-centered usability evaluations.

Through these stages, SecureJoin evolved from a conceptual solution into a fully functional, tested platform.

## 6.3 Key Achievements

The project resulted in several notable accomplishments:

1. **Secure Group Access Management:**
   - Development of verification workflows including custom quiz questions and one-time-use OTP codes, effectively minimizing unauthorized access and spam.
   - Building a user-friendly interface that ensures accessibility while maintaining high-security standards.
2. **Robust Security Infrastructure:**
   - Implementation of server-side validation, credential reuse prevention, and brute-force attack protections.
3. **User-Centered Interface:**
   - Creation of a responsive, intuitive frontend interface, validated by high scores in usability testing across effectiveness, efficiency, and learnability dimensions.
4. **System Integration:**
   - Successful integration with Clerk (authentication management), Supabase (real-time database support), and Waha (OTP delivery API).
5. **Validation through Testing:**
   - Positive outcomes from technical system testing and structured usability testing, confirming that SecureJoin meets its original objectives.

## 6.4 Challenges and Lessons Learned

During the development and testing phases, several challenges were encountered:

- **Third-Party API Limitations:** Integrating external services like Clerk and Waha required managing API constraints such as rate limits and response delays.
- **Third-Party API Limitations:** Ensuring that the system could handle concurrent verification requests and increasing user loads necessitated backend optimization.

- **Third-Party API Limitations:** Coordinating structured usability testing sessions with participants introduced scheduling challenges but ultimately provided valuable insights.

**Lessons Learned:**

- Early planning for scalability is critical for long-term system growth.
- External API dependencies require fallback strategies to maintain system reliability.
- Continuous usability feedback significantly enhances product design and user satisfaction.

## 6.5 Future Work

Although SecureJoin successfully meets its current objectives, several areas have been identified for future development and enhancement:

### 6.5.1 Database-Linked User Authentication

Future versions of SecureJoin should integrate a **full database-linked user authentication system**, allowing administrators to pre-upload lists of authorized members (e.g., student or employee databases). This would allow the system to automatically validate a user's eligibility before access is granted, improving security and efficiency.

### 6.5.2 Admin Onboarding Enhancements

- **Tooltips and Micro-Guides:** Provide real-time assistance through context-sensitive help during group setup.
- **Interactive Setup Wizard:** Guide administrators through the initial configuration process to streamline onboarding.

### 6.5.3 Advanced Security Features

- **Multi-Factor Authentication (MFA):** Introduce additional security layers by supporting MFA for administrative accounts.
- **Dynamic Threat Monitoring:** Implement real-time monitoring to detect and block suspicious activities.

### 6.5.4 Accessibility Enhancements

- **Keyboard Navigation Support:** Expand platform functionality for users relying on keyboard-only input.
- **Screen Reader Optimization:** Ensure full compatibility with screen readers and other assistive technologies.

### 6.5.5 Platform Expansion

- **Support for Additional Messaging Services:** Extend SecureJoin's capabilities to integrate with platforms like Slack, Discord, and Microsoft Teams, beyond just WhatsApp and Telegram.

## 6.6 Final Remarks

The SecureJoin project successfully addressed critical challenges in group access security and usability within messaging platforms. By balancing robust security mechanisms with user-centered design, SecureJoin delivers a strong foundation for safer and more controlled digital communications.

Testing and usability evaluations confirm that SecureJoin meets its intended objectives, providing a reliable, scalable, and intuitive solution for group management. The lessons learned and user feedback gathered during this phase offer valuable guidance for future iterations, particularly as the platform scales to accommodate broader user bases and evolving security requirements.

With its secure architecture, positive usability validation, and clear pathways for future improvements—such as database-linked authentication and enhanced onboarding—SecureJoin is well-positioned for continued growth and wider adoption in the digital communication ecosystem.

# Appendix

- **Appendix A: Survey Link**

  `https://forms.gle/a57rxf7L1ztCEQY39`

- **Appendix B: GitHub Repository**

  `https://github.com/SenQii/securejoin`

- **Appendix C: Project Website**

  `https://securejoin-dev.vercel.app`

- **Appendix D: Usability Testing Interview Responses**

  Detailed participant feedback categorized by usability criteria. *(See next page)*

# Appendix D: Usability Testing Interview Responses

This appendix presents the detailed answers collected during the usability testing phase. A total of 15 participants were interviewed—5 administrators and 10 regular users. The responses are categorized under three key usability criteria: **Effectiveness**, **Efficiency**, and **Learnability**.

## Administrator Responses

### Admin 1

**Effectiveness**

Were you able to complete the task successfully? Yes.

Did you encounter any errors or unexpected results? No.

On a scale of 1–5, how confident were you that you completed the task correctly? 5.

Was any important information or function difficult to find? No.

If you made a mistake, how easy was it to correct? The interface appeared user-friendly for corrections.

**Efficiency**

Time taken: About 5 minutes.

Clicks: Around 6.

Any step felt longer than needed? No.

Did you find what you needed quickly? Yes.

Smoothness rating: 5.

**Learnability**

First time using the system? Yes, very easy to get started.

Help or instructions needed? No.

Were buttons and labels easy to understand? Yes.

Ease of task (1–5): 5.

Can repeat task without guidance? Yes.

### Admin 2

#### Effectiveness

Task completed successfully? Yes.

Errors encountered? No.

Confidence (1–5): 4.

Difficult info to find? No.

Correction ease? Did not make mistakes, but layout seemed straightforward.

#### Efficiency

Time: Around 4 minutes.

Clicks: About 6.

Any unnecessarily complex step? No.

Found what needed quickly? Yes.

Smoothness: 4.

#### Learnability

First time? Yes, easy to begin.

Help needed? No.

Labels and buttons clear? Yes.

Ease rating: 5.

Repeat task alone? Absolutely.

### Admin 3

#### Effectiveness

Task completion: Yes.

Errors? No.

Confidence: 5.

Any difficulties? No.

Ease of correction? Did not make mistakes, but easy to fix.

**Efficiency**

Time: About 9 minutes.

Clicks: Around 10.

Complex steps? No.

Quick navigation? Yes.

Smoothness: 5.

**Learnability**

First time? Yes, easy to start.

Help needed? No.

Buttons/icons understandable? Yes.

Ease rating: 5.

Repeat without help? Yes.

**Admin 4**

**Effectiveness**

Completed successfully? Yes.

Errors? No.

Confidence level: 4.

Any hard-to-find info? No.

Correction? Didn't make mistakes, but seemed easy.

**Efficiency**

Time: Around 3 minutes.

Clicks: About 5.

Unnecessarily complex? No.

Ease of access? Yes.

Smoothness: 5.

### Learnability

First time? Yes, easy to start.

Need for instructions? No.

Understandable interface? Yes.

Ease rating: 5.

Confidence in repeating? Yes.

## Admin 5

### Effectiveness

Task success? Yes.

Errors? No.

Confidence score: 5.

Any difficult info? No.

Ease of corrections? Quick adjustments possible.

### Efficiency

Time taken: 30 seconds.

Clicks: 4.

Any complex step? No.

Quick navigation? Yes.

Smoothness: 5.

### Learnability

First time? Yes, clear button labels helped.

Need help? No.

Interface clear? Yes.

Ease of task (1–5): 5.

Repeat task without help? Yes.

### User Responses

The following summary highlights the common patterns observed across all 10 users during the evaluation:

**Effectiveness**

- All users completed the task successfully.
- No errors or unexpected results reported.
- Confidence rating: All rated 5.
- No difficulty in finding information.
- Correction (if needed): Very easy, even for new users.

**Efficiency**

- Time taken: Between 2 to 4 minutes.
- Clicks: Averaged 3–4.
- No steps felt overly complex.
- Everything was found quickly.
- Smoothness rating: All rated 5.

**Learnability**

- First time using the platform: Yes (for all).
- No help or instructions needed.
- All users said buttons and labels were clear.
- Ease of figuring out task: All rated 5.
- All users felt they could repeat the task confidently without assistance.

### User Responses

The following summary highlights the common patterns observed across all 10 users during the evaluation:

**Effectiveness**

- All users completed the task successfully
- No errors or unexpected results reported
- Confidence rating: All rated 5
- No difficulty in finding information
- Correction (if needed): Very easy, even for new users

**Efficiency**

- Time taken: Between 2 to 4 minutes
- Clicks: Averaged 3–4
- No steps felt overly complex
- Everything was found quickly
- Smoothness rating: All rated 5

**Learnability**

- First time using the platform: Yes (for all)
- No help or instructions needed
- All users said buttons and labels were clear
- Ease of figuring out task: All rated 5
- All users felt they could repeat the task confidently without assistance

# References

[1] N. Rastogi and J. Hendler, "Whatsapp security and role of metadata in preserving privacy," *Rensselaer Polytechnic Institute, Troy, NY, USA*, 2024.

[2] N. A. Nawaz, K. Ishaq, U. Farooq, A. Khalil, S. Rasheed, A. Abid, and F. Rosdi, "A comprehensive review of security threats and solutions for the online social networks industry," *PeerJ Comput. Sci.*, vol. 9, p. e1143, 2022.

[3] T. B. G. Herath, P. Khanna, and M. Ahmed, "Cybersecurity practices for social media users: A systematic literature review," *Journal of Cybersecurity and Privacy*, vol. 2, no. 1, pp. 1–18, 2022.

[4] R. Singh, A. N. S. Chauhan, and H. Tewari, "Blockchain-enabled end-to-end encryption for instant messaging applications," in *2022 IEEE 23rd International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, 2022, pp. 501–506.

[5] H. Lahti, M. Kokkonen, L. Hietajärvi, N. Lyyra, and L. Paakkari, "Social media threats and health among adolescents," *Child and Adolescent Psychiatry and Mental Health*, vol. 18, no. 62, 2024.

[6] S. Oesch, R. Abu-Salma, O. Diallo, J. Krämer, J. Simmons, J. Wu, and S. Ruoti, "User perceptions of security and privacy for group chat," *Digital Threats: Research and Practice*, vol. 3, no. 2, pp. 1–29, 2022.

[7] H. C. Chen, C. H. Mao, Y. T. Lin, T. L. Kung, and C. E. Weng, "A secure group-based mobile chat protocol," *Journal of Ambient Intelligence and Humanized Computing*, vol. 7, no. 5, pp. 681–695, 2016.

[8] O. Diallo, S. Yang, and M. Krueger, “Managing dynamic group membership in the evolving digital spaces,” *International Journal of Computer Applications*, vol. 12, no. 7, pp. 102–118, 2021.

[9] S. Kaddoura, G. Chandrasekaran, D. E. Popescu, and J. H. Duraisamy, “A systematic literature review on spam content detection and classification,” *PeerJ Comput. Sci.*, vol. 8, 2022.

[10] A. Sharma, M. Manisha, and R. Jain, “A survey on spam detection techniques,” *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 3, no. 12, pp. 8688–8690, 2014.

[11] J. Saltzer and M. D. Schroeder, “Usability of security: A case study,” in *Proceedings of the International Conference on Human-Computer Interaction*, 2020, pp. 123–134.

[12] A. Juels and M. Wattenberg, “A usability study of five two-factor authentication methods,” *Journal of Usability Studies*, vol. 15, no. 3, pp. 123–138, 2020.

[13] J. E. C. Hong, A. C. King, and T. McDonald, “Security and usability: The case of user authentication methods,” *Journal of Information Security*, vol. 9, no. 1, pp. 45–60, 2020.

[14] B. Schneier, M. D. Schroeder, and L. Lamport, “Evaluating user perception of multi-factor authentication: A systematic review,” *ACM Computing Surveys*, vol. 54, no. 6, pp. 1–38, 2021.

[15] N. L. Clarke, S. Furnell, and M. Sanderson, “Usable security: User preferences for authentication methods in ebanking and the effects of experience,” *Oxford Academic*, vol. 11, no. 2, pp. 120–135, 2021.

[16] A. A. Abdo, K. Alhajri, A. Alyami *et al.*, “Ai-based spam detection techniques for online social networks: challenges and opportunities,” *Journal of Internet Services and Information Security*, vol. 13, no. 3, pp. 78–103, 2023.

[17] A. Soliman and S. Girdzijauskas, “Dlsas: Distributed large-scale anti-spam framework for decentralized online social networks,” in *2016 IEEE 2nd International Conference on Collaboration and Internet Computing (IEEE CIC)*, Pittsburgh, PA, USA, 2016, pp. 363–372.