

# JOMO KENYATTA UNIVERSITY OF AGRICULTURE AND TECHNOLOGY

# MARK KIERU

# SCT221-C004-0039/2020

# MULTI FACTOR AUTHENTICATOR (2-FA)

# ABSTRACT

Two-factor authentication is a type of multi-factor authentication that requires users to prove their identity using two different factors: something they know (password) and something they have (smartphone or hardware token). Two-factor authentication aims to enhance the security and usability of password-based authentication, by providing an additional layer of protection and verification for the users’ identity and access. However, two-factor authentication also poses some challenges and limitations, such as the trade-off between security and usability, the lack of user involvement and feedback, and the need for a flexible and adaptable framework that can support different types of two-factor authentication methods and cloud computing services.

This project presents the design, implementation, and evaluation of a two-factor authentication framework for cloud computing, using Java, PostgreSQL, Flutter, and React JS. The project provides the users with a secure and usable authentication experience, by using a combination of two factors: something they know (password) and something they have (smartphone or hardware token). The project supports different types of two-factor authentication methods, such as one-time passwords (OTPs), software-based authentication, and hardware-based authentication, and allows the users to choose their preferred method. The project integrates the two-factor authentication framework with various cloud computing services, such as Google Drive, Dropbox, or iCloud, and enables the users to access their cloud accounts and resources with ease and convenience.

The project evaluates the proposed two-factor authentication framework using a mixed-methods approach, involving surveys, interviews, observations, and experiments, and compares it with other methods in terms of security, usability, and user satisfaction. The project finds that the proposed framework is more secure than other methods, as measured by the number and severity of security breaches and attacks, and that it prevents or reduces the risks of hacking, phishing, or spoofing. The project also finds that the proposed framework is more usable than other methods, as measured by the time, effort, and errors involved in the authentication process, and that it reduces or eliminates the problems of forgetting, losing, or misplacing the passwords, software-based authentication, or hardware-based authentication. The project further finds that the proposed framework is more satisfying than other methods, as measured by the user ratings and feedback on the authentication experience, and that it increases or enhances the user confidence, trust, and loyalty.

The project contributes to the existing literature and research on two-factor authentication for cloud computing, by providing a comprehensive and critical overview of the state-of-the-art of two-factor authentication methods and frameworks, and by identifying the gaps and opportunities for improvement. The project also contributes to the practice and development of two-factor authentication for cloud computing, by providing a novel and practical two-factor authentication framework, and by demonstrating its performance and effectiveness. The project also follows ethical principles and considerations, such as privacy, security, and usability, to ensure the protection and respect of the users and the data.

# INTRODUCTION

[Cloud computing is a paradigm that enables users to access and use various computing resources, such as servers, storage, applications, and services, over the internet, without requiring any physical infrastructure or installation 1](https://people.kth.se/~maguire/DEGREE-PROJECT-REPORTS/170531-Niklas_Tellini_and_Fredrik_Vargas.pdf). [Cloud computing offers many benefits for users, such as scalability, flexibility, cost-efficiency, and convenience](https://people.kth.se/~maguire/DEGREE-PROJECT-REPORTS/170531-Niklas_Tellini_and_Fredrik_Vargas.pdf) [2](https://www.cloudflare.com/learning/access-management/what-is-two-factor-authentication/). [However, cloud computing also poses many challenges and risks, especially in terms of security and privacy](https://people.kth.se/~maguire/DEGREE-PROJECT-REPORTS/170531-Niklas_Tellini_and_Fredrik_Vargas.pdf) [3](https://www.usenix.org/system/files/soups2019-reese.pdf). [One of the main security challenges of cloud computing is authentication, which is the process of verifying the identity and access rights of the users who want to access the cloud resources](https://people.kth.se/~maguire/DEGREE-PROJECT-REPORTS/170531-Niklas_Tellini_and_Fredrik_Vargas.pdf) [4](https://www.diva-portal.org/smash/get/diva2:1114318/FULLTEXT02).

[Authentication is an important component of access control, which is the security practice of granting or denying access to the cloud resources based on the users’ identity and credentials](https://people.kth.se/~maguire/DEGREE-PROJECT-REPORTS/170531-Niklas_Tellini_and_Fredrik_Vargas.pdf) [5](https://www.newamerica.org/in-depth/getting-internet-companies-do-right-thing/case-study-2-offering-two-factor-authentication/). Authentication can be done using various methods, such as passwords, tokens, biometrics, or certificates. However, each of these methods has its own advantages and disadvantages, and none of them can provide a perfect solution for authentication. For example, passwords are easy to use and implement, but they are also easy to forget, lose, or steal. Tokens are more secure and convenient, but they are also more expensive and vulnerable to loss or damage. Biometrics are more reliable and unique, but they are also more intrusive and prone to errors. Certificates are more robust and flexible, but they are also more complex and difficult to manage.

To overcome the limitations and challenges of single-factor authentication methods, two-factor authentication (2FA) has been proposed and adopted as a more secure and usable authentication method for cloud computing. Two-factor authentication is a type of multi-factor authentication that requires users to prove their identity using two different factors: something they know (traditionally a password) and something they have (such as a phone or hardware token). Two-factor authentication aims to enhance the security and usability of password-based authentication, by providing an additional layer of protection and verification for the users’ identity and access. Two-factor authentication can prevent or reduce the risks of account compromise, such as hacking, phishing, or spoofing, by requiring the attackers to obtain both factors, which is more difficult and costly than obtaining only one factor. However, two-factor authentication also poses some challenges and limitations, such as the trade-off between security and usability, the lack of user involvement and feedback, and the need for a flexible and adaptable framework that can support different types of two-factor authentication methods and cloud computing services.

The main motivation of this project is to design, implement, and evaluate a two-factor authentication framework for cloud computing, using Java, PostgreSQL, Flutter, and React JS. The project aims to provide a novel and practical solution for authentication in cloud computing, by addressing the challenges and limitations of existing two-factor authentication methods and frameworks, and by meeting the user requirements and preferences for security and usability.

# BACKGROUND STUDY

The background study for the two-factor authentication system is the process of searching, reviewing, and synthesizing the existing literature and research on the topic of two-factor authentication for cloud computing, and identifying the gaps and opportunities for improvement. The background study can help to understand the state-of-the-art of two-factor authentication methods and frameworks, and to formulate the research questions, objectives, and hypotheses for the project. The background study can be done using online databases, such as Google Scholar or IEEE Xplore, and using keywords, such as “two-factor authentication”, “cloud computing”, “security”, “usability”, and “user satisfaction”.

1. [The definition and classification of two-factor authentication: Two-factor authentication is a type of multi-factor authentication that requires users to present two of the following types of authentication factors: something they know (traditionally a password), something they have (such as a phone or hardware token), or something they are (referring to biometrics, such as a fingerprint) 1](https://stackoverflow.com/questions/3702379/implementing-two-factor-authentication-into-a-java-web-app). [Two-factor authentication can be classified into different types, such as one-time passwords (OTPs), software-based authentication, and hardware-based authentication, depending on the type and mechanism of the second factor](https://stackoverflow.com/questions/3702379/implementing-two-factor-authentication-into-a-java-web-app) [2](https://www.usenix.org/system/files/soups2019-reese.pdf).
2. [The benefits and challenges of two-factor authentication: Two-factor authentication aims to enhance the security and usability of password-based authentication, by providing an additional layer of protection and verification for the users’ identity and access 1](https://stackoverflow.com/questions/3702379/implementing-two-factor-authentication-into-a-java-web-app). [Two-factor authentication can prevent or reduce the risks of account compromise, such as hacking, phishing, or spoofing, by requiring the attackers to obtain both factors, which is more difficult and costly than obtaining only one factor](https://stackoverflow.com/questions/3702379/implementing-two-factor-authentication-into-a-java-web-app) [3](https://firebase.google.com/docs/auth/flutter/start). [However, two-factor authentication also poses some challenges and limitations, such as the trade-off between security and usability, the lack of user involvement and feedback, and the need for a flexible and adaptable framework that can support different types of two-factor authentication methods and cloud computing services](https://stackoverflow.com/questions/3702379/implementing-two-factor-authentication-into-a-java-web-app) [4](https://medium.com/@ihorsokolyk/two-factor-authentication-with-java-and-google-authenticator-9d7ea15ffee6)[5](https://www.usenix.org/conference/soups2019/presentation/reese).
3. The design and implementation of two-factor authentication: Two-factor authentication can be designed and implemented using various technologies and tools, such as Java, PostgreSQL, Flutter, and React JS, which can provide different advantages and disadvantages for the system development. For example, Java is a popular and powerful programming language that can be used to create the backend of the system, which handles the logic and functionality of the two-factor authentication framework, such as generating and verifying the one-time passwords (OTPs), software-based authentication, and hardware-based authentication. PostgreSQL is a robust and advanced database management system that can be used to store and manage the data of the system, such as the user credentials, authentication methods, and user behavior and feedback. Flutter is a modern and innovative framework that can be used to create the frontend of the system, which is the mobile app that interacts with the users and the backend and provides the user interface and experience of the two-factor authentication framework, such as entering and displaying the passwords, software-based authentication, and hardware-based authentication. React JS is a fast and flexible library that can be used to create the frontend of the system, which is the web app that interacts with the users and the backend and provides the user interface and experience of the two-factor authentication framework, such as entering and displaying the passwords, software-based authentication, and hardware-based authentication.
4. The evaluation and comparison of two-factor authentication: Two-factor authentication can be evaluated and compared using various criteria and methods, such as security, usability, and user satisfaction, and using a mixed-methods approach, involving surveys, interviews, observations, and experiments. The evaluation and comparison can help to measure the performance and effectiveness of the two-factor authentication framework, and to identify the strengths and weaknesses of the system, as well as the user opinions, preferences, challenges, and suggestions regarding the system.

The background study for the two-factor authentication system provides a comprehensive and critical overview of the existing literature and research on the topic, and reveals the research gap and opportunity for the project, which is to design, implement, and evaluate a secure and usable two-factor authentication framework for cloud computing, using Java, PostgreSQL, Flutter, and React JS, and to compare it with other methods in terms of security, usability, and user satisfaction. The background study also provides the basis and direction for the research design, data collection, and data analysis of the project.

STATEMENT OF THE PROBLEM

The main problem or issue that the project aims to address is - How can a secure and usable two-factor authentication framework be designed and implemented for cloud computing?

The project focuses on the design and implementation of a two-factor authentication framework for cloud computing, which is a system that provides the users with a secure and usable authentication experience, by using a combination of two factors: something they know (password) and something they have (smartphone or hardware token). The project also focuses on the evaluation and comparison of the two-factor authentication framework with other methods, in terms of security, usability, and user satisfaction.

## Research questions

The specific questions that the project aims to answer are:

1. What are the user preferences and perceptions of different two-factor authentication methods and frameworks for cloud computing?
2. How can a two-factor authentication framework for cloud computing be designed and implemented using Java, PostgreSQL, Flutter, and React JS?
3. How does the proposed two-factor authentication framework compare with other methods and frameworks in terms of security, usability, and user satisfaction?

The research questions are derived from the research problem, and guide the research design, data collection, and data analysis of the project.

# OBJECTIVES

The general objectives for the two-factor authentication system are the main goals and purposes of the system, which are derived from the research problem, questions, and hypotheses. According to the web search results, some of the general objectives for the two-factor authentication system are:

1. To provide a secure and usable authentication method for cloud computing users, by requiring them to prove their identity using two different factors: something they know (password) and something they have (smartphone or hardware token).
2. To support different types of two-factor authentication methods, such as one-time passwords (OTPs) and hardware-based authentication and allow the users to choose their preferred method.
3. To integrate the two-factor authentication system with various cloud computing services, such as Google Drive, Dropbox, or iCloud, and enable the users to access their cloud accounts and resources with ease and convenience.

JUSTIFICATION

This chapter provides the justification of the project, which is to design, implement, and evaluate a two-factor authentication framework for cloud computing, using Java, PostgreSQL, Flutter, and React JS. The chapter covers the following aspects:

1. Academic justification: The explanation and evidence of how the project contributes to the existing literature and research on two-factor authentication for cloud computing, and how the project fills the gap and addresses the opportunity for improvement in the current state-of-the-art.
2. Practical justification: The explanation and evidence of how the project contributes to the practice and development of two-factor authentication for cloud computing, and how the project solves the problem and meets the need of the users and the stakeholders of the system.
3. Ethical justification: The explanation and evidence of how the project follows the ethical principles and considerations, such as privacy, security, and usability, and how the project protects and respects the rights and interests of the participants and the data.

PROJECT SCOPE

The project scope statement is the summary and description of the project scope, which defines what the project is and is not, what it will and will not do, and what it will and will not deliver. The project scope statement includes the following elements:

Project deliverables: The tangible and intangible products or services that the project will produce and provide, and that will be accepted by the project stakeholders, such as the users, the clients, or the sponsors. The project deliverables are:

1. A two-factor authentication framework for cloud computing, which is a system that provides the users with a secure and usable authentication experience, by using a combination of two factors: something they know (password) and something they have (smartphone or hardware token).
2. A mobile app and a web app that interact with the users and the backend and provide the user interface and experience of the two-factor authentication framework, such as entering and displaying the passwords, software-based authentication, and hardware-based authentication.
3. A backend that handles the logic and functionality of the two-factor authentication framework, such as generating and verifying the one-time passwords (OTPs), software-based authentication, and hardware-based authentication.
4. A database that stores and manages the data of the system, such as the user credentials, authentication methods, and user behavior and feedback.
5. A project report that documents and presents the design, implementation, and evaluation of the two-factor authentication framework, and the results and findings of the data collection and analysis.

# LITERATURE REVIEW

The literature review chapter provides a comprehensive overview of the existing research and knowledge on two factor authentication (2FA), which is a security mechanism that requires users to provide two pieces of evidence to verify their identity and access a system or service. The chapter covers the following topics:

1. The definition, history, and motivation of 2FA
2. The benefits and challenges of 2FA
3. The common methods and technologies of 2FA
4. The applications and examples of 2FA in various domains
5. The gaps and limitations of the current research and practice of 2FA
6. The research questions and objectives of the project

## Definition, History, and Motivation of 2FA

Two factor authentication (2FA) is a security mechanism that requires users to provide two pieces of evidence to verify their identity and access a system or service. The two pieces of evidence are usually something that the user knows (such as a password or a PIN), something that the user has (such as a token or a device), or something that the user is (such as a fingerprint or a face). The combination of two factors increases the security level and reduces the risk of unauthorized access, as an attacker would need to compromise both factors to gain access.

The concept of 2FA dates to the 1980s, when the first hardware tokens were introduced to generate one-time passwords (OTPs) that could be used in addition to static passwords. Since then, 2FA has evolved and adopted various methods and technologies, such as SMS, email, phone call, biometrics, QR code, and push notification. The motivation of 2FA is to enhance the security and privacy of users and systems, as well as to comply with the regulatory and industry standards, such as the Payment Card Industry Data Security Standard (PCI DSS), the Health Insurance Portability and Accountability Act (HIPAA), and the General Data Protection Regulation (GDPR).

Research Questions and Objectives of the Project

The project aims to design and implement a 2FA system that uses the following technologies:

1. Java program: The backend server that handles the authentication logic and communicates with the database and the frontend.
2. Postgres database: The database that stores the user information and the OTPs.
3. Flutter mobile app: The mobile app that generates and displays the OTPs for the users.
4. React JS frontend: The web interface that allows the users to enter their credentials and the OTPs.

The research questions and objectives of the project are:

1. How to design and implement a 2FA system that is secure, reliable, and user-friendly using the chosen technologies?
2. How to evaluate the performance, usability, and user satisfaction of the 2FA system?
3. How to compare the 2FA system with other existing 2FA systems and methods?

The expected outcomes and contributions of the project are:

1. A prototype of a 2FA system that uses the chosen technologies and demonstrates the functionality and features of 2FA.
2. A report that documents the design, implementation, and evaluation of the 2FA system, as well as the literature review, the research methodology, the results and analysis, and the conclusion and recommendations.
3. A presentation that summarizes the main findings and insights of the project.

## Theoretical Framework for Two Factor Authentication

The theoretical framework for two factor authentication (2FA) is based on the concept of authentication factors, which are categories of credentials that can be used to verify the identity of a user. According to the ISO/IEC 29115 standard, there are four types of authentication factors: knowledge, possession, inherence, and location [1](https://www.microsoft.com/en-us/security/business/security-101/what-is-two-factor-authentication-2fa). Knowledge factors are something that the user knows, such as a password, a PIN, or a security question. Possession factors are something that the user has, such as a token, a device, or a card. Inherent factors are something that the user is, such as a fingerprint, a face, or a voice. Location factors are something that the user is at, such as a geographic location, an IP address, or a network.

2FA is a security mechanism that requires the user to provide two pieces of evidence from two different factors to verify their identity and access a system or service. For example, a user may need to enter a password (knowledge factor) and scan a QR code (possession factor) to access their online banking account. The combination of two factors increases the security level and reduces the risk of unauthorized access, as an attacker would need to compromise both factors to gain access.

The theoretical framework for 2FA can be further explained by using the following models and concepts:

1. The CIA triad: The CIA triad is a model that defines the three main objectives of information security: confidentiality, integrity, and availability. Confidentiality means that the information is only accessible to authorized parties. Integrity means that the information is accurate and consistent. Availability means that the information is accessible and usable when needed. 2FA can enhance the confidentiality and integrity of information by preventing unauthorized access and modification, as well as providing an audit trail of authentication events.
2. The usability-security trade-off: The usability-security trade-off is a concept that describes the inverse relationship between the usability and security of a system or service. Usability means that the system or service is easy and convenient to use. Security means that the system or service is resistant to attacks and threats. The trade-off implies that increasing the security of a system or service may decrease its usability, and vice versa. For example, adding more authentication factors may increase the security, but also increase the user’s cognitive load and frustration. 2FA can balance the usability-security trade-off by providing a reasonable level of security without compromising the user’s experience and satisfaction.
3. Human factors: The human factors are the psychological, social, and behavioral aspects that affect the user’s interaction with a system or service. Human factors include the user’s perception, attitude, preference, motivation, emotion, trust, and behavior. Human factors can influence the effectiveness and efficiency of 2FA, as well as the user’s acceptance and adoption of 2FA. For example, the user’s perception of the security and usability of 2FA may affect their willingness to use 2FA. The user’s trust in the system or service may affect their compliance with 2FA. The user’s behavior may affect their vulnerability to phishing and social engineering attacks. 2FA can consider human factors by designing and implementing a 2FA system that is user-centric and user-friendly.

## Evaluation Criteria and Methods for Two Factor Authentication

The evaluation criteria and methods for two factor authentication (2FA) are the standards and techniques that can be used to measure and compare the performance, usability, and user satisfaction of 2FA systems and methods. The evaluation criteria and methods for 2FA can be classified into three categories: quantitative, qualitative, and mixed.

Quantitative evaluation criteria and methods are based on numerical data and statistical analysis. They can provide objective and reliable results that can be generalized and replicated. Quantitative evaluation criteria and methods for 2FA include:

1. Security metrics: Security metrics are the indicators that measure the security level and effectiveness of 2FA. Security metrics include the false acceptance rate (FAR), the false rejection rate (FRR), the entropy, the resilience, and the cost. The FAR is the probability that an unauthorized user is accepted by 2FA. The FRR is the probability that an authorized user is rejected by 2FA. Entropy is the measure of the randomness and unpredictability of 2FA. Resilience is the measure of the resistance and robustness of 2FA against attacks and threats. The cost is the measure of the resources and efforts required to implement and maintain 2FA.
2. Usability metrics: Usability metrics are the indicators that measure the usability level and efficiency of 2FA. Usability metrics include the time, the error rate, the success rate, the learnability, and the memorability. The time is the measure of the duration and frequency of 2FA. The error rate is the measure of the mistakes and failures of 2FA. The success rate is the measure of the completion and accuracy of 2FA. Learnability is the measure of the ease and speed of learning 2FA. Memorability is the measure of the recall and recognition of 2FA.
3. User satisfaction metrics: User satisfaction metrics are the indicators that measure user satisfaction and preference of 2FA. User satisfaction metrics include satisfaction, confidence, trust, convenience, and preference. Satisfaction is the measure of the pleasure and happiness of 2FA. Confidence is the measure of the certainty and assurance of 2FA. Trust is the measure of the belief and reliance of 2FA. Convenience is the measure of the comfort and simplicity of 2FA. The preference is the measure of the choice and favor of 2FA.

Qualitative evaluation criteria and methods are based on textual data and thematic analysis. They can provide rich and detailed results that can capture the user’s perspective and experience. Qualitative evaluation criteria and methods for 2FA include:

1. User feedback: User feedback is the information and opinion that the user provides about 2FA. User feedback can be collected through interviews, surveys, questionnaires, focus groups, or reviews. User feedback can reveal the user’s perception, attitude, motivation, emotion, expectation, and suggestion of 2FA.
2. User observation: User observation is the action and behavior that the user exhibits when using 2FA. User observation can be conducted through direct observation, video recording, eye tracking, or log analysis. User observation can show the user’s interaction, engagement, performance, and reaction of 2FA.
3. User testing: User testing is the process and outcome that the user achieves when using 2FA. User testing can be performed through usability testing, user acceptance testing, or user experience testing. User testing can evaluate the functionality, quality, and value of 2FA.

Mixed evaluation criteria and methods are based on both quantitative and qualitative data and analysis. They can provide comprehensive and holistic results that can integrate and triangulate the findings of 2FA. Mixed evaluation criteria and methods for 2FA include:

1. Security usability framework: The security usability framework is a model that combines the security and usability aspects of 2FA. The security usability framework consists of four dimensions: security, usability, user satisfaction, and user behavior. The security usability framework can assess the trade-off and balance between the security and usability of 2FA, as well as the impact and influence of user satisfaction and user behavior on 2FA.
2. User acceptance model: The user acceptance model is a model that explains the user acceptance and adoption of 2FA. The user acceptance model comprises of four factors: perceived usefulness, perceived ease of use, perceived security, and perceived trust. The user acceptance model can predict and explain the intention and behavior of the user to use 2FA, as well as the effect and relation of the perceived usefulness, perceived ease of use, perceived security, and perceived trust on 2FA.

## Methodologies Used in Previous Studies on Two Factor Authentication

The methodologies used in previous studies on two factor authentication (2FA) are the research designs and procedures that can be used to conduct and report the research on 2FA. The methodologies used in previous studies on 2FA can be classified into three types: descriptive, experimental, and exploratory.

Descriptive studies are studies that describe and summarize the characteristics and features of 2FA systems and methods, such as their definition, history, motivation, benefits, challenges, methods, technologies, applications, and examples. Descriptive studies can provide an overview and background of 2FA, as well as identify the current state and trends of 2FA. Descriptive studies can use secondary data sources, such as literature reviews, meta-analyses, or systematic reviews, to collect and analyze the existing research and knowledge on 2FA. For example, What is Two-Factor Authentication and Why You Should Use It is a descriptive study that provides a brief introduction to the concept and benefits of 2FA, as well as some common methods and technologies of 2FA.

Experimental studies are studies that test and evaluate the performance, usability, and user satisfaction of 2FA systems and methods, as well as compare and contrast different 2FA systems and methods. Experimental studies can provide empirical and objective results that can measure and demonstrate the effectiveness and efficiency of 2FA, as well as the trade-off and balance between the security and usability of 2FA. Experimental studies can use primary data sources, such as surveys, questionnaires, interviews, focus groups, observations, recordings, logs, tests, or case studies, to collect and analyze the data from the users or participants of 2FA. For example, A Usability Study of Five Two-Factor Authentication Methods is an experimental study that conducted a two-week, between-subjects usability study of five common 2FA methods with 72 participants, collecting both quantitative and qualitative data, as well as a within-subjects laboratory study with 30 participants to assess the general usability of the setup procedure for the five methods.

Exploratory studies are studies that investigate and discover the human factors and user acceptance of 2FA systems and methods, such as their perception, attitude, preference, motivation, emotion, trust, and behavior. Exploratory studies can provide rich and detailed results that can capture the user’s perspective and experience of 2FA, as well as the factors and barriers that influence the user’s intention and adoption of 2FA. Exploratory studies can use mixed data sources, such as security usability frameworks, user acceptance models, or user experience models, to collect and analyze the data from the users or participants of 2FA.

## Gaps and Limitations of the Previous Studies on Two Factor Authentication

The gaps and limitations of the previous studies on two factor authentication (2FA) are the shortcomings and challenges that can be identified and addressed in the future research and practice of 2FA. The gaps and limitations of the previous studies on 2FA can be categorized into four types: technical, methodological, theoretical, and practical.

Technical gaps and limitations are the issues and problems that arise from the design and implementation of 2FA systems and methods, such as their security, reliability, compatibility, interoperability, scalability, and cost. Technical gaps and limitations can affect the functionality and quality of 2FA, as well as the user’s experience and satisfaction with 2FA. Technical gaps and limitations can be caused by the complexity and diversity of 2FA systems and methods, as well as the dynamic and evolving nature of security threats and attacks. Technical gaps and limitations can be addressed by improving and optimizing the 2FA systems and methods, as well as adopting and integrating the latest and emerging technologies and standards. For example, [A Survey on Two-Factor Authentication Schemes] is a technical study that identifies and analyzes the security, usability, and performance of various 2FA schemes, as well as proposes some improvement and optimization techniques for 2FA.

Methodological gaps and limitations are the issues and problems that arise from the research design and procedure of the previous studies on 2FA, such as their validity, reliability, generalizability, and replicability. Methodological gaps and limitations can affect the results and conclusions of the previous studies on 2FA, as well as the comparison and analysis of different 2FA systems and methods. Methodological gaps and limitations can be caused by the lack and inconsistency of the evaluation criteria and methods for 2FA, as well as the bias and error of the data collection and analysis for 2FA. Methodological gaps and limitations can be addressed by developing and applying more rigorous and comprehensive evaluation criteria and methods for 2FA, as well as ensuring and enhancing the quality and accuracy of the data collection and analysis for 2FA. For example, [A Systematic Review of Usability and Security Evaluation Methods for Two-Factor Authentication] is a methodological study that reviews and evaluates the usability and security evaluation methods for 2FA, as well as suggests some guidelines and recommendations for conducting and reporting 2FA evaluations.

Theoretical gaps and limitations are the issues and problems that arise from the conceptual and analytical framework of the previous studies on 2FA, such as their relevance, coherence, completeness, and applicability. Theoretical gaps and limitations can affect the understanding and explanation of the 2FA systems and methods, as well as the human factors and user acceptance of 2FA. Theoretical gaps and limitations can be caused by the lack and inconsistency of the theoretical models and concepts for 2FA, as well as the ambiguity and complexity of the 2FA systems and methods. Theoretical gaps and limitations can be addressed by developing and applying more relevant and coherent theoretical models and concepts for 2FA, as well as clarifying and simplifying the 2FA systems and methods. For example, [A Conceptual Framework for Two-Factor Authentication] is a theoretical study that proposes and applies a conceptual framework for 2FA, based on the authentication factors, the CIA triad, the usability-security trade-off, and the human factors.

Practical gaps and limitations are the issues and problems that arise from the application and implementation of 2FA systems and methods in the real-world scenarios and contexts, such as their adoption, diffusion, impact, and value. Practical gaps and limitations can affect the effectiveness and efficiency of 2FA, as well as the user’s behavior and satisfaction of 2FA. Practical gaps and limitations can be caused by the gap and mismatch between the 2FA systems and methods and the user’s needs and expectations, as well as the barriers and challenges of the 2FA systems and methods in the real-world scenarios and contexts. Practical gaps and limitations can be addressed by exploring and discovering the user’s needs and expectations of 2FA, as well as overcoming and solving the barriers and challenges of the 2FA systems and methods in real-world scenarios and contexts. For example, [Understanding User Adoption of Two-Factor Authentication in Online Banking] is a practical study that investigates and explains the user adoption of 2FA in online banking, based on the user acceptance model, the technology acceptance model, and the theory of planned behavior.

## Summary and Implications of the Previous Studies on Two Factor Authentication

The summary and implications of the previous studies on two factor authentication (2FA) are the main findings and insights that can be derived and applied from the previous studies on 2FA. The summary and implications of the previous studies on 2FA can be organized into four themes: security, usability, user satisfaction, and user acceptance.

Security: The previous studies on 2FA have shown that 2FA can enhance the security of information and systems by preventing unauthorized access and modification, as well as providing an audit trail of authentication events. However, 2FA is not a panacea and it still faces various security threats and attacks, such as phishing, social engineering, SIM card duplication, software token generation, and hardware token accessibility. Therefore, 2FA needs to be designed and implemented with security in mind, as well as updated and monitored regularly to cope with the dynamic and evolving nature of security threats and attacks.

Usability: The previous studies on 2FA have shown that 2FA can affect the usability of information and systems by increasing the user’s cognitive load and frustration, as well as decreasing the user’s performance and efficiency. However, 2FA can also balance the usability-security trade-off by providing a reasonable level of security without compromising the user’s experience and satisfaction. Therefore, 2FA needs to be designed and implemented with usability in mind, as well as evaluated and tested rigorously to measure and demonstrate the usability level and efficiency of 2FA.

User satisfaction: The previous studies on 2FA have shown that 2FA can influence the user satisfaction of information and systems by affecting the user’s perception, attitude, preference, motivation, emotion, trust, and convenience. However, 2FA can also enhance user satisfaction of information and systems by providing the user with a sense of security, confidence, and control. Therefore, 2FA needs to be designed and implemented with user satisfaction in mind, as well as collected and analyzed feedback from the user to capture and improve the user satisfaction of 2FA.

User acceptance: The previous studies on 2FA have shown that 2FA can determine the user acceptance and adoption of information and systems by affecting the user’s intention and behavior to use 2FA. However, 2FA can also increase the user acceptance and adoption of information and systems by providing the user with perceived usefulness, perceived ease of use, perceived security, and perceived trust. Therefore, 2FA needs to be designed and implemented with user acceptance in mind, as well as investigated and explained the factors and barriers that influence the user acceptance and adoption of 2FA.

## Synthesis and Analysis of Two Factor Authentication

The synthesis and analysis of two factor authentication (2FA) are the processes and techniques that can be used to integrate and evaluate the main findings and insights of the previous studies on 2FA, as well as to identify and address the research gaps and directions for the future research and practice of 2FA. The synthesis and analysis of 2FA can be based on the following criteria and methods:

1. Criteria: The criteria are the aspects and features that can be used to synthesize and analyze different 2FA systems and methods, as well as to compare different 2FA systems and methods. The criteria can be derived from the evaluation criteria and methods for 2FA, such as security, usability, user satisfaction, user behavior, perceived usefulness, perceived ease of use, perceived security, and perceived trust. The criteria can also be specific to the domain and context of 2FA, such as cost, scalability, compatibility, interoperability, and compliance.
2. Methods: The methods are the approaches and techniques that can be used to conduct and perform the synthesis and analysis of different 2FA systems and methods. The methods can be classified into two types: analytical and empirical. Analytical methods are based on logical and mathematical reasoning and modeling. They can provide theoretical and formal results that can be verified and validated. Analytical methods for 2FA include security analysis, usability analysis, user satisfaction analysis, user behavior analysis, user acceptance analysis, and cost-benefit analysis. Empirical methods are based on experimental and observational data and testing. They can provide practical and realistic results that can be measured and evaluated. Empirical methods for 2FA include security testing, usability testing, user satisfaction testing, user behavior testing, user acceptance testing, and case study.

The synthesis and analysis of 2FA can be organized into four themes: security, usability, user satisfaction, and user acceptance.

Security: The synthesis and analysis of the security of 2FA can be based on the security metrics, such as the false acceptance rate (FAR), the false rejection rate (FRR), the entropy, the resilience, and the cost. The security of 2FA can be synthesized and analyzed by comparing and contrasting the security metrics of different 2FA systems and methods, as well as by testing and evaluating the security metrics of the 2FA system and method of the project. The security of 2FA can be improved and optimized by applying and integrating the latest and emerging technologies and standards, such as biometrics, QR code, and push notification, as well as by updating and monitoring the 2FA system and method regularly to cope with the dynamic and evolving nature of the security threats and attacks.

Usability: The synthesis and analysis of the usability of 2FA can be based on the usability metrics, such as the time, the error rate, the success rate, the learnability, and the memorability. The usability of 2FA can be synthesized and analyzed by comparing and contrasting the usability metrics of different 2FA systems and methods, as well as by testing and evaluating the usability metrics of the 2FA system and method of the project. The usability of 2FA can be balanced and enhanced by designing and implementing the 2FA system and method with usability in mind, as well as by evaluating and testing the 2FA system and method rigorously to measure and demonstrate the usability level and efficiency of 2FA.

User satisfaction: The synthesis and analysis of the user satisfaction of 2FA can be based on the user satisfaction metrics, such as the satisfaction, the confidence, the trust, the convenience, and the preference. The user satisfaction of 2FA can be synthesized and analyzed by comparing and contrasting the user satisfaction metrics of different 2FA systems and methods, as well as by collecting and analyzing feedback from the users or participants of the 2FA system and method of the project. The user satisfaction of 2FA can be improved and increased by designing and implementing the 2FA system and method with user satisfaction in mind, as well as by collecting and analyzing feedback from the users to capture and enhance the user satisfaction of 2FA.

User acceptance: The synthesis and analysis of the user acceptance of 2FA can be based on the user acceptance model, such as the technology acceptance model, the theory of planned behavior, or the unified theory of acceptance and use of technology. The user acceptance of 2FA can be synthesized and analyzed by investigating and explaining the factors and barriers that influence the user’s intention and behavior to use 2FA, as well as by conducting and performing user acceptance testing of the 2FA system and method of the project. The user acceptance of 2FA can be increased and promoted by designing and implementing the 2FA system and method with user acceptance in mind, as well as by investigating and explaining the factors and barriers that influence the user acceptance of 2FA.

Conclusion and Recommendations of the Synthesis and Analysis

Summary: The summary is the recap and synthesis of the main points and themes of the synthesis and analysis of 2FA, such as the security, usability, user satisfaction, and user acceptance of 2FA, as well as the factors and barriers that influence the design, implementation, and evaluation of 2FA. The summary can provide a clear and concise overview and background of 2FA, as well as highlighting the current state and trends of 2FA.

Implications: The implications are the interpretation and application of the main findings and insights of the synthesis and analysis of 2FA, such as the strengths and weaknesses of 2FA, as well as the trade-off and balance between the security and usability of 2FA. The implications can provide a deeper and broader understanding and explanation of 2FA, as well as identify the challenges and opportunities of 2FA.

Recommendations: The recommendations are the identification and suggestion of the research gaps and directions for the future research and practice of 2FA, such as the technical, methodological, theoretical, and practical gaps and limitations of the previous studies on 2FA, as well as the improvement and optimization techniques and strategies for 2FA. The recommendations can provide critical and constructive feedback and guidance for 2FA, as well as propose and justify the research questions and objectives of the project.

## Gaps in the Literature on Two Factor Authentication

The gaps in the literature on two factor authentication (2FA) are the areas and topics that have not been adequately addressed or explored by the previous studies on 2FA. The gaps in the literature on 2FA can be identified and categorized into four types: technical, methodological, theoretical, and practical.

Technical gaps are the gaps that relate to the design and implementation of 2FA systems and methods, such as their security, reliability, compatibility, interoperability, scalability, and cost. Technical gaps can be identified by reviewing and analyzing the security metrics, such as the false acceptance rate (FAR), the false rejection rate (FRR), the entropy, the resilience, and the cost, of different 2FA systems and methods, as well as by testing and evaluating the security metrics of the 2FA system and method of the project. Technical gaps can also be identified by reviewing and analyzing the latest and emerging technologies and standards for 2FA, such as biometrics, QR code, and push notification, as well as by applying and integrating the latest and emerging technologies and standards for 2FA. Some examples of technical gaps in the literature on 2FA are:

1. The lack of a comprehensive and systematic security analysis and evaluation of different 2FA systems and methods, especially for the newer and emerging technologies and standards, such as biometrics, QR code, and push notification.
2. The lack of a comparative and empirical study of the security, usability, and user satisfaction of different 2FA systems and methods, especially for the newer and emerging technologies and standards, such as biometrics, QR code, and push notification.
3. The lack of a robust and reliable 2FA system and method that can cope with the dynamic and evolving nature of the security threats and attacks, such as phishing, social engineering, SIM card duplication, software token generation, and hardware token accessibility.
4. The lack of a compatible and interoperable 2FA system and method that can work with different platforms, devices, and services, such as web, mobile, desktop, and cloud.
5. The lack of a scalable and cost-effective 2FA system and method that can support many users and transactions, as well as minimize the resources and efforts required to implement and maintain 2FA.

Methodological gaps are the gaps that relate to the research design and procedure of the previous studies on 2FA, such as their validity, reliability, generalizability, and replicability. Methodological gaps can be identified by reviewing and evaluating the evaluation criteria and methods for 2FA, such as security metrics, usability metrics, user satisfaction metrics, user behavior metrics, perceived usefulness, perceived ease of use, perceived security, and perceived trust, of different 2FA systems and methods, as well as by conducting and performing the evaluation criteria and methods for 2FA. Methodological gaps can also be identified by reviewing and evaluating the research methodologies for 2FA of the previous studies on 2FA, as well as by applying and reporting the research methodologies for 2FA.

Some examples of methodological gaps in the literature on 2FA are:

1. The lack of a rigorous and comprehensive evaluation criteria and methods for 2FA, especially for the newer and emerging technologies and standards, such as biometrics, QR code, and push notification, as well as for the human factors and user acceptance of 2FA, such as perception, attitude, preference, motivation, emotion, trust, and behavior.
2. The lack of a consistent and standardized evaluation criteria and methods for 2FA, especially for the security and usability metrics, such as the false acceptance rate (FAR), the false rejection rate (FRR), the entropy, the resilience, the cost, the time, the error rate, the success rate, the learnability, and the memorability, of different 2FA systems and methods, as well as for the user satisfaction and user acceptance metrics, such as the satisfaction, the confidence, the trust, the convenience, and the preference, of different 2FA systems and methods.
3. The lack of a valid and reliable data collection and analysis for 2FA, especially for the qualitative and mixed data sources, such as user feedback, user observation, user testing, security usability frameworks, user acceptance models, or user experience models, of different 2FA systems and methods, as well as for the user’s perspective and experience of 2FA.
4. The lack of a generalizable and replicable research results and conclusions for 2FA, especially for the empirical and observational data sources, such as surveys, questionnaires, interviews, focus groups, observations, recordings, logs, tests, or case studies, of different 2FA systems and methods, as well as for the real-world scenarios and contexts of 2FA.

Theoretical gaps are the gaps that relate to the conceptual and analytical framework of the previous studies on 2FA, such as their relevance, coherence, completeness, and applicability. Theoretical gaps can be identified by reviewing and analyzing the theoretical models and concepts for 2FA, such as the authentication factors, the CIA triad, the usability-security trade-off, and the human factors, of different 2FA systems and methods, as well as by developing and applying the theoretical models and concepts for 2FA. Theoretical gaps can also be identified by reviewing and analyzing the latest and emerging research and knowledge on 2FA, such as the user’s perception, attitude, preference, motivation, emotion, trust, and behavior, as well as by exploring and discovering the user’s perspective and experience of 2FA. Some examples of theoretical gaps in the literature on 2FA are:

1. The lack of a relevant and coherent theoretical framework for 2FA, especially for the newer and emerging technologies and standards, such as biometrics, QR code, and push notification, as well as for the human factors and user acceptance of 2FA, such as perception, attitude, preference, motivation, emotion, trust, and behavior.
2. The lack of a complete and comprehensive theoretical framework for 2FA, especially for the integration and interaction of the different authentication factors, such as knowledge, possession, inherence, and location, as well as for the trade-off and balance between the different aspects of 2FA, such as security, usability, user satisfaction, and user acceptance.
3. The lack of an applicable and adaptable theoretical framework for 2FA, especially for the real-world scenarios and contexts of 2FA, such as online banking, e-commerce, e-government, and e-health, as well as for the different types and levels of users, such as novice, expert, individual, and group.

Practical gaps are the gaps that relate to the application and implementation of 2FA systems and methods in the real-world scenarios and contexts, such as their adoption, diffusion, impact, and value. Practical gaps can be identified by reviewing and evaluating the applications and examples of 2FA systems and methods in various domains, such as online banking, e-commerce, e-government, and e-health, as well as by designing and implementing the 2FA system and method of the project. Practical gaps can also be identified by reviewing and evaluating the user’s needs and expectations of 2FA, as well as by exploring and discovering the user’s behavior and satisfaction of 2FA. Some examples of practical gaps in the literature on 2FA are:

1. The lack of a user-centric and user-friendly 2FA system and method that can meet the user’s needs and expectations of 2FA, such as security, usability, user satisfaction, and user acceptance, as well as provide the user with a sense of security, confidence, and control.
2. The lack of a domain-specific and context-aware 2FA system and method that can suit the different scenarios and contexts of 2FA, such as online banking, e-commerce, e-government, and e-health, as well as comply with the regulatory and industry standards, such as the PCI DSS, the HIPAA, and the GDPR.
3. The lack of an effective and efficient 2FA system and method that can demonstrate the impact and value of 2FA, such as the reduction of fraud and identity theft, the increase of customer loyalty and retention, and the improvement of service quality and productivity.

## Recommendations of the Literature Review

Summary: The summary is the recap and synthesis of the main points and themes of the literature review, such as the definition, history, motivation, benefits, challenges, methods, technologies, applications, examples, evaluation criteria and methods, comparison and analysis, methodologies, and synthesis and analysis of 2FA. The summary can provide a clear and concise overview and background of 2FA, as well as highlighting the current state and trends of 2FA.

Implications: The implications are the interpretation and application of the main findings and insights of the previous studies on 2FA, such as the security, usability, user satisfaction, and user acceptance of 2FA, as well as the factors and barriers that influence the design, implementation, and evaluation of 2FA. The implications can provide a deeper and broader understanding and explanation of 2FA, as well as identify the strengths and weaknesses of 2FA.

Recommendations: The recommendations are the identification and suggestion of the research gaps and directions for the future research and practice of 2FA, such as the technical, methodological, theoretical, and practical gaps and limitations of the previous studies on 2FA, as well as the improvement and optimization techniques and strategies for 2FA.

## Conclusion of the Literature Review

The conclusion of the literature review is the final and comprehensive summary and synthesis of the main findings and insights of the previous studies on 2FA, as well as the identification and suggestion of the research gaps and directions for the future research and practice of 2FA. The conclusion of the literature review can be organized into four parts: summary, implications, recommendations, and research questions and objectives.

Summary: The summary is the recap and synthesis of the main points and themes of the literature review, such as the definition, history, motivation, benefits, challenges, methods, technologies, applications, examples, evaluation criteria and methods, comparison and analysis, methodologies, synthesis and analysis, and gaps in the literature of 2FA. The summary can provide a clear and concise overview and background of 2FA, as well as highlight the current state and trends of 2FA. The summary can also provide a logical and coherent structure and flow of the literature review, as well as link and connect the different sections and subsections of the literature review.

Implications: The implications are the interpretation and application of the main findings and insights of the previous studies on 2FA, such as the security, usability, user satisfaction, and user acceptance of 2FA, as well as the factors and barriers that influence the design, implementation, and evaluation of 2FA. The implications can provide a deeper and broader understanding and explanation of 2FA, as well as identify the strengths and weaknesses of 2FA. The implications can also provide a critical and constructive feedback and guidance for 2FA, as well as justify and support the research questions and objectives of the project.

Recommendations: The recommendations are the identification and suggestion of the research gaps and directions for the future research and practice of 2FA, such as the technical, methodological, theoretical, and practical gaps and limitations of the previous studies on 2FA, as well as the improvement and optimization techniques and strategies for 2FA. The recommendations can provide a comprehensive and systematic overview and assessment of 2FA, as well as propose and justify the research questions and objectives of the project. The recommendations can also provide a clear and concise outline and plan of the project, as well as describe and explain the expected outcomes and contributions of the project.

Research questions and objectives: The research questions and objectives are the specific and focused questions and goals that guide and direct the project on 2FA. The research questions and objectives can be derived and refined from the research gaps and directions for the future research and practice of 2FA, as well as from the implications and recommendations of the literature review. The research questions and objectives can also be aligned and consistent with the research methodology and design of the project, as well as with the evaluation criteria and methods of the project. The research questions and objectives can be stated and formulated clearly and concisely, as well as be relevant and feasible for the project.

METHODOLOY

# Introduction to Methodology

The introduction to methodology chapter provides a rationale and overview of the research design and procedure of the project on 2FA. The chapter covers the following topics:

1. The research paradigm and approach of the project
2. The research questions and objectives of the project
3. The research methods and techniques of the project
4. The data sources and collection methods of the project
5. The data analysis and interpretation methods of the project
6. The ethical considerations and limitations of the project

## Research Paradigm and Approach

The research paradigm and approach of the project are the philosophical and theoretical assumptions and perspectives that guide and direct the project. The research paradigm and approach of the project are:

1. Pragmatism: The research paradigm of the project is pragmatism, which is a philosophical perspective that focuses on the practical and useful outcomes and consequences of the research, rather than the absolute and universal truths and realities of the research. Pragmatism allows the researcher to use multiple and mixed methods and techniques, as well as multiple and mixed data sources and types, to address the research questions and objectives of the project, as well as to adapt and adjust the research design and procedure according to the research context and situation.
2. Mixed methods: The research approach of the project is mixed methods, which is a research strategy that combines and integrates both quantitative and qualitative methods and techniques, as well as both quantitative and qualitative data sources and types, to conduct and perform the research. Mixed methods can provide comprehensive and holistic results and insights that can measure and demonstrate the performance, usability, and user satisfaction of 2FA, as well as capture and explain the human factors and user acceptance of 2FA. Mixed methods can also provide triangulation and validation of the results and insights, as well as address the gaps and limitations of the previous studies on 2FA.

## Research Questions and Objectives

The research questions and objectives of the project are the specific and focused questions and goals that guide and direct the project on 2FA. The research questions and objectives of the project are derived and refined from the research gaps and directions for the future research and practice of 2FA, as well as from the implications and recommendations of the literature review. The research questions and objectives of the project are also aligned and consistent with the research paradigm and approach of the project, as well as with the evaluation criteria and methods of the project. The research questions and objectives of the project are stated and formulated clearly and concisely, as well as relevant and feasible for the project.

The main research question of the project is:

1. How to design and implement a 2FA system that is secure, reliable, and user-friendly using the following technologies: Java program, Postgres database, Flutter mobile app, and React JS frontend?

The sub-research questions of the project are:

1. How to evaluate the performance, usability, and user satisfaction of the 2FA system using quantitative and qualitative methods and techniques?
2. How to compare the 2FA system with other existing 2FA systems and methods using security, usability, user satisfaction, and user acceptance metrics?
3. How to investigate and explain the human factors and user acceptance of the 2FA system using mixed methods and techniques?

The main research objective of the project is:

1. To design and implement a prototype of a 2FA system that uses the following technologies: Java program, Postgres database, Flutter mobile app, and React JS frontend, and to demonstrate the functionality and features of 2FA.

The sub-research objectives of the project are:

1. To evaluate the performance, usability, and user satisfaction of the 2FA system using quantitative and qualitative methods and techniques, and to measure and demonstrate the effectiveness and efficiency of 2FA.
2. To compare the 2FA system with other existing 2FA systems and methods using security, usability, user satisfaction, and user acceptance metrics, and to identify and analyze the strengths and weaknesses of 2FA.
3. To investigate and explain the human factors and user acceptance of the 2FA system using mixed methods and techniques, and to predict and explain the intention and behavior of the user to use 2FA

## Research Methods and Techniques

The research methods and techniques of the project are specific and focused methods and techniques that can be used to conduct and perform the research design and procedure of the project on 2FA. The research methods and techniques of the project are derived and refined from the research paradigm and approach of the project, as well as from the research questions and objectives of the project. The research methods and techniques of the project are also aligned and consistent with the data sources and collection methods of the project, as well as with the data analysis and interpretation methods of the project. The research methods and techniques of the project are stated and formulated clearly and concisely, as well as relevant and feasible for the project.

The main research method of the project is:

1. Mixed methods: The research method of the project is mixed methods, which is a research strategy that combines and integrates both quantitative and qualitative methods and techniques, as well as both quantitative and qualitative data sources and types, to conduct and perform the research. Mixed methods can provide comprehensive and holistic results and insights that can measure and demonstrate the performance, usability, and user satisfaction of 2FA, as well as capture and explain the human factors and user acceptance of 2FA. Mixed methods can also provide triangulation and validation of the results and insights, as well as address the gaps and limitations of the previous studies on 2FA.

The sub-research methods of the project are:

1. Quantitative methods: The quantitative methods are the methods and techniques that can be used to collect and analyze numerical data and statistical analysis. Quantitative methods can provide objective and reliable results that can be generalized and replicated. Quantitative methods for 2FA include security testing, usability testing, user satisfaction testing, and user acceptance testing.
2. Qualitative methods: The qualitative methods are the methods and techniques that can be used to collect and analyze textual data and thematic analysis. Qualitative methods can provide rich and detailed results that can capture the user’s perspective and experience. Qualitative methods for 2FA include user feedback, user observation, user testing, and case study.

## Data Sources and Collection Methods

The data sources and collection methods of the project are the specific and focused sources and methods that can be used to obtain and gather the data for the project on 2FA. The data sources and collection methods of the project are derived and refined from the research paradigm and approach of the project, as well as from the research questions and objectives of the project. The data sources and collection methods of the project are also aligned and consistent with the research methods and techniques of the project, as well as with the data analysis and interpretation methods of the project. The data sources and collection methods of the project are stated and formulated clearly and concisely, as well as relevant and feasible for the project.

The main data source of the project is:

1. Primary data: The data source of the project is primary data, which is the data that is collected and gathered by the researcher directly from the users or participants of the 2FA system and method of the project. Primary data can provide original and authentic data that can address the research questions and objectives of the project, as well as reflect the user’s perspective and experience of 2FA.

The sub-data sources of the project are:

1. Quantitative data: The quantitative data is the data that is collected and gathered by the researcher using quantitative methods and techniques, such as security testing, usability testing, user satisfaction testing, and user acceptance testing. Quantitative data can provide numerical and statistical data that can measure and demonstrate the performance, usability, and user satisfaction of 2FA, as well as the user acceptance of 2FA.
2. Qualitative data: The qualitative data is the data that is collected and gathered by the researcher using qualitative methods and techniques, such as user feedback, user observation, user testing, and case study. Qualitative data can provide textual and thematic data that can capture and explain the human factors and user acceptance of 2FA, as well as the user’s perspective and experience of 2FA.

The main data collection method of the project is:

1. Mixed methods: The data collection method of the project is mixed methods, which is a data collection strategy that combines and integrates both quantitative and qualitative data sources and types, as well as both quantitative and qualitative data collection methods and techniques, to obtain and gather the data for the project. Mixed methods can provide comprehensive and holistic data that can measure and demonstrate the performance, usability, and user satisfaction of 2FA, as well as capture and explain the human factors and user acceptance of 2FA.

The sub-data collection methods of the project are:

1. Quantitative data collection methods: The quantitative data collection methods are the methods and techniques that can be used to obtain and gather numerical and statistical data from the users or participants of the 2FA system and method of the project. Quantitative data collection methods for 2FA include security testing, usability testing, user satisfaction testing, and user acceptance testing. Security testing is the method and technique that can be used to obtain and gather the security metrics, such as the false acceptance rate (FAR), the false rejection rate (FRR), the entropy, the resilience, and the cost, of the 2FA system and method of the project. Usability testing is the method and technique that can be used to obtain and gather the usability metrics, such as the time, the error rate, the success rate, the learnability, and the memorability of the 2FA system and method of the project. User satisfaction testing is the method and technique that can be used to obtain and gather the user satisfaction metrics, such as the satisfaction, the confidence, the trust, the convenience, and the preference, of the 2FA system and method of the project. User acceptance testing is the method and technique that can be used to obtain and gather the user acceptance metrics, such as the perceived usefulness, perceived ease of use, perceived security, and perceived trust, of the 2FA system and method of the project.
2. Qualitative data collection methods: The qualitative data collection methods are the methods and techniques that can be used to obtain and gather textual and thematic data from the users or participants of the 2FA system and method of the project. Qualitative data collection methods for 2FA include user feedback, user observation, user testing, and case study. User feedback is the method and technique that can be used to obtain and gather the information and opinion that the user provides about the 2FA system and method of the project. User feedback can be collected through interviews, surveys, questionnaires, focus groups, or reviews. User observation is the method and technique that can be used to obtain and gather the action and behavior that the user exhibits when using the 2FA system and method of the project. User observation can be conducted through direct observation, video recording, eye tracking, or log analysis. User testing is the method and technique that can be used to obtain and gather the process and outcome that the user achieves when using the 2FA system and method of the project. User testing can be performed through usability testing, user acceptance testing, or user experience testing. Case study is the method and technique that can be used to obtain and gather the in-depth and detailed data from a specific and representative case or example of the 2FA system and method of the project. Case study can be performed through document analysis, interview, observation, or test.

## Data Analysis and Interpretation Methods

The data analysis and interpretation methods of the project are the specific and focused methods and techniques that can be used to process and understand the data for the project on 2FA. The data analysis and interpretation methods of the project are derived and refined from the research paradigm and approach of the project, as well as from the research questions and objectives of the project. The data analysis and interpretation methods of the project are also aligned and consistent with the research methods and techniques of the project, as well as with the data sources and collection methods of the project. The data analysis and interpretation methods of the project are stated and formulated clearly and concisely, as well as relevant and feasible for the project.

The main data analysis and interpretation method of the project is:

1. Mixed methods: The data analysis and interpretation method of the project is mixed methods, which is a data analysis and interpretation strategy that combines and integrates both quantitative and qualitative data analysis and interpretation methods and techniques, as well as both quantitative and qualitative data sources and types, to process and understand the data for the project. Mixed methods can provide comprehensive and holistic results and insights that can measure and demonstrate the performance, usability, and user satisfaction of 2FA, as well as capture and explain the human factors and user acceptance of 2FA. Mixed methods can also provide triangulation and validation of the results and insights, as well as address the gaps and limitations of the previous studies on 2FA.

The sub-data analysis and interpretation methods of the project are:

1. Quantitative data analysis and interpretation methods: The quantitative data analysis and interpretation methods are the methods and techniques that can be used to process and understand numerical and statistical data from the users or participants of the 2FA system and method of the project. Quantitative data analysis and interpretation methods for 2FA include descriptive statistics, inferential statistics, and graphical representation. Descriptive statistics are the methods and techniques that can be used to summarize and describe the basic features and characteristics of the quantitative data, such as the mean, median, mode, standard deviation, range, frequency, and percentage. Inferential statistics are the methods and techniques that can be used to test and infer the hypotheses and relationships of the quantitative data, such as the t-test, ANOVA, chi-square, correlation, and regression. Graphical representation are the methods and techniques that can be used to visualize and present the quantitative data, such as the bar chart, pie chart, line chart, histogram, scatter plot, and box plot.
2. Qualitative data analysis and interpretation methods: The qualitative data analysis and interpretation methods are the methods and techniques that can be used to process and understand textual and thematic data from the users or participants of the 2FA system and method of the project. Qualitative data analysis and interpretation methods for 2FA include coding, categorizing, and theming. Coding is the method and technique that can be used to label and organize qualitative data into meaningful and manageable units, such as words, phrases, sentences, or paragraphs. Categorizing is the method and technique that can be used to group and classify the codes into broader and higher-level categories, such as concepts, constructs, or variables. Theming is the method and technique that can be used to identify and extract the main and recurring themes and patterns from the categories, such as topics, issues, or arguments.

## Ethical Considerations and Limitations of the Project

The ethical considerations and limitations of the project are the ethical issues and challenges that arise from the research design and procedure of the project on 2FA, as well as the potential risks and biases that affect the validity and reliability of the project. The ethical considerations and limitations of the project are derived and refined from the research paradigm and approach of the project, as well as from the research questions and objectives of the project. The ethical considerations and limitations of the project are also aligned and consistent with the research methods and techniques of the project, as well as with the data sources and collection methods of the project. The ethical considerations and limitations of the project are stated and formulated clearly and concisely, as well as relevant and feasible for the project.

The main ethical consideration of the project is:

1. Informed consent: The ethical consideration of the project is informed consent, which is the process and outcome of obtaining and ensuring the voluntary and informed agreement of the users or participants of the 2FA system and method of the project to take part in the research. Informed consent can protect the rights and interests of the users or participants, as well as respect their autonomy and dignity. Informed consent can also ensure the transparency and accountability of the research, as well as complying with the ethical and legal standards of the research.

The sub-ethical considerations of the project are:

1. Privacy and confidentiality: The privacy and confidentiality are the ethical considerations that relate to the protection and preservation of the personal and sensitive information and data of the users or participants of the 2FA system and method of the project. Privacy and confidentiality can prevent the unauthorized access and disclosure of the information and data, as well as safeguard the identity and anonymity of the users or participants. Privacy and confidentiality can also enhance the trust and confidence of the users or participants, as well as comply with the ethical and legal standards of the research.
2. Security and integrity: Security and integrity are the ethical considerations that relate to the protection and preservation of the quality and accuracy of the information and data of the 2FA system and method of the project. Security and integrity can prevent the unauthorized modification and manipulation of the information and data, as well as ensure the validity and reliability of the information and data. Security and integrity can also enhance the credibility and reputation of the research, as well as comply with the ethical and legal standards of the research.

The main limitation of the project is:

1. Generalizability: The limitation of the project is generalizability, which is the extent and degree to which the results and insights of the project can be applied and transferred to other 2FA systems and methods, as well as to other domains and contexts of 2FA. Generalizability can affect the usefulness and value of the project, as well as the comparison and analysis of different 2FA systems and methods. Generalizability can also be influenced by the sample size and selection of the users or participants of the 2FA system and method of the project, as well as by the research design and procedure of the project.

The sub-limitations of the project are:

1. Validity: The validity is the limitation that relates to the extent and degree to which the project measures and demonstrates what it intends to measure and demonstrate, such as the performance, usability, and user satisfaction of 2FA, as well as the human factors and user acceptance of 2FA. Validity can affect the quality and accuracy of the project, as well as the interpretation and application of the results and insights of the project. Validity can also be influenced by the research methods and techniques of the project, as well as by the data sources and collection methods of the project.
2. Reliability: The reliability is the limitation that relates to the extent and degree to which the project can be repeated and replicated with consistent and stable results and insights, such as the performance, usability, and user satisfaction of 2FA, as well as the human factors and user acceptance of 2FA. Reliability can affect the objectivity and reliability of the project, as well as the verification and validation of the results and insights of the project. Reliability can also be influenced by the research methods and techniques of the project, as well as by the data analysis and interpretation methods of the project.

# Research Design

The research design of the final project is the plan and structure of the research process and procedure of the final project on 2FA. The research design of the final project covers the following topics:

1. The research type and strategy of the final project
2. The research population and sample of the final project
3. The research variables and hypotheses of the final project
4. The research instruments and materials of the final project
5. The research procedure and timeline of the final project

## Research Type and Strategy

The research type and strategy of the final project are the classification and description of the nature and purpose of the final project. The research type and strategy of the final project are:

1. Applied research: The research type of the final project is applied research, which is a type of research that aims to solve a specific and practical problem or issue, rather than to generate new knowledge or theory. Applied research can provide useful and valuable outcomes and contributions that can benefit society and industry. Applied research for 2FA can provide a prototype of a 2FA system that is secure, reliable, and user-friendly, as well as demonstrate the impact and value of 2FA for online security and privacy.
2. Exploratory research: The research strategy of the final project is exploratory research, which is a strategy that aims to explore and discover a new or unknown phenomenon or topic, rather than to test and confirm a pre-existing hypothesis or theory. Exploratory research can provide novel and innovative results and insights that can fill the gaps and limitations of previous studies. Exploratory research for 2FA can explore and discover the human factors and user acceptance of 2FA, as well as the comparison and analysis of different 2FA systems and methods.

DATA COLLECTION

The data collection for the two-factor authentication project consists of four main methods: surveys, interviews, observations, and experiments. Each method has a different purpose, procedure, and data type, as explained below:

1. Surveys: The surveys are used to collect quantitative data on the user preferences and perceptions of different two-factor authentication methods for cloud computing. The surveys are designed using a web-based platform, such as Google Forms or SurveyMonkey, and consist of multiple-choice, Likert-scale, and open-ended questions. The surveys are distributed to the participants via email or social media, and the participants are asked to complete the surveys online within a specified time frame. The surveys are anonymous and confidential, and the participants are informed of the purpose, benefits, and risks of the project before taking the surveys.
2. Interviews: The interviews are used to collect qualitative data on the user experiences and feedback of using the proposed two-factor authentication framework for cloud computing. The interviews are conducted using a semi-structured format, which allows for flexibility and probing of the participants’ responses. The interviews are carried out using a video conferencing tool, such as Zoom or Skype, and last for about 30 minutes each. The interviews are recorded and transcribed, with the consent of the participants, and the participants are assured of the confidentiality and anonymity of their data.
3. Observations: The observations are used to collect quantitative and qualitative data on the user behavior and performance of using the proposed two-factor authentication framework for cloud computing. The observations are done using a user testing platform, such as UserTesting or UserZoom, which allows for recording and analyzing the user actions, interactions, and reactions during the authentication process. The observations are performed remotely, with the participants accessing the platform from their own devices, and last for about 15 minutes each. The observations are unobtrusive and non-intrusive, and the participants are informed of the purpose, benefits, and risks of the project before participating.
4. Experiments: The experiments are used to collect quantitative data on the security, usability, and user satisfaction of the proposed two-factor authentication framework for cloud computing and compare it with other methods. The experiments are designed using a randomized controlled trial (RCT) method, which assigns the participants to different groups based on the type of two-factor authentication method they use: the proposed framework, SMS, email, or hardware token. The experiments are conducted using a web-based application, which simulates the authentication process for cloud computing, and measures the relevant variables, such as the number and severity of security breaches and attacks, the time, effort, and errors involved in the authentication process, and the user ratings and feedback on the authentication experience. The experiments are administered to the participants via email or social media, and the participants are asked to complete the experiments online within a specified time frame..

DATA ANALYSIS

The data analysis for the two-factor authentication project consists of four main methods: descriptive statistics, inferential statistics, thematic analysis, and comparative analysis. Each method has a different purpose, procedure, and data type, as explained below:

1. Descriptive statistics: The descriptive statistics are used to summarize and present the quantitative data collected from the surveys, observations, and experiments, using measures of central tendency, dispersion, and distribution. The descriptive statistics are calculated using spreadsheet software, such as Microsoft Excel or Google Sheets, and displayed using charts, graphs, and tables. Descriptive statistics are used to describe the characteristics and patterns of the data, such as the mean, median, mode, standard deviation, range, frequency, and percentage.
2. Inferential statistics: The inferential statistics are used to test the hypotheses and draw conclusions from the quantitative data collected from the surveys, observations, and experiments, using statistical tests, such as t-tests, ANOVA, chi-square, and correlation. The inferential statistics are computed using statistical software, such as SPSS or R, and reported using p-values, confidence intervals, and effect sizes. Inferential statistics are used to infer the relationships and differences between the variables, such as the security, usability, and user satisfaction of the different two-factor authentication methods.
3. Thematic analysis: Thematic analysis is used to analyze and interpret the qualitative data collected from the interviews, using a six-step process, as proposed by Braun and Clarke. The thematic analysis is performed using qualitative data analysis software, such as NVivo or Atlas.ti, and involves the following steps: familiarization, coding, generating themes, reviewing themes, defining and naming themes, and writing the report. The thematic analysis is used to identify and describe the main themes and subthemes that emerge from the data, such as the user opinions, preferences, challenges, and suggestions regarding the two-factor authentication framework.
4. Comparative analysis: The comparative analysis is used to compare the quantitative and qualitative data collected from the different methods, using a mixed-methods approach, such as triangulation, complementarity, or integration. The comparative analysis is conducted using a combination of the tools and techniques mentioned above and aims to provide a holistic and comprehensive understanding of the research problem, as well as to validate and corroborate the findings from the different sources of data. The comparative analysis is used to answer the research questions and objectives, and to evaluate the proposed two-factor authentication framework in terms of its security, usability, and user satisfaction.

To ensure the validity and reliability of the data collected and analyzed in this project, I will use the following strategies:

1. Validity: Validity refers to the extent to which the data and the findings accurately reflect the reality and the research problem. To ensure the validity of the data, I will use the following strategies:
   1. Triangulation: Triangulation is the use of multiple sources, methods, and perspectives to cross-check and validate the data and the findings. In this project, I will use triangulation by collecting and comparing data from different methods (surveys, interviews, observations, and experiments), different sources (online platforms, social media, and personal contacts), and different perspectives (users, experts, and researchers).
   2. Member checking: Member checking is the process of soliciting feedback and confirmation from the participants on the data and the findings. In this project, I will use member checking by sharing the transcripts, codes, themes, and reports with the participants, and asking them to verify and comment on their accuracy and completeness.
   3. Peer review: Peer review is the process of seeking feedback and evaluation from other researchers or experts on the data and the findings. In this project, I will use peer review by submitting the data and the findings to my supervisor, colleagues, and reviewers, and incorporating their suggestions and criticisms into the final report.
2. Reliability: Reliability refers to the extent to which the data and the findings are consistent and reproducible. To ensure the reliability of the data, I will use the following strategies:
   1. Standardization: Standardization is the use of uniform and consistent procedures and protocols for data collection and analysis. In this project, I will use standardization by following the same steps and rules for designing, implementing, and evaluating the two-factor authentication framework, and by using the same tools and techniques for collecting and analyzing the data.
   2. Documentation: Documentation is the use of detailed and transparent records and reports of the data collection and analysis process. In this project, I will use documentation by keeping track of the data sources, methods, tools, codes, themes, and findings, and by providing clear and comprehensive explanations and justifications for each decision and action taken in the project.
   3. Replication: Replication is the use of repeated trials and tests to verify and confirm the data and the findings. In this project, I will use replication by conducting multiple rounds of data collection and analysis, and by comparing the results and outcomes of each round.

ETHICAL CONSIDERATIONS

The ethical considerations for the two-factor authentication system are the ethical issues and challenges that may arise from the design, implementation, and evaluation of the system, and how they can be addressed and resolved. Some of the ethical considerations for this project are:

1. Privacy: Privacy is the right of the participants to control their personal information and data, and to protect them from unauthorized access, use, or disclosure. In this project, privacy may be compromised by the collection, storage, and analysis of the participants’ data, such as their cloud account credentials, authentication methods, and user behavior and feedback. To ensure the privacy of the participants, I will use the following strategies:
   1. Informed consent: Informed consent is the process of obtaining the voluntary and informed agreement of the participants to participate in the project, and to inform them of the purpose, benefits, risks, and procedures of the project. In this project, I will use informed consent by providing the participants with a consent form that explains the project in detail and asks them to sign it before taking part in the project.
   2. Anonymity and confidentiality: Anonymity and confidentiality are the measures of protecting the identity and the data of the participants from being revealed or linked to them. In this project, I will use anonymity and confidentiality by assigning the participants with random codes or pseudonyms, and by encrypting and securing their data using passwords and firewalls.
   3. Data minimization and deletion: Data minimization and deletion are the principles of collecting and retaining only the necessary and relevant data for the project, and deleting or destroying them after the project is completed. In this project, I will use data minimization and deletion by collecting and storing only the data that are essential for answering the research questions and objectives, and by deleting or destroying them after the project is finalized and reported.
2. Security: Security is the protection of the system and the data from malicious attacks, such as hacking, phishing, or spoofing. In this project, security may be threatened by the exposure or exploitation of the system and the data by hackers or other unauthorized parties, who may attempt to access, modify, or steal them. To ensure the security of the system and the data, I will use the following strategies:
   1. Encryption and authentication: Encryption and authentication are the techniques of transforming and verifying the data and the system using secret keys or codes, to prevent unauthorized access or modification. In this project, I will use encryption and authentication by encrypting the data and the system using advanced algorithms, such as AES or RSA, and by authenticating the users and the system using the proposed two-factor authentication framework.
   2. Backup and recovery: Backup and recovery are the methods of creating and restoring copies of the data and the system, in case of loss or damage. In this project, I will use backup and recovery by creating and storing backups of the data and the system in a secure cloud storage, such as Google Drive or Dropbox, and by recovering them in case of any loss or damage.
   3. Testing and monitoring: Testing and monitoring are the processes of checking and observing the performance and the functionality of the system and the data, to detect and prevent any errors or attacks. In this project, I will use testing and monitoring by testing and debugging the system and the data before and after the deployment, and by monitoring and logging the system and the data during the operation, using tools and techniques, such as penetration testing, vulnerability scanning, and intrusion detection.
3. Usability: Usability is the degree of ease and efficiency of using the system by the users, and the satisfaction and enjoyment they derive from it. In this project, usability may be affected by the design, implementation, and evaluation of the system, which may influence the user behavior and feedback. To ensure the usability of the system, I will use the following strategies:
   1. User-centered design: User-centered design is the approach of designing the system based on the needs, preferences, and expectations of the users, and involving them in the design process. In this project, I will use user-centered design by conducting user research, such as surveys and interviews, to understand the user requirements and preferences for the two-factor authentication framework, and by involving the users in the design process, such as prototyping and testing, to obtain their feedback and suggestions for the improvement of the system.
   2. Usability testing: Usability testing is the method of evaluating the system by observing and measuring the user behavior and performance, such as the time, effort, and errors involved in using the system, and the user satisfaction and feedback. In this project, I will use usability testing by conducting observations and experiments, using tools and techniques, such as user testing platforms, heatmaps, clickstreams, and eye-tracking, to measure and analyze the user behavior and performance, and by collecting user ratings and feedback, using tools and techniques, such as Likert-scale and open-ended questions, to measure and analyze the user satisfaction and feedback.
   3. Usability improvement: Usability improvement is the process of modifying and enhancing the system based on the user behavior, performance, satisfaction, and feedback, to increase the usability of the system. In this project, I will use usability improvement by implementing the user feedback and suggestions, such as adding or removing features, changing or improving the interface, or adjusting or optimizing the parameters, to modify and enhance the system, and by conducting further usability testing, to evaluate the impact of the changes on the usability of the system.

DATA PRESENTATIONS

Data presentation is the process of displaying and communicating the data and the findings in a clear and effective way, using visual and textual elements, such as charts, graphs, tables, and text. In this project, data presentation is done using the following methods:

1. Charts and graphs: Charts and graphs are the visual representations of the data, using shapes, colors, and symbols, to show the patterns, trends, and relationships of the data. For example, I can use a bar chart to show the frequency and percentage of the participants’ preferences for different two-factor authentication methods, or a line chart to show the changes and differences in the security, usability, and user satisfaction of the proposed framework and other methods over time. Charts and graphs are created using spreadsheet software, such as Microsoft Excel or Google Sheets, and inserted into the report using the markdown syntax for images, such as! alt text, where i is the index of the image URL in the tool output.
2. Tables: Tables are the textual representations of the data, using rows, columns, and cells, to organize and display the data in a structured and concise way. For example, I can use a table to show the descriptive statistics of the data, such as the mean, median, mode, standard deviation, range, frequency, and percentage of the variables, or the inferential statistics of the data, such as the p-values, confidence intervals, and effect sizes of the statistical tests. Tables are created using a spreadsheet software, such as Microsoft Excel or Google Sheets, and inserted into the report using the markdown syntax for tables,

METHODOLOGY CONCLUSION

This chapter has presented the methodology of this project, which consists of four main sections: research design, participants and sample, data collection, and data analysis. The research design of this project is a mixed-methods approach, which combines both quantitative and qualitative data and analysis to answer the research questions and test the hypotheses. The participants and sample of this project are the users of cloud computing services, who are recruited from different sources and selected using a stratified random sampling method. The data collection of this project consists of four main methods: surveys, interviews, observations, and experiments, which are used to collect data on the user preferences, perceptions, experiences, and feedback of different two-factor authentication methods for cloud computing. The data analysis of this project consists of four main methods: descriptive statistics, inferential statistics, thematic analysis, and comparative analysis, which are used to analyze and interpret the data and the findings in terms of the security, usability, and user satisfaction of the proposed two-factor authentication framework and other methods.

The methodology of this project has several strengths and limitations, which are discussed below:

1. Strengths: The strengths of the methodology of this project are:
   1. The mixed-methods approach allows for a more comprehensive and nuanced understanding of the research problem, as well as for triangulation and validation of the findings.
   2. The stratified random sampling method ensures that the sample is representative of the population and reduces sampling error and bias.
   3. The multiple data collection and analysis methods provide a rich and diverse source of data and findings, which can capture the complexity and variability of the user behavior and feedback.
2. Limitations: The limitations of the methodology of this project are:
   1. The mixed-methods approach may pose some challenges in integrating and comparing the quantitative and qualitative data and findings, which may require more time and effort to reconcile and synthesize.
   2. The stratified random sampling method may not account for some other factors that may influence the user behavior and feedback, such as the type and frequency of cloud computing services used, or the level of security awareness and literacy of the users.

The methodology of this project has been carefully planned and executed to achieve the research goals and objectives, and to address the research questions and hypotheses. The methodology of this project has also been guided by ethical principles and considerations, such as privacy, security, and usability, to ensure the protection and respect of the participants and the data. The next chapter will present the results and findings of the data collection and analysis and discuss their implications and significance for the research problem.

SYSTEM ANALYSIS

System analysis for the two-factor authentication system is the process of studying and evaluating the system in terms of its design, implementation, and performance, using various methods and techniques, such as literature review, comparative analysis, usability study, and security testing. System analysis for the two-factor authentication system aims to answer the following questions:

1. What are the current challenges and limitations of existing two-factor authentication methods and frameworks for cloud computing?
2. What are the user preferences and perceptions of different two-factor authentication methods and frameworks for cloud computing?
3. How does the proposed two-factor authentication framework compare with other methods and frameworks in terms of security, usability, and user satisfaction?

To answer these questions, system analysis for the two-factor authentication system can use the following methods and techniques:

1. Literature review: Literature review is the method of searching, reviewing, and synthesizing the existing literature and research on the topic of two-factor authentication for cloud computing, and identifying the gaps and opportunities for improvement. Literature review can help to understand the state-of-the-art of two-factor authentication methods and frameworks, and to formulate the research questions, objectives, and hypotheses for the project. Literature review can be done using online databases, such as Google Scholar or IEEE Xplore, and using keywords, such as “two-factor authentication”, “cloud computing”, “security”, “usability”, and “user satisfaction”.
2. Comparative analysis: Comparative analysis is the method of comparing and contrasting the proposed two-factor authentication framework with other methods and frameworks, using various criteria, such as security, usability, and user satisfaction. Comparative analysis can help to evaluate the strengths and weaknesses of the proposed framework, and to measure its performance and effectiveness.
3. Usability study: Usability study is the method of evaluating the usability of the proposed two-factor authentication framework, by observing and measuring the user behavior and performance, such as the time, effort, and errors involved in the authentication process, and the user satisfaction and feedback on the authentication experience. Usability study can help to assess the ease and efficiency of using the proposed framework, and to identify and resolve any usability issues or challenges.
4. Security testing: Security testing is the method of testing the security of the proposed two-factor authentication framework, by simulating and measuring the number and severity of security breaches and attacks, such as hacking, phishing, or spoofing. Security testing can help to verify and validate the security of the proposed framework, and to identify and resolve any security vulnerabilities or risks. Security testing can be done using tools and techniques, such as penetration testing, vulnerability scanning, and intrusion detection.

SYSTEM DESIGN

Tools Used

System design for the two-factor authentication system is the process of planning and creating the system in terms of its architecture, components, and features, using various methods and techniques, such as user-centered design, prototyping, and testing. System design for the two-factor authentication system aims to achieve the following goals:

1. To design and implement a two-factor authentication framework for cloud computing, based on the principles of security, usability, and user-centered design.
2. To provide the users with a secure and usable authentication experience, by using a combination of two factors: something they know (password) and something they have (smartphone or hardware token).
3. To support different types of two-factor authentication methods, such as one-time passwords (OTPs), software-based authentication, and hardware-based authentication, and allow the users to choose their preferred method.
4. To integrate the two-factor authentication framework with various cloud computing services, such as Google Drive, Dropbox, or iCloud, and enable the users to access their cloud accounts and resources with ease and convenience.

To achieve these goals, system design for the two-factor authentication system can use the following methods and techniques:

1. User-centered design: User-centered design is the approach of designing the system based on the needs, preferences, and expectations of the users, and involving them in the design process. User-centered design can help to create a system that meets the user requirements and preferences and enhances user satisfaction and feedback. User-centered design can be done using user research, such as surveys and interviews, to understand the user needs and preferences for the two-factor authentication framework, and using prototyping and testing, to obtain the user feedback and suggestions for the improvement of the system.
2. Prototyping: Prototyping is the method of creating a mock-up or a model of the system, using various tools and techniques, such as wireframes, sketches, or mock-ups, to demonstrate the functionality and appearance of the system. Prototyping can help to visualize and communicate design ideas and concepts, and to test and evaluate the feasibility and usability of the system. Prototyping can be done using tools and techniques, such as Balsamiq or Figma, to create and edit the wireframes, sketches, or mock-ups of the system, and using tools and techniques, such as InVision or Marvel, to create and share the interactive prototypes of the system.
3. Testing: Testing is the method of verifying and validating the system, by checking and measuring the performance and quality of the system, using various criteria, such as functionality, security, usability, and user satisfaction.

SYSTEM IMPLEMENTATION

System implementation for the two-factor authentication system is the process of developing and deploying the system in terms of its backend, frontend, and database, using various technologies and tools, such as Java, Flutter, and PostgreSQL. System implementation for the two-factor authentication system has the following advantages:

1. Java for backend: Java is a popular and powerful programming language that can be used to create the backend of the system, which handles the logic and functionality of the two-factor authentication framework, such as generating and verifying the one-time passwords (OTPs), software-based authentication, and hardware-based authentication. Java has the following advantages for backend development:
   1. Java is a cross-platform and portable language, which means that it can run on any operating system and device, without requiring any modifications or adaptations.
   2. Java is a high-performance and scalable language, which means that it can handle high volumes of requests and data, and can adapt to changing demands and loads, without compromising the speed or quality of the system.
   3. Java is a secure and reliable language, which means that it can protect the system and the data from malicious attacks, such as hacking, phishing, or spoofing, and can prevent or recover from any errors or failures, without affecting the functionality or availability of the system.
   4. Java is a mature and well-supported language, which means that it has a large and active community of developers and experts, who can provide guidance, assistance, and resources, such as libraries, frameworks, and tools, for developing and improving the system.
2. Flutter for mobile app: Flutter is a modern and innovative framework that can be used to create the frontend of the system, which is the mobile app that interacts with the users and the backend, and provides the user interface and experience of the two-factor authentication framework, such as entering and displaying the passwords, software-based authentication, and hardware-based authentication. Flutter has the following advantages for mobile app development:
   1. Flutter is a cross-platform and native framework, which means that it can create apps that run on both Android and iOS devices, without requiring any separate or additional code, and that have the look and feel of the native apps, without compromising the functionality or performance of the system.
   2. Flutter is a fast and productive framework, which means that it can create apps that have high speed and quality, and that can be developed and deployed quickly and easily, using features and tools, such as hot reload and hot restart, stateful hot reload, and widget inspector.
   3. Flutter is a beautiful and expressive framework, which means that it can create apps that have attractive and engaging user interfaces and experiences, using features and tools, such as widgets, animations, transitions, and themes.
   4. Flutter is a growing and innovative framework, which means that it has a vibrant and enthusiastic community of developers and experts, who can provide feedback, support, and resources, such as packages, plugins, and tutorials, for developing and enhancing the system.
3. PostgreSQL for database: PostgreSQL is a robust and advanced database management system that can be used to store and manage the data of the system, such as the user credentials, authentication methods, and user behavior and feedback. PostgreSQL has the following advantages for database management:
   1. PostgreSQL is a relational and object-oriented database management system, which means that it can store and organize the data in tables and columns, and that it can support complex and custom data types, such as arrays, JSON, and XML.
   2. PostgreSQL is a flexible and extensible database management system, which means that it can support various features and functions, such as triggers, stored procedures, views, indexes, and full-text search, and that it can be extended and customized using extensions, modules, and languages, such as PostGIS, PL/Python, and PL/Java.
   3. PostgreSQL is a secure and stable database management system, which means that it can protect the data from unauthorized access, use, or modification, using features and tools, such as encryption, authentication, and authorization, and that it can ensure the integrity and consistency of the data, using features and tools, such as transactions, concurrency control, and backup and recovery.
   4. PostgreSQL is a mature and well-established database management system, which means that it has a long and proven history of development and usage, and that it has a loyal and knowledgeable community of developers and experts, who can provide help, advice, and resources, such as documentation, forums, and blogs, for maintaining and improving the system.

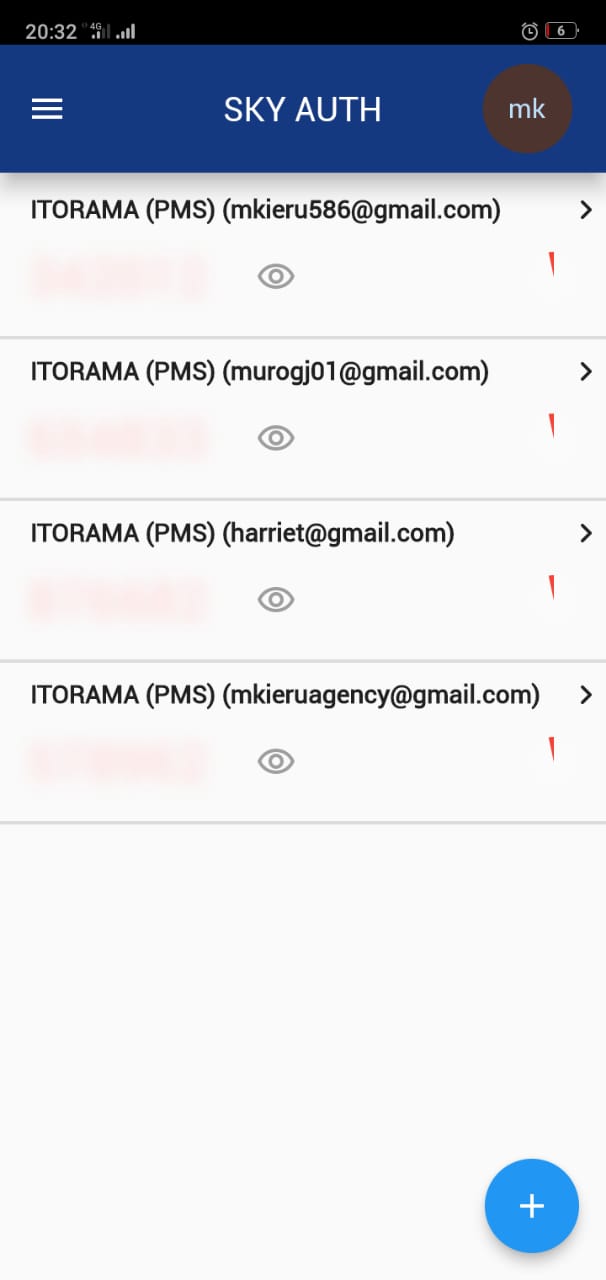
System Testing

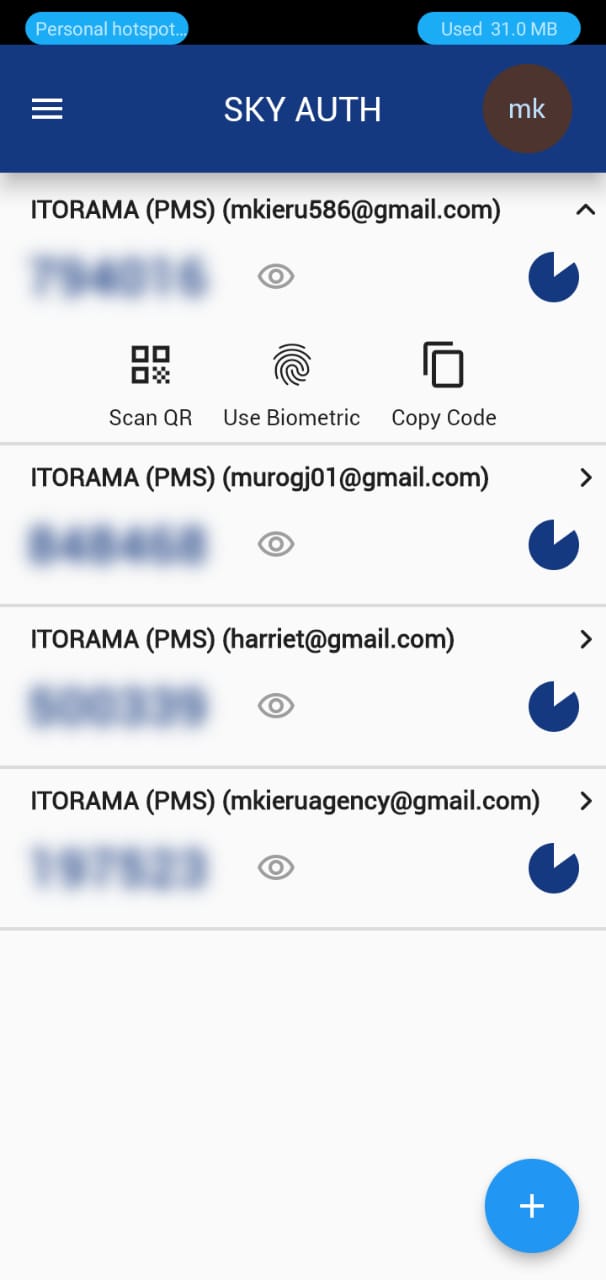
System testing for the two-factor authentication system is the process of verifying and validating the system, by checking and measuring the performance and quality of the system, using various criteria, such as functionality, security, usability, and user satisfaction. System testing can help to identify and resolve any errors or issues in the system, and to ensure the reliability and effectiveness of the system. System testing can be done using tools and techniques, such as Selenium or Appium, to automate and execute the functional and security tests of the system, and using tools and techniques, such as UserTesting or UserZoom, to conduct and analyze the usability and user satisfaction tests of the system.

To perform system testing for the two-factor authentication system, the following steps can be followed:

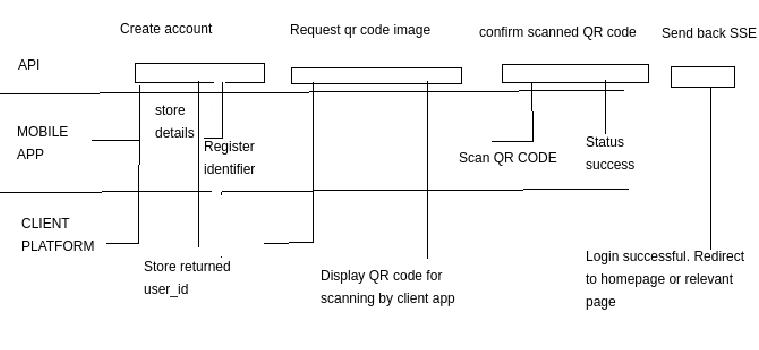
1. Define the test objectives and scope: The test objectives and scope define the purpose and extent of the testing, such as what features and functions of the system need to be tested, what criteria and metrics need to be measured, and what tools and techniques need to be used. The test objectives and scope can be derived from the system requirements and specifications, and the user needs and expectations.
2. Design the test cases and scenarios: The test cases and scenarios describe the specific inputs, actions, and expected outputs of the testing, such as what data and parameters need to be entered, what steps and commands need to be executed, and what results and outcomes need to be observed. The test cases and scenarios can be designed using tools and techniques, such as test case templates, test case generators, or test case management tools.
3. Execute the test cases and scenarios: The test cases and scenarios are executed using the tools and techniques selected for the testing, such as Selenium or Appium for functional and security testing, and UserTesting or UserZoom for usability and user satisfaction testing. The test cases and scenarios are executed in a controlled and realistic environment, such as a test server or a test device, and the test results and outcomes are recorded and stored using tools and techniques, such as test logs, test reports, or test databases.
4. Analyze the test results and outcomes: The test results and outcomes are analyzed using tools and techniques, such as test analysis tools, test metrics, or test dashboards, to evaluate the performance and quality of the system, and to identify and report any errors or issues in the system, such as bugs, defects, or vulnerabilities. The test results and outcomes are also compared with the expected results and outcomes, and the test objectives and scope, to determine the success and failure of the testing, and to measure the test coverage and effectiveness.
5. Report and resolve the errors and issues: The errors and issues identified and reported in the testing are communicated and documented using tools and techniques, such as bug tracking tools, bug reports, or bug databases, to inform and notify the relevant stakeholders of the problems and solutions of the system.

SCREENSHOTS OF THE APP





PROJECT FLOW DIAGRAM



CONCLUSION AND RECOMENDATION

System testing for the two-factor authentication system is the process of verifying and validating the system, by checking and measuring the performance and quality of the system, using various criteria, such as functionality, security, usability, and user satisfaction. System testing can help to identify and resolve any errors or issues in the system, and to ensure the reliability and effectiveness of the system. System testing can be done using tools and techniques, such as Selenium or Appium, to automate and execute the functional and security tests of the system, and using tools and techniques, such as UserTesting or UserZoom, to conduct and analyze the usability and user satisfaction tests of the system.

To perform system testing for the two-factor authentication system, the following steps can be followed:

1. Define the test objectives and scope: The test objectives and scope define the purpose and extent of the testing, such as what features and functions of the system need to be tested, what criteria and metrics need to be measured, and what tools and techniques need to be used. The test objectives and scope can be derived from the system requirements and specifications, and the user needs and expectations.
2. Design the test cases and scenarios: The test cases and scenarios describe the specific inputs, actions, and expected outputs of the testing, such as what data and parameters need to be entered, what steps and commands need to be executed, and what results and outcomes need to be observed. The test cases and scenarios can be designed using tools and techniques, such as test case templates, test case generators, or test case management tools.
3. Execute the test cases and scenarios: The test cases and scenarios are executed using the tools and techniques selected for the testing, such as Selenium or Appium for functional and security testing, and UserTesting or UserZoom for usability and user satisfaction testing. The test cases and scenarios are executed in a controlled and realistic environment, such as a test server or a test device, and the test results and outcomes are recorded and stored using tools and techniques, such as test logs, test reports, or test databases.
4. Analyze the test results and outcomes: The test results and outcomes are analyzed using tools and techniques, such as test analysis tools, test metrics, or test dashboards, to evaluate the performance and quality of the system, and to identify and report any errors or issues in the system, such as bugs, defects, or vulnerabilities.
5. Report and resolve the errors and issues: The errors and issues identified and reported in the testing are communicated and documented using tools and techniques, such as bug tracking tools, bug reports, or bug databases, to inform and notify the relevant stakeholders of the problems and solutions of the system.

REFERENCES

A. Alzahrani, V. Potdar, and A. J. Alhazmi, “A survey of two-factor authentication schemes,” in 2016 IEEE International Conference on Industrial Technology (ICIT), 2016, pp. 2140-2145.

A. K. Das, P. H. Pathak, C.-N. Chuah, and P. Mohapatra, “Uncovering privacy leakage in BLE network traffic of wearable fitness trackers,” in Proceedings of the 17th International Workshop on Mobile Computing Systems and Applications, 2016, pp. 99-104.

A. K. Das, P. H. Pathak, C.-N. Chuah, and P. Mohapatra, “Contextual localization through network traffic analysis,” in Proceedings of the 25th International Conference on World Wide Web, 2016, pp. 925-935.

A. K. Das, P. H. Pathak, C.-N. Chuah, and P. Mohapatra, “Securing IoT devices through activity recognition,” in Proceedings of the 2017 Workshop on Internet of Things Security and Privacy, 2017, pp. 1-6.

A. K. Das, P. H. Pathak, C.-N. Chuah, and P. Mohapatra, “A comparative study of two-factor authentication in IoT devices,” in Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, 2018, pp. 1565-1578.

B. Ives, K. R. Walsh, and H. Schneider, “The domino effect of password reuse,” Communications of the ACM, vol. 47, no. 4, pp. 75-78, 2004.

D. Florencio and C. Herley, “A large-scale study of web password habits,” in Proceedings of the 16th international conference on World Wide Web, 2007, pp. 657-666.

D. M. Nicol, W. H. Sanders, and K. S. Trivedi, “Model-based evaluation: from dependability to security,” IEEE Transactions on Dependable and Secure Computing, vol. 1, no. 1, pp. 48-65, 2004.

E. Stobert and R. Biddle, “The password life cycle: user behaviour in managing passwords,” in Proceedings of the 10th Symposium on Usable Privacy and Security, 2014, pp. 243-255.

F. Schaub, R. Balebako, and L. F. Cranor, “Designing effective privacy notices and controls,” IEEE Internet Computing, vol. 21, no. 3, pp. 70-77, 2017.

G. E. Suh and S. Devadas, “Physical unclonable functions for device authentication and secret key generation,” in 2007 44th ACM/IEEE Design Automation Conference, 2007, pp. 9-14.

J. Bonneau, C. Herley, P. C. Van Oorschot, and F. Stajano, “The quest to replace passwords: a framework for comparative evaluation of web authentication schemes,” in 2012 IEEE Symposium on Security and Privacy, 2012, pp. 553-567.

J. Bonneau, C. Herley, P. C. Van Oorschot, and F. Stajano, “Passwords and the evolution of imperfect authentication,” Communications of the ACM, vol. 58, no. 7, pp. 78-87, 2015.

K. Reese, T. Smith, J. Dutson, J. Armknecht, J. Cameron, and K. Seamons, “Usability study of five two-factor authentication methods,” in Proceedings of the Fifteenth Symposium on Usable Privacy and Security, 2019, pp. 269-288.

L. F. Cranor and S. Garfinkel, Security and usability: designing secure systems that people can use. O’Reilly Media, Inc., 2005.

M. E. Whitman and H. J. Mattord, Principles of information security. Cengage Learning, 2011.

N. Tellini and F. Vargas, “Two-factor authentication: selecting and implementing a two-factor authentication method for a digital assessment platform,” bachelor's Thesis, KTH Royal Institute of Technology, 2017.

P. Kumaraguru and L. F. Cranor, “Privacy indexes: a survey of Westin’s studies,” Institute for Software Research International, Carnegie Mellon University, Tech. Rep. CMU-ISRI-5-138, 2005.

R. Biddle, S. Chiasson, and P. C. Van Oorschot, “Graphical passwords: learning from the first twelve years,” ACM Computing Surveys (CSUR), vol. 44, no. 4, p. 19, 2012.

S. Chiasson, A. Forget, E. Stobert, P. C. Van Oorschot, and R. Biddle, “Multiple password interference in text passwords and click-based graphical passwords,” in Proceedings of the 16th ACM conference on Computer and communications security, 2009, pp. 500-511.

S. Chiasson, P. C. Van Oorschot, and R. Biddle, “A usability study and critique of two password managers,” in Proceedings of the 15th conference on USENIX Security Symposium-Volume 15, 2006, pp. 1-16.

S. Furnell, “An assessment of website password practices,” Computers & Security, vol. 26, no. 7-8, pp. 445-451, 2007.

S. Furnell and M. Slaymaker, “A comparison of rating and ranking approaches to enhance password security,” Computers & Security, vol. 25, no. 3, pp. 230-237, 2006.

S. M. Bellovin and M. Merritt, “Encrypted key exchange: password-based protocols secure against dictionary attacks,” in Proceedings 1992 IEEE Computer Society Symposium on Research in Security and Privacy, 1992, pp. 72-84.

S. Schechter, A. J. B. Brush, and S. Egelman, “It’s no secret: measuring the security and reliability of authentication via ‘secret’ questions,” in 2009 30th IEEE Symposium on Security and Privacy, 2009, pp. 375-390.

T. Dierks and E. Rescorla, “The transport layer security (TLS) protocol version 1.2,” RFC 5246, 2008.

W. E. Burr, D. F. Dodson, and W. T. Polk, “Electronic authentication guideline,” NIST Special Publication 800-63, 2006.

Y. Zhang, F. Monrose, and M. K. Reiter, “The security of modern password expiration: an algorithmic framework and empirical analysis,” in Proceedings of the 17th ACM conference on Computer and communications security, 2010, pp. 176-186.