Strathmore
UNIVERSITY

MITIGATING IDENTITY THEFT BY THE USE OF BIOMETRIC AUTHENTICATION ON SOCIAL MEDIA APPLICATIONS

BY: AKUNGO KATE STACY

146201

SUPERVISOR: DR. VITALIS OZIANYI

A COMPUTER NETWORKS AND CYBER SECURITY PROJECT I SUBMITTED TO THE SCHOOL OF COMPUTING AND ENGINEERING SCIENCES IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE AWARD OF THE DEGREE IN BACHELOR OF SCIENCE IN COMPUTER NETWORKS AND CYBER SECURITY OF STRATHMORE UNIVERSITY.

NAIROBI, KENYA

JUNE 2023

DECLARATION AND APPROVAL

I declare that this work has not been previously submitted and approved for the award of a degree by this or any University. To the best of my knowledge and belief, the work contains no material previously published or written by another person except where due reference is made in the work itself.

Student's Name: Akungo Kate Stacy

Student Number: 146201

Sign: _____ Date: _____

The proposal of **Akungo Kate** has been reviewed and approved by **Dr. Vitalis Ozianyi**

Sign:_____ Date: _____

ABSTRACT

Identity theft on social media applications can have serious and lasting impacts on the user's life. Existing authentication methods are not effective enough since they are susceptible to breaches, hence the need for a stronger authentication method, biometric authentication. This project aims to mitigate identity theft on social media applications using biometric authentication, focusing on fingerprint identification. The project uses Kotlin programming language to incorporate biometric capture and processing modules using AndroidX Biometric library, which provides a set of APIs to access the biometric sensors and algorithms available on the user's device. The project will use agile methodology which is user centric and iterative for its development to ensure the final product is timely and meaningful to the user. The significance of the project is to improve the security of social media applications contributing to a healthy and safe social media environment.

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

2FA	- Two Factor Authentication
FIDO Alliance	- Fast Identity Online Alliance
FTC	- Federal Trade Commission
GPU	- Graphical Processing Unit
M-pesa APP	- Mobile money application
NIST	- National Institute of Standards and Technology
OOBA	- Out of Band Authentication
OTP	- One Time Password
PIN	- Personal Identification Number
SIM	- Subscriber Identity Module
SMS	- Short Message Service
SP	- Service Provider

LIST OF FIGURES

CHAPTER 1: INTRODUCTION

1.1 Background

With the widespread adoption of social media platforms, concerns related to identity theft and unauthorized access to personal information have become more prevalent. According to the FTC, there were over 1.4 million reports of identity theft in 2020, and 28% of them involved social media or email accounts,(Anon 2021).

Social media applications have emerged as prime targets for identity thieves due to the wealth of personal information they store and the vast number of active users. These platforms contain users' photos, contact details, connections, and even their daily activities, making them an attractive source of data for cybercriminals. Unauthorized access to social media accounts not only compromises the individual user but also risks affecting their social connections.

Traditional authentication methods, such as passwords and two-factor authentication (2FA), have been the primary means of securing social media accounts. However, these methods suffer from certain limitations. According to a survey by Google, 52% of users reuse the same password for multiple accounts, and 13% of users have more than 100 passwords to remember, after examining a database of over 28 million users and their 61 million passwords, they have uncovered an alarming figure: 52% of the users studied have the same passwords (or very similar and easily hackable ones) for different services, (Security 2018). 2FA, although an improvement, can still be bypassed through various techniques, including social engineering and SIM swapping, (Anon n.d.-a).

Biometric authentication offers a robust solution to overcome the limitations of traditional authentication methods. In contrast to passwords, badges, or documents, biometric data cannot be forgotten, exchanged, stolen, or forged, offering a high level of accuracy and security, (Anon 2023). By utilizing an individual's unique physical traits, social media platforms can ensure more accurate and reliable user identification. Biometric factors commonly used for authentication include fingerprints and facial recognition.

1.2 Problem Statement

With the wide adoption of social media platforms for communication, entertainment, and information sharing, there has been a subsequent rise in identity theft posing significant risks to users' personal and financial data.

Traditional methods of user authentication on social media apps, such as passwords and security questions, have proven to be susceptible to breaches and attacks. As a result, there is a pressing need for stronger and more secure authentication mechanisms to protect users' identities and personal data.

This project seeks to provide a solution by incorporating biometric authentication on social media applications which is safe from breaches because it uses the unique physical characteristics of users to verify their identities, which are difficult to forge, steal, or guess.

1.3 General Aim

This project aims to contribute to the mitigation of identity theft, by incorporating biometric authentication on social media applications.

1.4 Specific Objectives

i. To review existing authentication methods on social media applications and their efficiency.
ii. To review existing works related to biometric authentication on other applications i.e., financial applications like M-PESA APP.
iii. To design an authentication system that supports the use of biometric sensors to eliminate the need for username and password authentication in compliance with FIDO Alliance.
iv. To develop the authentication system and test it on users.

1.5 Justification

The project is justified due to; the rising incidents of identity theft, the limitations of traditional authentication methods, the enhanced security and user experience offered by biometric authentication, the fraud detection capabilities, the industry trend towards biometric technology, and the need to address privacy concerns. By implementing biometric authentication, the project aims to provide a proactive and effective solution to mitigate identity theft on social media platforms, contributing to a safer and more secure online environment for users.

1.6 Scope and delimitations

1.6.1 Scope

Design and implement a biometric authentication system for social media applications as an alternative authentication method that can enhance users' security and privacy, as well as reduce the incidence and impact of identity theft when interacting with social media applications.

1.7 Delimitations

The project will prioritize the use of fingerprint authentication as the primary method for verifying the identity of social media account users. Alternative methods such as face recognition or voice recognition will not be employed as backup or alternative authentication methods.

The project will employ optical scanners specifically designed for capturing and processing fingerprint images. Other types of scanners, such as capacitive, ultrasonic, or thermal scanners, will not be utilized in the authentication process.

1.8 Limitations

The biometric authentication system for social media accounts may encounter several challenges and limitations. Firstly, individuals with physical disabilities may face difficulties as the system may struggle to recognize their changing physical traits caused by injuries, illnesses, aging, or even the loss of fingerprints due to burning or scars.

Secondly, the effectiveness of the authentication system heavily relies on the quality and accuracy of the biometric scanners. Issues such as environmental factors, human errors, wet or dirty fingers, or damaged scanners can lead to inaccurate or failed authentication attempts.

Thirdly, the system may lack remote access capabilities, restricting users from accessing their accounts or services from different devices or locations. If a user forgets or loses the device that contains their biometric data, they may not be able to access their account from another device.

These challenges highlight the need for alternative authentication methods or supplementary security measures to ensure a seamless and inclusive user experience while maintaining the security of social media applications.

CHAPTER 2: LITERATURE REVIEW

2.1 Introduction

In the chapter, related works as well as gaps regarding the proposed project are discussed. The significance of the project is explained, and a conceptual framework is designed.

2.2 Existing Password Less Authentication Technologies and Gaps

2.2.1 Password Manager

A study conducted on three popular cross-platform password managers; 1password, lastpass and keepass password safe. They are software applications that help users generate, store and retrieve their passwords for different online services.

Our analysis based on this model and experiments on GPU both show that the security of authentication mechanism relies on the master password and iteration number. Hence, long password and big iteration number should be used in password managers.(Yu and Yin, 2021).

While password managers improve user experience by removing the need to generate and remember many passwords as long as the user remembers the master password, password managers still have some limitations such as; the potential for a single point of failure, as the security of all stored passwords relies on the master password, dependency on the master password i.e. weak and guessable passwords potentially undermine the effectiveness of password managers.

2.2.2 One-Time-Password Authentication

One-time password (OTP) is a unique authentication code that is valid for a single use or a short duration, typically generated by a server or authentication system and sent to the user's registered device. The user enters the OTP to the primary authentication channel to verify their identity. Once used, OTP becomes invalid and cannot be reused for unauthorized access.

Since the password (a four or six-digit numerical PIN code in most instances) can be entered just once, it's not as risky as static passwords that can be used a second time.(Anon n.d.-c)

As much as OTPs improve convenience and user experience, they are still susceptible to; phishing and man n the middle attacks where attackers trick users to expose their OTPs through

deceptive websites and emails. They are also prone to replay attacks where the attacker captures the OTP during transmission and attempt to use it during the valid time window, compromising the security of OTP authentication.

2.2.3 Out-Of-Band authentication

Out-of-band authentication (OOBA) requires users to verify their identities through two different communications channels. This makes it harder for fraudsters to bypass or tamper with the authentication process, providing an increased level of security.(Anon n.d.-d)

OOBA typically involves the use of a secondary channel, the user receives the OTP on their email and enters it to the primary authentication channel i.e. the application. The system verifies the OTP and if it matches the one generated by the secondary channel access is granted.

While OOBA is a good authentication system it has limitations i.e. it is susceptible to social engineering attacks, an attacker may pose as legitimate service provider and contact the user to share their OTPs, when the user falls victim to such scams, they compromise the effectiveness of OOBA.

OOBA has poor user experience and convenience. Even though it enhances security it also introduces additional steps and complexities to the authentication process, impacting user experience negatively.

2.3 User Identity Management Model

Isolated User Identity Model is the most common identity management model it lets service providers act as both credential provider and identifier provider to their clients. They control the name space for a specific service domain and allocate identifiers to users. A user gets separate unique identifiers from each service/identifier provider he transacts with. In addition, each user will have separate credentials, such as passwords associated with each of their identifiers.

The identifier and credential indexes in the figure below- refer to the issuing entity. For example, an identifier and credential with index 1 means that it has been issued by SP 1. This approach might provide simple identity management for service providers but is rapidly becoming unmanageable for users. The explosive growth in the number of online services based on this model results in users being overloaded with identifiers and credentials that they need to manage.

Users are often required to memorize passwords, which unavoidably leads to users forgetting passwords to infrequently used services. Forgotten passwords, or simply the fear of forgetting, create a significant barrier to usage, resulting in many services not reaching their full potential. For important sensitive services, where password recovery must be highly secure, forgotten passwords can also significantly increase the cost for the service provider.

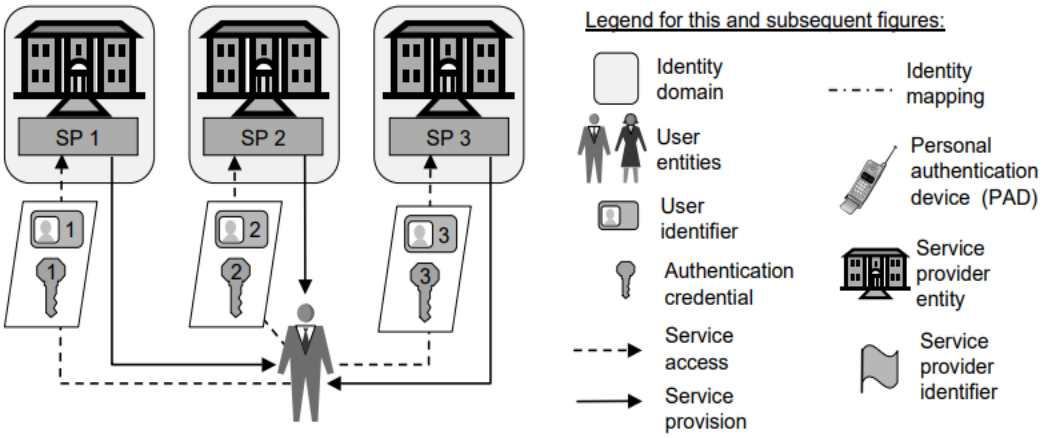

Figure 2-1 Isolated User Identity Model

Isolated User Identity Model is secure, the problem is managing many passwords and increased cost for service providers. Otherwise, it is relatively safe because there are no third parties whose database can be compromised. This problem can be mitigated by replacing passwords with biometric data which cannot be forgotten.(Jøsang and Pope n.d.)

Hence Isolated User Identity Model is the most secure user identity management model to implement the project, since no third parties will be needed for credentials authentication since they can also be a potential point of weakness when compromised.

2.4 Biometric Technology

Ultrasonic fingerprint scanners, this is the latest fingerprint scanning technology to enter the smartphone space. Unlike its predecessors i.e. optical and capitative scanners, ultrasonic scanners can capture highly detailed three-dimensional image of the fingerprint, by generating and transmitting an ultrasonic pulse against the finger. Depending upon the ridges, valleys, pores, and other nuisances of the finger, some of the pulse gets absorbed while some bounces back to the sensor.(Davies 2019) Making it more secure.

Optical scanners are easy to fool as the technology only captures two-dimensional picture which can be copied by use of prosthetic and good quality pictures. Also the optical sensor has a finite resolution hence the higher the resolution, the finer the details the sensor can discern about your finger increasing the level of security.

2.5 Conceptual Framework

Figure 2-2 illustrates how the biometric authentication system works. The user either signs in or logs in depending on whether they have interacted with the application before. If it is the first contact, the user signs in, their biometric data is taken using biometric sensors available on the user's smart phone. The biometric template is encrypted and stored in the application's database.

On second contact, the user logs in to the application by using their biometric data, the data is checked on the database if a match is made, they are given access to the account otherwise access is denied.

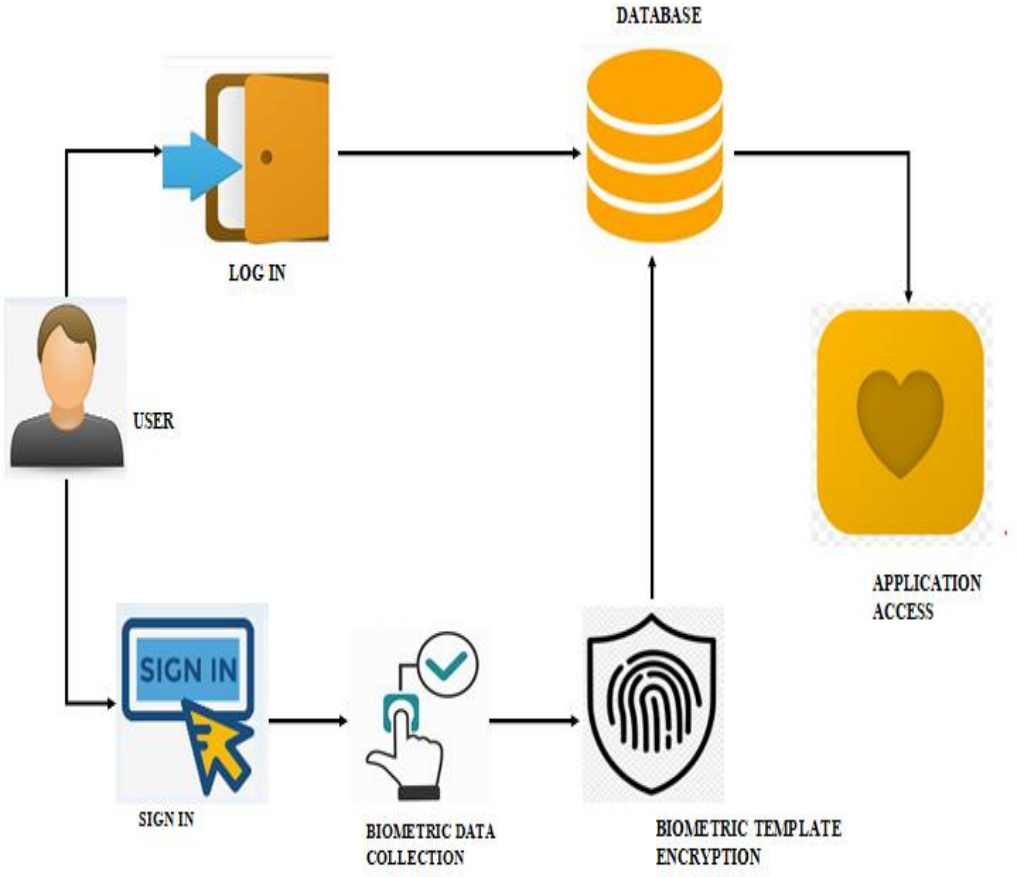

Figure 2-2 Conceptual Framework

CHAPTER 3: METHODOLOGY

3.1 Introduction

The methodology to be used during the development and implementation of the project is discussed together with the requirements. It highlights the system development tools, technologies and programming languages that have been used in the development.

3.2 System Development Methodology

The project has been developed using agile methodology.

The emphasis of the agile methodology is rapid and iterative development with considerable interaction between the developers and the users who will be the application customers. This methodology is popular in Web development and gamers.(Anon n.d.-b)

Figure 3-1 is a pictorial explanation of how agile methodology is incorporated into the development of the project.

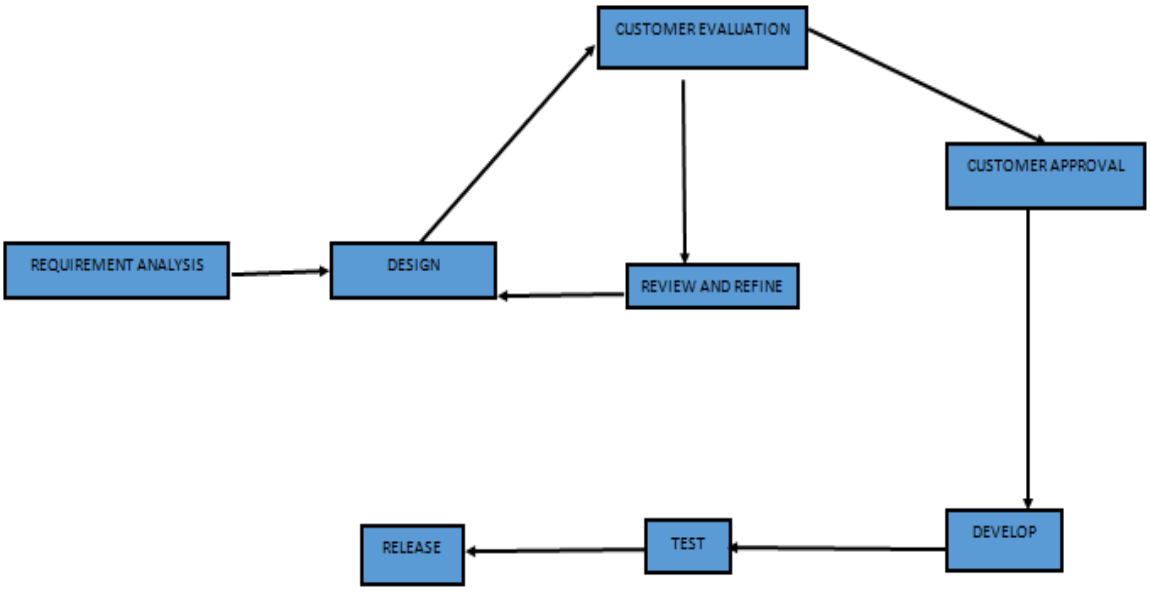

Figure 3-1 Agile Methodology

Key elements of agile methodology in regard to the project are discussed below:

3.2.1 Requirement Analysis

In this phase, requirements for the project development will be analyzed and stated. This will involve the project objectives, and the expected functionality of the system. The requirement analysis phase will help to establish a clear vision for the model and define the key features and performance goals.

3.2.2 Design

The general outlook of the biometric interface is created. The system architecture and components of the biometric authentication system are designed. The functions and interactions of each component, such as the user interface, the biometric capture module, the biometric processing module, the biometric matching module, the biometric database module, and the biometric verification module are defined.

3.2.3 Customer Evaluation

A usability test is done to measure the user experience and performance of the biometric authentication system. A sample of users are recruited who use the biometric authentication system to log in to their social media accounts. The user behavior and outcomes, such as the success rate, error rate, time taken, number of attempts, and user comments are measured and recorded.

3.2.4 Review and Refinement

The biometric authentication system is modified and refined to address the issues and problems captured during customer evaluation phase. Changes are made to the system design, architecture, components, algorithms, or specifications as needed. New features or functionalities that are requested or suggested by the users are added.

3.2.5 Development

The biometric authentication system is coded and programed using the selected programming languages(kotlin), frameworks, and tools, following the coding standards and best practices to ensure the quality and readability of the code. The code is also documented and commented to explain its logic and functionality.

3.2.6 Test

A test report that summarizes and presents the results and findings of the functional test, performance test, security test, and usability test is created using; graphs, charts, tables, and text to illustrate and explain the tests.

3.2.7 Release

The complete and stable biometric authentication system is prepared and packaged for delivery and deployment. Necessary documentation such as user manuals, installation guides and troubleshooting tips are included.

3.3 Justification Of Methodology

3.3.1 Interactive development

Agile methodology involves iterative development cycles with regular feedback and continuous improvement. This aligns well with the implementation of the project, which may require multiple iterations to refine the authentication process and address any issues or user feedback.

3.3.2 Flexibility and adaptability

Agile methodology is designed to handle changing requirements and evolving technologies. As biometric authentication technologies and user expectations evolve, an Agile approach allows for flexibility and adaptation, ensuring that the authentication implementation remains up-to-date and aligned with industry advancements.

3.3.3 User-centric focus

Biometric authentication directly affects the user experience on social media applications. Agile methodology emphasizes close collaboration with stakeholders, including end users, to gather feedback and continuously improve the user experience. This is crucial when implementing biometric authentication, as it needs to be seamless, user-friendly, and well-received by the application's user base.

3.3.4 Risk mitigation

Agile methodology emphasizes early identification and mitigation of risks. When implementing biometric authentication, potential risks such as technical challenges, data privacy concerns, or user acceptance can be addressed in a timely manner through regular reviews, feedback loops, and risk management practices inherent in Agile approach.

3.4 Tools And Techniques

The project requires the use of specific tools and technologies to implement and support the biometric authentication functionality. Below are essential tools that are required:

3.4.1 Biometric SDKs

Software Development Kits (SDKs). These SDKs provide the necessary APIs (Application Programming Interfaces) and libraries to interact with the biometric sensors available on the target devices. They enable developers to capture, process, and authenticate biometric data.

3.4.2 Biometric Sensors

These sensors are physical hardware components that capture the biometric traits of the user. For the development of the project, fingerprint sensors incorporated on the smartphone is used.

3.4.3 Biometric Algorithms

Biometric algorithms are responsible for processing and analyzing the captured biometric data to perform authentication. These algorithms compare the captured biometric traits with previously enrolled templates to determine a match. The SDKs often include pre-built libraries that handle these computations.

3.4.4 Encryption and Security Tools

Tools such as cryptographic libraries, secure communication protocols (e.g., SSL/TLS), and secure storage mechanisms (e.g., Keychain on iOS, Keystore on Android) are used to ensure the security and privacy of biometric information.

3.4.5 Testing and Validation Tools

Testing tools specific to biometrics, such as simulation tools, can help validate the performance and effectiveness of the biometric authentication implementation under different scenarios and conditions.

3.4.6 Development Environment and IDE

A standard development environment and Integrated Development Environment (IDE) is required for writing, testing, and debugging the biometrics code. For the development of the project, Android Studio is used. It provides the necessary features, debugging capabilities, and integration with SDKs for smooth development.

REFERENCES

Anon. 2021. “Identity Theft Awareness Week Starts Today.” *Consumer Advice*. Retrieved June 15, 2023 (https://consumer.ftc.gov/consumer-alerts/2021/02/identity-theft-awareness-week-starts-today).

Anon. 2023. “Biometrics: Definition, Use Cases, Latest News.” *Thales Group*. Retrieved June 15, 2023 (https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/biometrics).

Anon. n.d.-a. “New Data Shows FTC Received 2.2 Million Fraud Reports from Consumers in 2020 | Federal Trade Commission.” Retrieved June 15, 2023 (https://www.ftc.gov/news-events/news/press-releases/2021/02/new-data-shows-ftc-received-22-million-fraud-reports-consumers-2020).

Anon. n.d.-b. “Project Methodology - an Overview | ScienceDirect Topics.” Retrieved June 1, 2023 (https://www.sciencedirect.com/topics/computer-science/project-methodology).

Anon. n.d.-c. “What Are One-Time Passwords and Their Pros and Cons?” *Infosec Resources*. Retrieved May 31, 2023 (https://resources.infosecinstitute.com/topic/one-time-passwords-pros-and-cons/).

Anon. n.d.-d. “What Is Out-of-Band Authentication (OOBA)?” Retrieved June 11, 2023 (https://www.pingidentity.com/en/resources/blog/post/what-is-out-of-band-authentication-ooba.html).

Davies, Marion. 2019. “Fingerprint Scanners 101: Capacitive vs. Optical vs. Ultrasonic.” *Konsyse*. Retrieved June 11, 2023 (https://www.konsyse.com/articles/fingerprint-scanners-101-capacitive-vs-optical-vs-ultrasonic/).

Jøsang, Audun, and Simon Pope. n.d. “User Centric Identity Management.”

Security, Panda. 2018. “52% of Users Reuse Their Passwords for Different Services.” *Panda Security Mediacenter*. Retrieved June 15, 2023 (https://www.pandasecurity.com/en/mediacenter/security/password-reuse/).

Yu, Fei, and Hao Yin. 2021. “A Security Analysis of the Authentication Mechanism of Password Managers.” Pp. 865–69 in *2021 IEEE 21st International Conference on Communication Technology (ICCT)*.

APPENDICES

APPENDIX 1: Gantt Chart