An AI-Driven, Secure, and Trustworthy Ranking System for Blockchain-Based Wallets

A thesis submitted in partial fulfilment of the requirements for the degree of

Doctor of Philosophy

in Information Systems

by

Mwaheb Almadani

Under the supervision of Professor Farookh Khadeer Hussain

University of Technology Sydney
Faculty of Engineering and Information Technology
Sydney, Australia
April 2024

Certificate of Original Authorship

I, *Mwaheb Almadani*, declare that this thesis, submitted in partial fulfilment of the requirements for the award of Doctor of Philosophy, in the *Computer Science*, *Faculty of Engineering and Information Technology* at the University of Technology Sydney, Australia.

This thesis is wholly my own work unless otherwise referenced or acknowledged. In addition, I certify that all information sources and literature used are indicated in the thesis.

This document has not been submitted for qualifications at any other academic institution.

This research is supported by the Australian Government Research Training Program.

Production Note:

SIGNATURE: Signature removed prior to publication.

DATE: April, 2024

Acknowledgments

In the name of Allah, the Most Gracious, the Most Merciful,

I humbly express my deepest gratitude to Allah (God), the source of knowledge and power, for providing me guidance, determination and good health throughout the journey of completing this thesis. I have embarked on this scholarly endeavor and seen it through to completion only because of God’s boundless mercy and blessings. Also, to my supervisor, Professor Farookh Hussain, I express my sincere gratitude for his constant support, direction, and insightful feedback, all of which have been crucial in helping me to accomplish this thesis. Professor Farookh’s expertise, dedication, and encouragement have been a constant source of inspiration, guiding me through the challenges and milestones. Additionally, I would like to express my gratitude to my country, Saudi Arabia, for offering me this scholarship, which has enabled me to pursue my academic goal, develop as a scholar and contribute meaningfully to society. Furthermore, I am profoundly thankful to my children, Majdi and Murooj, for their genuine excitement and inspiration, which motivated me to continue striving for success. Throughout the challenges, especially during the COVID-19 pandemic, their patience, understanding, resilience and compassion have been a constant source of strength. I am endlessly grateful for their love, which has been a guiding light, illuminating the path towards achievement and fulfillment. Special gratitude is extended to my parents, siblings, and friends for their unwavering good wishes, steadfast support, and heartfelt prayers. Their presence has been a source of immense strength and comfort, uplifting me through every challenge and success. Their unconditional love and encouragement have guided my journey and provided a sense of companionship that I appreciate gratefully. Finally, I sincerely thank the University of Technology Sydney (UTS) for providing me with enriching experiences and opportunities. The university’s commitment to excellence in education has empowered me to thrive academically and personally, profoundly shaping my growth and development.

Abstract

The significance of blockchain security has gained considerable interest as blockchain technologies grow in popularity. The spectacular rise in cryptocurrency values has also increased the adoption of blockchain-based wallets(BW/BWs). This tendency emphasizes the need for comprehensive security measures to protect digital assets, maintain transaction integrity and preserve trust in the blockchain networks. The most critical concern surrounding blockchain-based wallets is managing users' private keys, which are essential for authorizing transactions and accessing the digital cryptocurrencies stored in the blockchain network. In recent years, malicious actors have increased efforts to compromise these private keys and take control of the BW's digital assets. Therefore, ensuring the security of private keys through rigorous security protocols is paramount to defend against unauthorized access and potential financial losses. This thesis aims to investigate the integration of hard security, such as authentication techniques and access controls, and soft security measures, such as trust models and ranking systems, in the context of BWs. By incorporating tangible physical defenses (hard security) with intangible procedural strategies (soft security), we present a comprehensive framework for enhancing BW solution security and trustworthiness. This is essential for the widespread adoption and use of blockchain technology in financial transactions and digital asset management. This thesis proposes a secure, intelligent, and trustworthy approach for BW solutions that incorporates 2FA and MFA as hard security measures and an AI-driven ranking system as soft security measures. We have developed a BW website (BWW) with four authentication mechanisms, including different factors such as TOTP and biometrics through facial recognition, allowing BW users to choose their preferred level of security. The BWW remarkably improves the security of BW solutions by defending them against various threats, including sophisticated cyber-attacks, unauthorized access and human-caused weaknesses. Moreover, We introduce a trust-based ranking system (TBW-RAnk) for BW solutions that transparently ranks the BW solutions according to several objective and trusted criteria.

TBW-RAnk is built using three AI models, namely the random forest classifier (RFC), the support vector classifier (SVC) and deep neural network (DNN). It has two modes: general and customized for a comprehensive and accurate assessment and recommendation for BW users. Consequently, BW users can make informed decisions and increase their security within the blockchain ecosystem. The proposed approach enhances the security and trustworthiness of BWs and increases their acceptance in the market.

Publications

Journal Papers

1. Almadani, M. S., Alotaibi, S., Alsobhi, H., Hussain, O. K., & Hussain, F. K. (2023). Blockchain-based multi-factor authentication: A systematic literature review. Internet of Things. (Published)

2. A secure and trustworthy blockchain-based wallet framework: A systematic literature review. (Under Review - submitted to Knowledge-Based Systems)

3. A Trustworthy Ranking System for Blockchain-Based Wallets Using AI Algorithms. (Under Review - submitted to Future Generation Computer Systems)

Conference Papers

1. Almadani, M. S., & Hussain, F. K. (2023, November). Implementing a Secure Blockchain-Based Wallet System with Multi-Factor Authentication. InIEEE International Conference on E-Business Engineering (pp. 23-30). IEEE. (Published)

2. Alsobhi, H., Mirdad, A., Alotaibi, S., Almadani, M., Alanazi, I., Alalyan, M., ... & Hussain, F. K. (2021, May). Innovative Blockchain-Based Applications-State of the Art and Future Directions. In International Conference on Advanced Information Networking and Applications (pp. 323-335). Cham: Springer International Publishing. (Published)

Abbreviations

2FA: Two Factor Authentication

AI: Artificial Intelligence

ASR: Attack Success Rate

BW: Blockchain-based Wallet

BWs: Blockchain-based Wallets

BWW: BW Website

DLT: Distributed Ledger Technology

DNN: Deep Neural Network

DSRM: Design Science Research Methodology

LS: Level of Security

MFA: Multi-Factor Authentication

ML: Machine Learning

OTPs: One Time Passwords

RFC: Random Forest Classifier

SLR: Systematic Literature Review

STBWF: Secure and Trustworthy Blockchain Wallet Framework

SVC: Support Vector Classifier

TBW-RAnk: Trust-based Ranking of BW Solution

TOTP: Time-based One Time Passwords

بسم الله الرحمن الرحيم
اقرأ باسم ربك الذي خلق
خلق الإنسان من علق

Table of Contents

List of Figures

FIGURE Page

List of Tables

CHAPTER

1 Introduction

1.1 Thesis Background

Blockchain networks, such as Bitcoin and Ethereum, continue to develop as a widely used medium for money transfer, alongside an accompanying ecosystem and community support. Bitcoin, introduced in 2008 by Nakamoto, was the first practical application of blockchain technology[1]. It is a payment medium based on cryptography mechanisms that guarantee the security of transactions among participants within the network where the ownership and security of assets are validated by public-key cryptography mechanisms. The public keys represent the asset's address, while the private keys are used for the unique authentication of asset ownership. In addition, the cryptocurrency system requires blockchain-based wallets to send and receive cryptocurrencies within the network. Blockchain-based wallets are software or devices containing no currency, but keychains which include private keys, with each key correlated with a public key address [2]. Cryptocurrencies such as Bitcoin, Ether, and Ripple are recorded in ledgers as transactions and managed by signing transactions with the private keys deposited in blockchain-based wallets to verify ownership[3]. The development of distributed applications that eliminate the need for intermediaries such as third parties and central authorities has revolutionized various businesses and organizations.

The most significant issue with blockchain-based wallets is that they hold the users' private keys, thus they are potential targets for cyber attacks. If an intruder gains possession of a private key, they will be able to control the compromised wallet's cryptocurrencies. Hence, the private key is a critical wallet component since it can be used to transmit cryptocurrencies in the wallet to another entity. It should be kept safe and stable to prevent loss and theft. Deciding on the most appropriate and secure blockchain-based wallet is critical when joining the blockchain network as hundreds of cryptocurrency wallet applications and services are available to the public. Although conventional infrastructure-level security techniques are essential to enhance the structure's foundational security, no encryption level or access control can determine the trustworthiness of BW applications and services within the community.

The aforementioned issues drive the critical need for a new generation of security mechanisms. These mechanisms integrate hard security techniques [4] like effective access control and soft security measures [5] aimed at building system trustworthiness. There is a growing demand for studies where procedures are provided to make private keys secure and trustworthy so that blockchain-based wallets are reliable and consistent. BWs can be enhanced by integrating hard and soft security measures. Hard security provides tangible defences against threats, while soft security mitigates the risks arising from misconduct, inadequate knowledge, or emerging threats. Combining both aspects guarantees that wallet security is not solely determined by one aspect and addresses a wide range of security issues. The implementation of hard security measures, including powerful authentication techniques, will significantly strengthen the access control mechanisms of BWs and reduce unauthorized access. Also, BWs will be considerably more trustworthy if a trust or ranking system is introduced as a soft security measure. This will result in improved intelligent decisions and the increased adoption of trustworthy BWs within the blockchain community.

The purpose of this thesis is to investigate the integration of ”hard security” and ”soft security” measures in the context of blockchain-based wallets. By understanding and incorporating tangible physical defences (hard security) with intangible procedural strategies (soft security), we present a comprehensive framework for enhancing BW security and trustworthiness. Through rigorous analysis and exploration, this research demonstrates that the systematic integration of both hard and soft security mechanisms can significantly improve the security of BW applications, services and solutions, protecting them against various threats, from sophisticated cyber-attacks to human-induced vulnerabilities.

1.1.1 Blockchain Technology

Blockchain technology is a decentralized network of systems or nodes that allows multiple parties to record and preserve a sequence of transactions in a secure, reliable, and transparent manner. It is based on distributed ledger technology (DLT:), where transactions are continuously verified by a network of participants called miners. Once recorded and sufficiently confirmed, these transactions become resistant to unauthorized alterations due to the combined characteristics of cryptographic security and the distributed nature of the ledger. All network miners adhere to the same consensus protocols, preventing any single entity from controlling the underlying infrastructure, exerting administrative pressures, or interfering with blockchain transactions [6]. The expansion of blockchain technology has significantly transcended its initial association with Bitcoin and Ethereum. Various other blockchain networks have emerged, each characterized by distinct features and specific applications. These networks are designed to accommodate particular requirements. For instance, Monero [7] and Zcash [8] have been developed with a strong emphasis on privacy in transactions, offering enhanced anonymity. On the other hand, enterprise-level blockchain solutions such as Hyperledger Fabric [9] and Corda [10] are designed to address the sophisticated needs of businesses, providing robust and scalable platforms. Furthermore, Polkadot [11] and Cosmos [12] focus on interoperability, facilitating seamless communication and exchange between blockchain networks. This interoperability is crucial for creating a more connected and efficient blockchain ecosystem where cryptocurrencies and valuable assets can be transferred across diverse networks without barriers. Blockchain technology's key characteristics have been adapted and enhanced in the aforementioned networks, making it highly innovative and transformative. These essential features are outlined below:

1.1.1.1 Decentralization and Transparency:

In contrast to centralized networks, blockchains operate as distributed networks comprising numerous nodes. This decentralized structure, where no single entity exercises control over the entire network, significantly enhances the network's resilience and reduces its vulnerability to control by centralized authorities. Each node in the network holds an exact copy of the digital ledger, ensuring a high level of transparency. In other words, on public digital ledgers, all transactions are transparent and verifiable by any entity within the network, reducing the risk of fraud and preventing disputes. In addition, transparency provides enhanced traceability and auditability, making transaction tracking and verification highly effective [13].

1.1.1.2 Security and Immutability:

Blockchain consists of records of transactions, known as blocks, linked by cryptographic algorithms. Each block contains a hash of the previous block, a timestamp, and transaction data. As every block is connected to the previous one to ensure the integrity of the blockchain, manipulating one block affects all other blocks. The timestamp prevents the block data from being altered without detection, and the hash connects the blocks, forming a secure chain. This makes blockchains a trustworthy, reliable, and immutable technology[14].

1.1.1.3 Tokenization and Digital Assets:

Blockchain can be used to create tokens and digital assets. In addition to cryptocurrencies, tokens can represent real-world assets, access rights, utilities, and ownership rights. A key development of tokenization is initial coin offerings, which opens up new opportunities for asset management, crowdfunding, and decentralized finance[15].

1.1.1.4 Consensus Mechanisms:

Blockchain technology utilizes a variety of consensus mechanisms to achieve agreement among distributed nodes on the ledger's state. Proof of Work (PoW) in Bitcoin requires solving complex mathematical puzzles, which consume significant computational resources. Alternatively, Proof of Stake (PoS) allows token holders to contribute to block validation based on their stake amount. In Delegated Proof of Stake (DPoS) and Proof of Authority (PoA), a select group of predefined trusted entities are given validation responsibilities. Also, validators must commit disk space or burn some of their tokens to earn validation rights under Proof of Space (PoSpace) and Proof of Burn (PoB). It is common for permissioned networks to employ Proof of Elapsed Time (PoET), which involves selecting validators based on a fair, random process of waiting. Proof of Activity (PoA) combines Proof of Whale and Proof of Stake into a hybrid approach. In contrast, Proof of Capacity (PoC) and Proof of History (PoH) focus on the validators' ability to store and maintain data. Unique mechanisms, such as Proof of Importance and Proof of Stake Velocity, consider transaction frequency and coin age factors. Through Leased Proof of Stake (LPoS), validators can lease coins, enhancing participation in the network. Furthermore, private blockchains utilize Byzantine fault tolerance, which involves a group of trusted nodes. As an alternative to traditional blockchains, directed acyclic graphs (DAGs) allow transactions to be linked directly without requiring a block. Security, speed, and decentralization are all balanced differently by each mechanism, influencing their suitability for different blockchain applications [16].

1.1.1.5 Scalability:

Blockchain network scalability refers to its ability to handle increasing transactions without performance degradation or compromising security. Additionally, it addresses the issue of ensuring high transaction responsiveness levels, regardless of the network's size or demand level. In particular, scalability is essential since traditional blockchain networks, such as Bitcoin or Ethereum, face limitations in terms of their capacity to process transactions and their ability to scale. These networks experience congestion and slower transaction confirmations during periods of high demand. A key feature of blockchain is its scalability since its widespread adoption and real-world applications depend on its ability to handle numerous users and transactions [17].

1.1.2 Blockchain-based Wallets (BW:/BWs:)

The cryptocurrency system requires blockchain-based wallets (BWs) to send and receive cryptocurrencies, digital assets and tokens within the network. The BW solutions provide applications and services that facilitate secure interaction between the BW users and the blockchain network. A BW contains private keys cryptographically associated with public key addresses. [18]. The public keys represent the digital asset's address, while the private keys are used to prove digital asset ownership. Blockchain networks maintain an immutable record of digital assets and cryptocurrencies as transactions on distributed ledgers. Hence, the primary difference between a blockchain-based and a traditional digital wallet is that a single authority does not manage the BW, and it operates on a distributed network rather than a centralized network (see Figure 1.1). In contrast, a traditional digital wallet is controlled by a central authority and enables customers to conduct electronic transactions while storing monetary value in compliance with financial regulations.

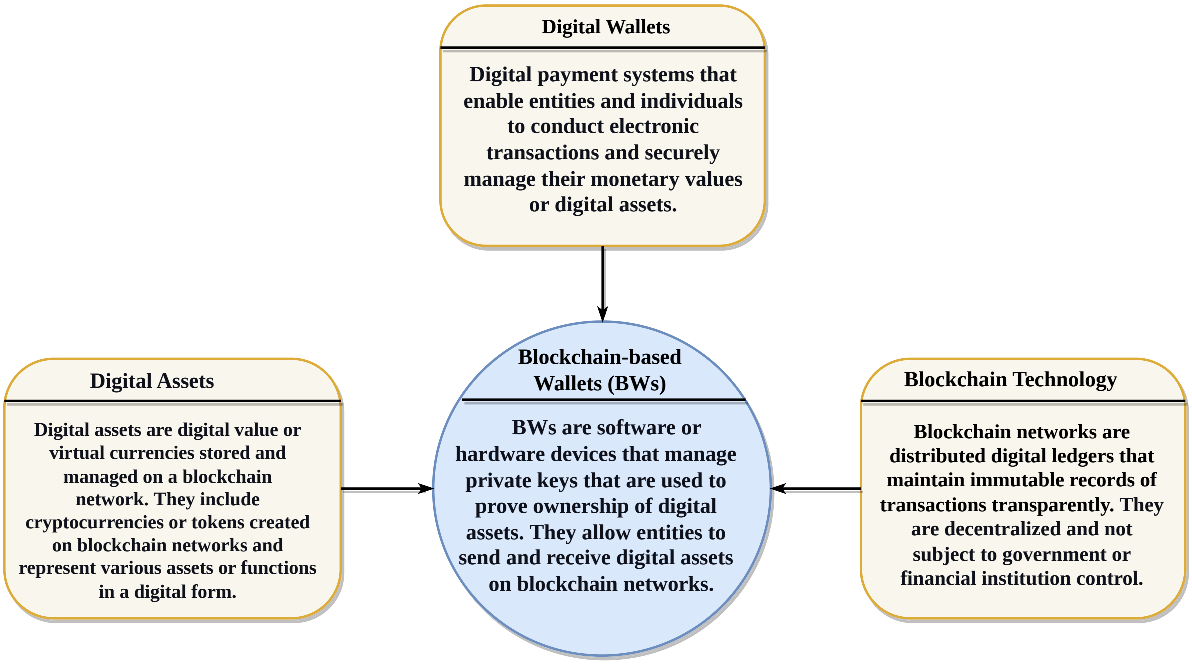

Digital Wallets
Digital payment systems that enable entities and individuals to conduct electronic transactions and securely manage their monetary values or digital assets.
Digital Assets
Digital assets are digital value or virtual currencies stored and managed on a blockchain network. They include cryptocurrencies or tokens created on blockchain networks and represent various assets or functions in a digital form.
Blockchain-based Wallets (BWs)
BWs are software or hardware devices that manage private keys that are used to prove ownership of digital assets. They allow entities to send and receive digital assets on blockchain networks.
Blockchain Technology
Blockchain networks are distributed digital ledgers that maintain immutable records of transactions transparently. They are decentralized and not subject to government or financial institution control.

Figure 1.1: The primary differences between a blockchain-based wallet and a digital wallet

BWs vary in the way private keys are stored and controlled, namely in software, hardware, and paper wallet form. In hardware wallets, a user's private key is stored offline on a hardware device like a Universal Serial Bus thumb drive or a small flash drive. In paper wallets, the private key is generated by software and is stored offline in a physical copy or printout form. A software wallet is an application downloaded and installed on a platform such as a PC and a mobile phone, and the user's private keys are available in a local file [19]. Several factors can differentiate BW types, including wallet functionality, custody, connectivity, and platform, as shown in Figure 1.2. BW functionality is the set of features a wallet provides its users. A basic wallet manages transactions for one type of cryptocurrency, such as BTC, while multi-currency wallets offer enhanced functionality by supporting multiple cryptocurrencies, such as Ethereum (ETH), Ripple (XRP) and Litecoin (LTC). In contrast, web3 wallets like MetaMask [1] have advanced features that enable them to interact with Web3.0, execute smart contracts and access various decentralized applications. Furthermore, a wallet's custody is determined by who controls its private keys. It can be categorized into custodial wallets controlled by a third party, such as a cryptocurrency exchange or wallet service, and non-custodial wallets owned by users. Wallet connectivity refers to whether the wallet is connected or disconnected from the Internet, which includes hot wallets, which are connected to the Internet for convenient transactions, and cold wallets, which are disconnected from the Internet. The wallet platform refers to the device or environment where the wallet is installed or accessed. Web wallets can be accessed from any device with an internet connection, whereas mobile wallets are software downloaded on a smartphone or tablet. Desktop wallets are software applications installed on a computer, while hardware wallets are physical devices that access private keys offline, like a USB stick [20].

The BW framework module integrates sophisticated authentication, verification, and access control mechanisms. These components are crucial in enabling the secure exchange, deposit, and withdrawal of cryptocurrencies and tokens. Authentication ensures that only authorized users can access the wallet, verification confirms the integrity and legitimacy of transactions, and access control governs what actions each authenticated user can perform. Collectively, these techniques provide a robust security framework essential for safely handling digital assets within the blockchain environment. Figure 1.3 illustrates the steps in making a transaction using BWs. In the initial phase, when creating BWs, private keys are automatically generated by a cryptographically secure pseudo-random number generator (CSPRNG). Private keys are then applied to derive the corresponding public keys. Public keys are publicly available for entities within the blockchain network to verify transactions. In the second step, the public key's hash and specific encoding schemes are used to generate a unique identifier, known as a wallet address, which facilitates cryptocurrency and digital asset transactions between individuals and entities. Finally, private keys are utilized to create a digital signature by using the elliptic curve digital signature algorithm (ECDSA) and attaching it to the transaction. Digital signatures are associated with the transaction and can be verified by the public keys to confirm and authenticate

[1] https://metamask.io/

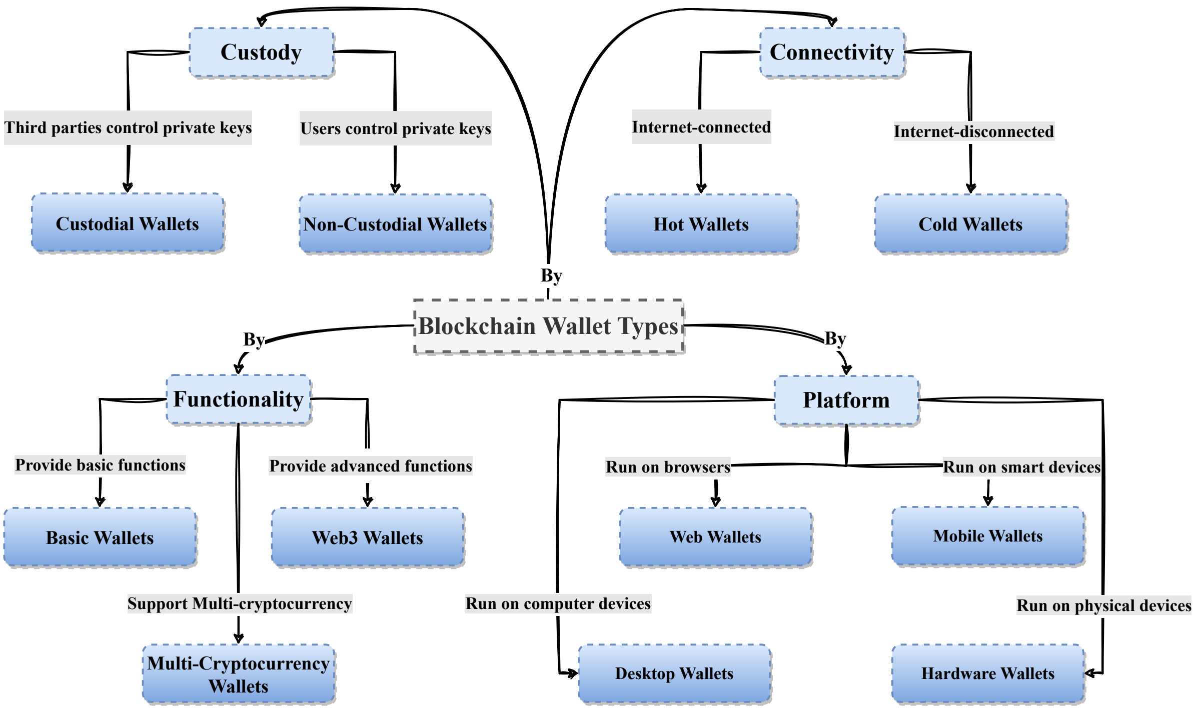
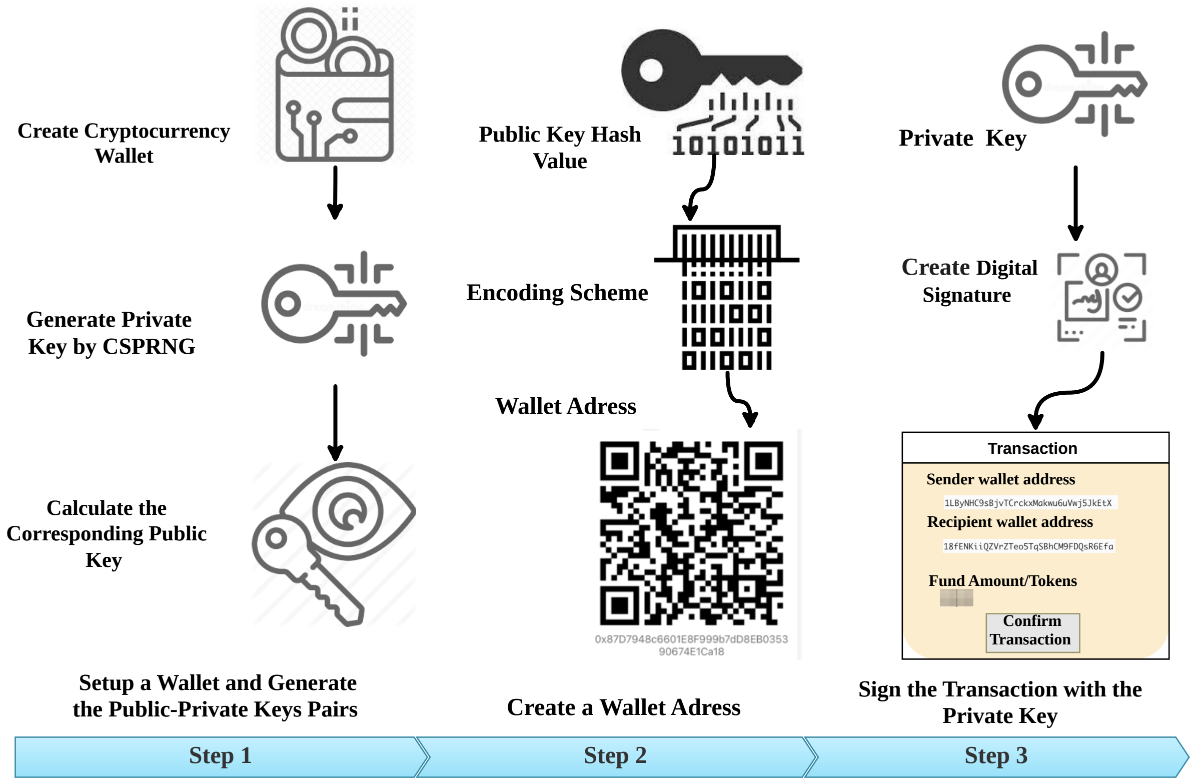


Figure 1.2: BW types

the transaction. Miners and validators on the blockchain network use the digital signature to verify that the transaction is authentic and has not been tampered with. The transaction is added to the blockchain if the signature is valid, and the cryptocurrency or digital asset is transferred to the recipient's wallet address. Thus, when a cryptocurrency is sent, the individuals who make the transaction essentially sign off on the digital assets' ownership to a wallet address [21]. The previous process guarantees that only the wallet owners, who control the unique private key, can initiate and approve transactions related to their wallets.


Create Cryptocurrency Wallet
Generate Private Key by CSPRNG
Calculate the Corresponding Public Key
Setup a Wallet and Generate the Public-Private Keys Pairs
Public Key Hash Value
10101011
Encoding Scheme
Wallet Adress
0x87D7948c6601E8F999b7dD8EB0353 90674E1Ca18
Create a Wallet Adress
Private Key
Create Digital Signature
Sign the Transaction with the Private Key
Step 1
Step 2
Step 3

Transaction

Sender wallet address

1LByNHC9sBjvTCrckxMakwu6uVwj5JkEtX

Recipient wallet address

18fENKiiQZVrZTeo5TqSBhCM9FDQsR6Efa

Fund Amount/Tokens

Confirm Transaction

Figure 1.3: The steps in making transactions using BWs

1.2 Statement of the Problem

Blockchain-based wallets are based on a fundamental principle: the ownership and secrecy of private keys, where cryptocurrency ownership is linked to wallet addresses. However, the associated private keys determine control and access to those cryptocurrencies. Therefore, it becomes imperative to ensure the security of these private keys. There is a growing demand for studies where procedures are provided to make private keys secure and trustworthy so that blockchain-based wallet applications and services are reliable and consistent. Managing and storing cryptocurrencies and digital assets securely is one of the critical requirements for blockchain-based wallets. Despite the growing value of these assets, the evolving cyber threat landscape raises concerns about their security and trustworthiness. One of the solutions to these challenges is integrating hard and soft security mechanisms. A hard security mechanism involves cryptographic techniques and hardware-based protection, while a soft security mechanism involves behavioral analysis, artificial intelligence, and user-centric security. Several studies have emphasized the importance of implementing robust security for BWs, such as authentication techniques, access controls, digital signatures and key management. However, despite the critical role that private keys play in the security of BWs, current research has yet to fully investigate how hard and soft security measures can be combined to reduce the risk of attacks against blockchain-based wallets and protect digital assets. Moreover, one of the fundamental weaknesses of existing BW approaches is how to efficiently implement these security measures.

1.2.1 Thesis Scope

This thesis examines the dynamic relationship between hard and soft security mechanisms in the context of blockchain-based wallets. It assesses the effectiveness of integrating these mechanisms to create enhanced and reliable BW platforms. By investigating the complementary effects of hard and soft security approaches, this thesis contributes to the understanding of how BWs can enhance security against a wide range of threats by implementing advanced intelligent defence features to build user trust.

1.2.2 Stakeholders

This thesis will assist a diverse group of stakeholders such as the BW owner who seeks secure storage, seamless transactions, and assurance that their assets are secure and the wallet developer or engineer who aims to create user-friendly, robust, and trustworthy BW applications and services. Blockchain projects and foundations that seek to develop secure wallets for their specific cryptocurrency increase trust and facilitate adoption. Additionally, the blockchain community drives public awareness of secure wallet practices, addressing concerns and shaping the future of wallet functionality and security measures. Academic researchers on blockchain and security will also be introduced to some open challenges worth exploring in the future.

1.3 Current challenges faced by blockchain-based wallets

Several researchers have highlighted the importance of robust security measures for cryptocurrency wallets in the rapidly advancing field of digital currencies. Despite this, the current security aspects of BWs face many challenges, as described in the literature:

1.3.1 Private Key Concerns:

This challenge relates to the complicated relationship between advanced technology and user responsibility in the context of digital assets. It is imperative to note that, despite the robust security features inherent in blockchain technology, BWs specifically designed for storing and transacting cryptocurrencies and tokens are vulnerable due to private key security and management issues [22]. The security of BWs is primarily determined by the confidentiality and management of their private keys. Private keys are the foundation of asset control and user identification within a blockchain network. The wallet and its contents may be compromised if the key is lost, forgotten, or stolen. Although users have sovereignty over their assets, they also have a critical responsibility concerning the management of their private keys. As a result, there are two main issues: the lack of a safe and efficient way to manage private keys and the inability to promptly prevent unauthorized access to private keys [23].

1.3.2 Hard Security Concerns:

Hard security methods in BWs are critical for defending digital assets against various cyber threats. While the nature of blockchain brings innovative security considerations, a comprehensive defence system provides a strong foundation for maintaining wallet security and user trust [24]. It focuses on conventional, well-established security practices such as authentication techniques, access control and encryption algorithms. Nonetheless, challenges are associated with a prevalent form of cyber threat, which targets the human element in security. Deception is often carried out by meticulously crafted emails or websites that imitate legitimate sources, resulting in even the most diligent users to compromise their credentials. Inexperienced users may be unable to identify signs of phishing attempts or the risks of using unverified wallet software [25]. A lack of awareness creates a significant security challenge, making the user the weakest security element. Without a comprehensive, layered defence approach, relying solely on single security measures, such as strong passwords or basic MFA, leaves room for sophisticated cyber threats to succeed [26].

1.3.3 Soft Security Concerns:

Without a trusted soft security measure for BWs, users face considerable challenges that may complicate their experience and compromise their cryptocurrencies and digital assists [27]. The most problematic of these difficulties is evaluating the trustworthiness, security and reliability of different wallet applications and services. This can be challenging for those new to the world of cryptocurrencies. The lack of clear, objective guidance significantly increases the risk of users falling victim to scams or fraudulent BW developers. The cryptocurrency market offers various BW solution options, each offering security assurances and features. Choosing a BW solution can often be an overwhelming and uncertain process for BW users. Consequently, it is challenging for individuals or entities to identify a BW that meets their requirements, is secure against cyber attacks and meets their risk tolerance[28].

1.4 Thesis Motivations

The rapid development of blockchain technology and its subsequent adoption across numerous industries has demonstrated the considerable potential of decentralized systems [29]. The BW, however, is the cornerstone of this technological revolution, which ensures that users can access and manage their digital assets securely. The blockchain ecosystem faces a number of challenges and threats as it continues to grow. Several incidents have resulted in compromised wallets, stolen assets, and users being locked out of their funds, raising doubts and concerns about the technology's adequate security measures [30]. It is imperative to understand BW security in depth because billions of dollars worth of assets are at stake, as well as individual financial sovereignty. This thesis is motivated by a profound sense of urgency to strengthen BWs, protecting them against emerging threats.

Furthermore, a significant improvement in BW security can be achieved by integrating hard and soft security mechanisms. Combining the strengths of traditional defences and soft security strategies can provide a more robust and comprehensive security framework [31]. Thus, cryptocurrency wallets must be enhanced in terms of security and trustworthiness, making them more resilient to a wide range of cyber threats and vulnerabilities. To enhance the hard security of BWs, robust security measures must be implemented. Hence, providing a more comprehensive defence against a wide range of cyber threats can be achieved by integrating diverse authentication factors where each factor has distinct strengths and weaknesses. This is where MFA plays a crucial role, as it adds an additional layer of protection, making it more difficult for attackers to compromise wallets [32].

There is a wide variety of BW applications and services in the rapidly evolving blockchain landscape, each claiming high levels of security and usability. However, the absence of a standardized, trustworthy method for evaluating these claims poses a significant risk[33]. Thus, users may make uninformed decisions, compromising their digital assets and personal security. To address this issue, this study develops a trust-based ranking system for BWs. This solution provides an effective and reliable platform that systematically assesses and ranks wallet applications and services according to various trust and security criteria. It achieves two purposes: first, to empower users with the knowledge to make informed decisions about which wallet services to trust and utilize, and second, to encourage BW applications and service providers to adhere to the highest standards of safety and security.

1.5 Thesis Significance

The motivation section (1.4) discusses the importance of robust security measures for cryptocurrency wallets since they ensure users can access, manage, and store valuable digital assets securely. Furthermore, the challenges section (1.3) explains the challenges BWs face regarding private keys, soft and hard security measures. This section details the innovative solutions and crucial results of this thesis and demonstrates how the proposed approach not only addresses the challenges associated with the security of BWs but also has significant implications for the blockchain community.

1.5.1 Scientific Significance of the Thesis

a) This is the first research that integrates soft and hard security measures for BW solutions.

b) This is the first research that develops an AI-driven trust-based ranking model for BW solutions.

c) This is the first research that enables BW users to personalize the ranking based on their needs.

d) This is the first research that evaluates and quantifies 2FA and MFA with TOTP and biometric factors as a hard measure for securing BW solutions.

1.5.2 Social Significance of the Thesis

a) The proposed approach empowers BW developers to build BW solutions with enhanced security and greater resilience to attacks, thus fostering trust among the BW community and encouraging wider adoption.

b) The proposed approach utilizes objective criteria and transparent implementation that highlights the strengths and weaknesses of different BW solutions. Thus, it motivates developers to continuously improve their products, benefiting BW users through sophisticated features and services.

c) The proposed approach can educate BW users about important features and how different security measures protect their assets to make informed decisions on the appropriate BW solutions. This knowledge is invaluable in a complex and intimidating landscape for newcomers.

1.6 Structure of the Thesis

This thesis proposes a comprehensive approach for securing BW solutions by integrating soft and hard security mechanisms. It comprises eight chapters that present the proposed methodologies for achieving the thesis objectives (3.4), as shown in Figure 1.4. The chapters are organized as follows:

- **Chapter 1:** This chapter provides a comprehensive overview of blockchain technology focusing on the security and trustworthiness of BW solutions. It also defines the problem statement and discusses the challenges associated with BW solutions, particularly the issues surrounding private keys and the distinction between hard and soft security concerns. Furthermore, the thesis motivations and significance are discussed.
- **Chapter 2:** This chapter presents an SLR and a categorical analysis of the research topic to provide a comprehensive overview of the existing literature on BWs and the current security challenges. This helps to identify the gaps in the literature and provides a framework for designing the proposed methodologies.
- **Chapter 3:** This chapter provides an overview of the key terms used throughout the thesis. The chapter also outlines the research objectives and questions.
- **Chapter 4:** This chapter defines the methodology adopted to address the gaps highlighted in the literature review. It also elaborates on the proposed solutions for achieving the research objectives. In particular, the design science research methodology is applied to achieve the research objectives.
- **Chapter 5:** This chapter provides a detailed illustration and description of the proposed framework to achieve Objective 1, namely to develop a secure, intelligent and trustworthy framework to enhance the security and trustworthiness of BW solutions.
- **Chapter 6:** This chapter presents the solution to research Objective 2. It proposes a BW website that provides a secure platform for users to manage and control their cryptographic keys and digital assets effectively. A key design process component is to develop a detailed system model that incorporates four authentication settings, including 2FA and MFA. Also, the authentication setting's effectiveness is evaluated and quantified using attack simulations against BW accounts.

- **Chapter 7:** This chapter presents the solution to research Objective 3. It details the implementation of a trust-based ranking system using deep learning algorithms to help users make informed decisions about the trustworthiness of BW applications and services.
- **Chapter 8:** This chapter presents the conclusion, outlines the contributions of this thesis and provides recommendations for further research.

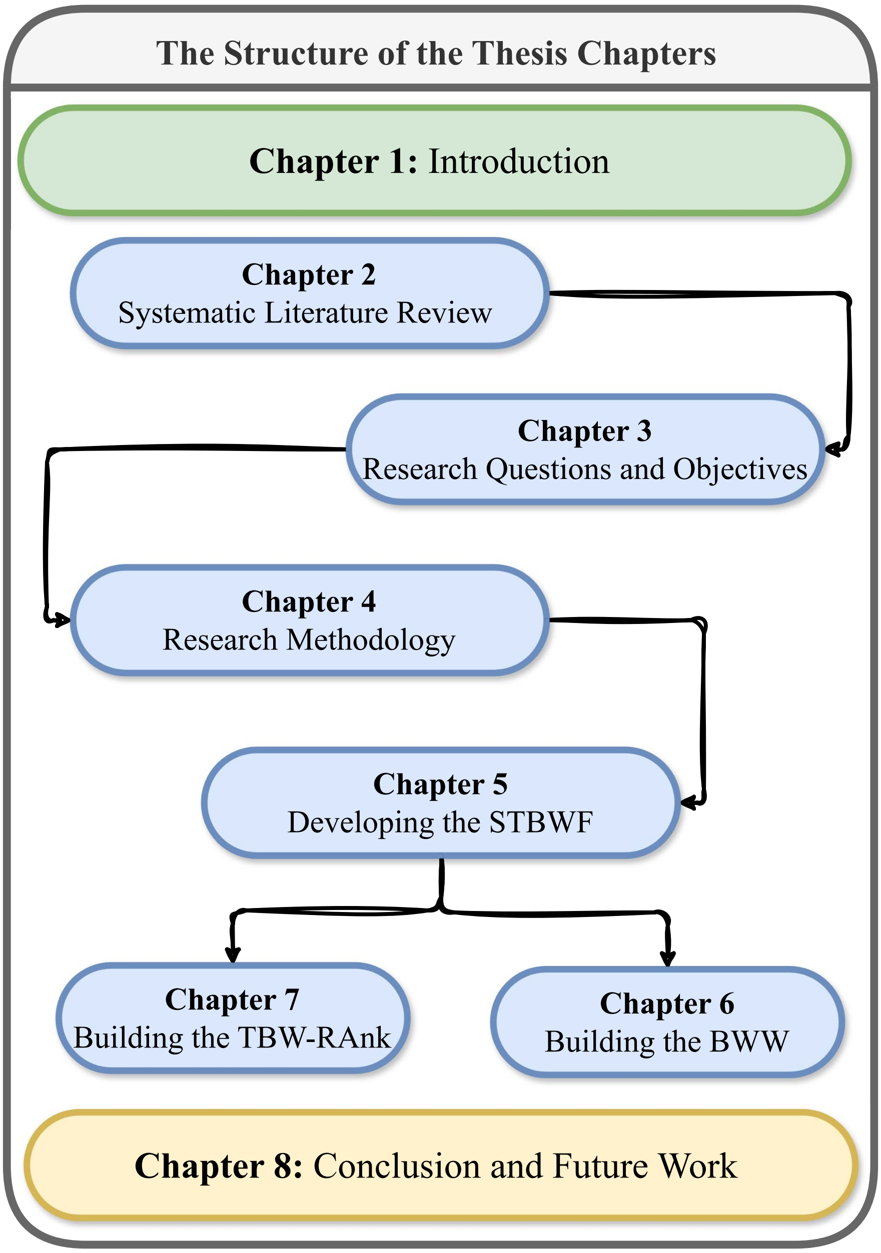


Figure 1.4: The thesis chapters

CHAPTER

2

A Systematic Literature Review (SLR:)

2.1 Chapter Overview

Chapter 1 highlighted the importance of BW solutions in the context of blockchain networks. Also, it identified the problem statement and discussed the challenges associated with BW solutions, including private keys and the relationship between hard and soft security issues. The significance and motivations of the thesis were also presented. This chapter reports on a systematic literature review (SLR) which was conducted to understand, analyze, and identify the gaps in the current literature on BW security and trustworthiness.

The structure of the chapter is as follows. Section 2.2 introduces the five key requirements that improve the security and trustworthiness of BW solutions. Section 2.3 describes and discusses the approach adopted to shortlist the papers for this SLR. Section 2.4 introduces a categorical analysis of all the peer-reviewed papers that were shortlisted, a total of 40. Section 2.5 discusses the research gaps in the current studies from the standpoint of the security and trustworthiness requirements associated with BW solutions. Finally, Section 2.6 summarizes the SLR.

2.2 Key Requirements for a Secure and Trustworthy BW Solutions Framework

This section discusses the requirements which need to be considered to enhance BW security and trustworthiness. These requirements form the basis for comparing the papers selected for this SLR. Due to the vast number of BW solutions offered in the market and the customers' need for efficiency and security, wallet developers have created various ways to improve their solutions. But, at the same time, they must adhere to particular requirements that ensure the security, trustworthiness and functionality of their developed BWs. As shown in Figure 2.1, these requirements are as follows:

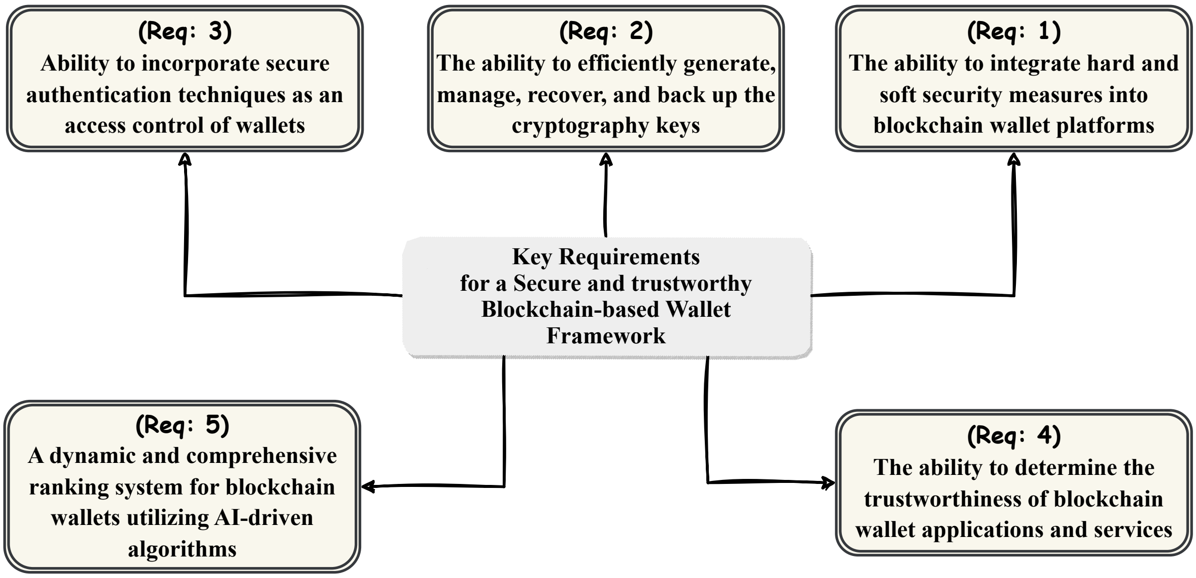

(Req: 3)
Ability to incorporate secure authentication techniques as an access control of wallets
(Req: 2)
The ability to efficiently generate, manage, recover, and back up the cryptography keys
(Req: 1)
The ability to integrate hard and soft security measures into blockchain wallet platforms
Key Requirements for a Secure and trustworthy Blockchain-based Wallet Framework
(Req: 5)
A dynamic and comprehensive ranking system for blockchain wallets utilizing AI-driven algorithms
(Req: 4)
The ability to determine the trustworthiness of blockchain wallet applications and services

Figure 2.1: Key requirements for blockchain-based wallets

2.2.1 The ability to integrate hard and soft security measures into BW platforms (Req: 1)

A hard security measure relies on conventional and well-established security techniques, such as authentication, access control, and encryption algorithms. In contrast, a soft security measure employs behavioural analysis, artificial intelligence, and user-centric security strategies. Combining the strengths of hard security defences and soft security strategies provides a comprehensive, secure and trustworthy framework for BW solutions [4], [5]. By combining both characteristics, wallet security is not solely determined by one aspect and can address many security concerns. By implementing hard security measures, including effective authentication techniques, blockchain wallets can significantly strengthen access control mechanisms and reduce the likelihood of unauthorized access. Also, BW solutions can be considerably trustworthy if a trust system is introduced as a soft security measure. This will result in improved intelligent decisions and the increased adoption of trustworthy wallets within the blockchain community.

2.2.2 The ability to efficiently generate, manage, recover, and back up the cryptography keys (Req: 2)

BW solutions are responsible for assisting entities and individuals to manage and secure their private keys [34]. To this end, key management techniques are one of the crucial factors in implementing cryptocurrency wallets. Key management in BWs involves generating, storing, and backing up cryptographic keys. Blockchain technology is built on public-key cryptography and users have to sign transactions digitally to demonstrate that they own their assets. Since the elliptic curve digital signature algorithm secures blockchain transactions, private keys are imperative to secure the entities' assets. Thus, wallet key management is a salient aspect of the blockchain network's reliability because losing private keys means losing funds. Various crypto wallets use different storage techniques and operate on different digital platforms. The chosen platform or terminal (including a computer or mobile phone) and the data storage mechanism can significantly impact the security of the wallet's private keys [35]. In addition, how private keys are generated is another important issue. The early BWs generated a set of sufficient random private keys when the system was initialized and each private key was only used once. This method of generating keys requires more storage space and sophisticated key management techniques. Thus, early wallets have gradually been replaced by deterministic wallets that generate private keys from a random seed. The deterministic wallets create a backup at the beginning of the initialization process, therefore the seed is enough to recover all the private keys, which reduces the complexity of key management [36].

Moreover, recovery mechanisms are needed to securely re-establish access credentials by entities that have lost their private keys after hardware failure or natural disasters. The backup and recovery mechanism in existing BWs is a significant issue, as most rely on a word list (mnemonics) to back up private keys and restore them when necessary [37]. The recovery mechanisms ensure that missing or attacked private keys can be recovered with a high degree of certainty. Some vulnerabilities in the existing backup solution, such as the paper backup method, may be exploited by a malicious party to hack the system, recover the private keys, and steal the funds. Thus, choosing reliable recovery mechanisms that can withstand common attacks during the recovery process is essential.

2.2.3 The ability to incorporate secure authentication techniques as an access control of wallets (Req: 3)

Blockchain technology employs traditional cryptographic algorithms and schemes for consensus and transaction verification, such as hash functions and digital signatures. However, these technologies do not satisfy security requirements in a complex business environment or prevent potential future threats. Hence, the requirements for BW security not only include primary security elements such as tamper resistance, trade dispute resistance, and trustworthiness, they also require better authentication techniques [38]. The traditional wallet system, which only authenticates individuals by passwords, is not secure and is vulnerable to many attacks. Therefore, these wallet systems require a stronger authentication method, particularly for platforms that are more vulnerable to attacks, such as mobile wallets. The most popular technique for protecting BWs is the attribute-based authentication method, even though passwords are vulnerable to various threats and could be compromised. Designing a reliable authentication protocol could resolve security flaws or performance issues in BWs, as most of these vulnerabilities will be addressed when using a secure user authentication protocol, potentially avoiding major economic losses. Thus, it is desirable to provide authentication protocols tailored to the various blockchain network environments to securely store private keys [39].

2.2.4 The ability to determine the trustworthiness of BW solutions (Req: 4)

Applications and services manage billions of dollars of digital assets and cryptocurrencies, allowing users to connect with the blockchain network [40]. A wide range of BW solutions have emerged in the rapidly evolving blockchain landscape, each claiming high levels of security and trustworthiness. However, the absence of a standardized, trustworthy method for evaluating these claims poses significant risks. Thus, users may make uninformed decisions, compromising their digital assets and personal security. Therefore, it is imperative to implement a trust-based ranking system for applications and services to allow users to differentiate between reliable platforms and potential threats [41]. A trust-based ranking system empowers users to make informed decisions about the trustworthiness of BW solutions, such as their security measures, wallet features, and regulatory compliance. This knowledge will help users make an informed decision about which platform to trust with their valuable digital assets and cryptocurrencies.

2.2.5 A dynamic and comprehensive ranking system for blockchain wallets utilizing AI-driven algorithms (Req: 5)

With the rapid evolution of blockchain technology, ranking wallet applications and services presents a unique challenge due to their inherent complexity and diverse user behavior. Various ranking systems may prioritize different factors, resulting in variations in the rankings assigned to entities based on their methodologies, criteria, and accuracy [42]. Understanding the methodology and limitations of a ranking system is essential when interpreting or utilizing its results. For example, mathematical models are straightforward and easier to understand when ranking criteria are well-defined. However, their fixed structure might limit adaptability, potentially leading to less accurate rankings as blockchain technologies and user behaviors evolve [43]. The current trustworthiness of applications and services needs to be calculated using an intelligent AI model that predicts the value of trust based on specific criteria. By incorporating AI models, it is possible to evaluate applications and services in a dynamic, adaptable, and comprehensive manner that is compatible with the unique characteristics and demands of the blockchain ecosystem [44]. Stakeholders can enhance the user experience and trust in the blockchain space by leveraging AI to ensure that rankings reflect current trends and technologies and are personalized to meet diverse user needs. AI algorithms emerge as a particularly effective solution in this context, capable of handling the complex data patterns characteristic of blockchain ecosystems. Their ability to process and interpret a wide range of data, from transaction histories and security features to user ratings, allows for a comprehensive and accurate assessment of wallet applications.

2.3 Methodology adopted for shortlisting papers in the SLR

We conducted an SLR to select and analyze relevant studies. In phase one, the literature is searched to identify the database sources, define the search terms, and collect the data. In phase two, the inclusion and exclusion criteria are determined to facilitate the selection of the most important studies. In phase three, for the articles and studies that are identified, a quality assessment is performed. Finally, in phase four, data analysis is undertaken on all articles that passed the previous phases and their data are collected and recorded. Figure 2.2 summarizes the evaluation and selection steps of the relevant papers for the SLR.

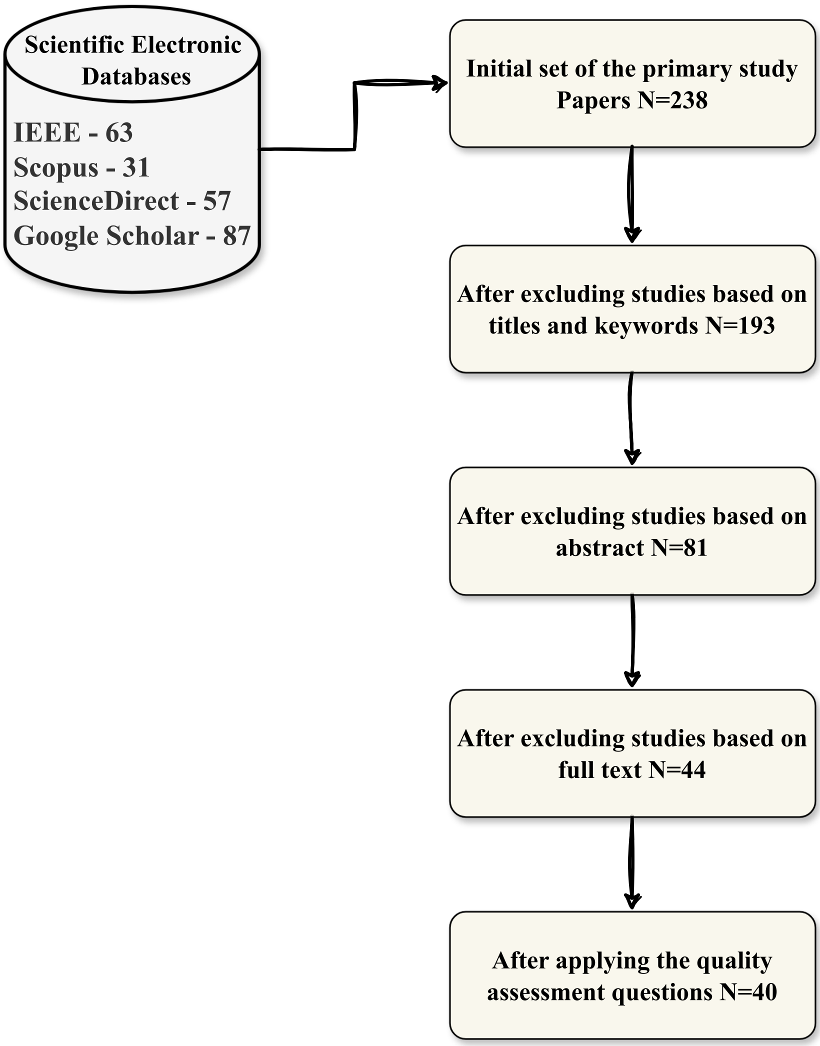

Scientific Electronic Databases
IEEE - 63
Scopus - 31
ScienceDirect - 57
Google Scholar - 87
Initial set of the primary study Papers N=238
After excluding studies based on titles and keywords N=193
After excluding studies based on abstract N=81
After excluding studies based on full text N=44
After applying the quality assessment questions N=40

Figure 2.2: Literature review filtration process.

2.3.1 Phase 1: The literature search criteria

In this phase, the following is determined:

A) Databases Searched:

The following scientific electronic databases were used to identify relevant studies for this SLR:

a) ScienceDirect (www.sciencedirect.com).

b) Scopus (https://www.scopus.com).

c) IEEE Xplore Digital Library (www.ieexplore.ieee.org/Xplore).

d) Google Scholar (https://scholar.google.com).

B) Keywords Used:

Relevant studies were identified by entering the keywords into the search engines. The search terms were used to obtain research outcomes that better address the research questions. A search strategy to obtain the maximum number of relevant studies was adopted. Using the Boolean operator AND, the search statement can be constructed to form a combination of search terms from different categories and the Boolean operator OR using several keywords from the same category. The search terms ”blockchain-based wallet security and trust”, ”cryptocurrency wallet security and trust”, ”Bitcoin wallet security and trust” were inserted in publication databases to generate records and develop the literature data source.

C) Publication date and results:

To be eligible for the SLR, the study must be published between 2016 and 2023 because very little knowledge of blockchain technology was published before 2016. This initial search process resulted in the retrieval of 238 articles. These articles were examined for further inclusion and exclusion filtration.

2.3.2 Phase 2: Inclusion and Exclusion criteria

In the second phase, the following inclusion and exclusion are applied:

1. Inclusion Criteria:

a) The paper must be published between 2016 and 2023.

b) The paper must present empirical data related to the security of blockchain-based, bitcoin, or cryptocurrency wallets.

c) The paper must be published in a peer-reviewed journal or conference proceeding.

2. Exclusion Criteria:

   a) Papers that apply blockchain technology to address application problems or surveys that focus on blockchain-based wallets in general.

   b) Informal articles that are without defined research questions or a specified method of data extraction.

   c) Papers that are duplicate reports or have not been published in English.

3. Paper Selection Procedure:
   In this step, we determine whether an article should be included in the SLR. The filtration process was divided into three stages.

   a) **First stage:** The titles of 238 papers were reviewed and only those papers which contained the search keywords were retained. Papers that weren't clear from the titles or keywords were further evaluated at the next stage. In this stage, the number of papers reduced to 193.

   b) **Second stage:** In this stage, the abstracts were evaluated to determine their relevance to this research. Papers were selected based on their abstracts, which reduced the number of retained articles to 81.

   c) **Third stage:** After reading the full texts of the remaining articles, only 44 were significant for the research.

2.3.3 Phase 3: Quality evaluation

The 44 remaining documents were evaluated based on the following quality assessment questions:

QE1: Does the document report on preliminary studies and discuss the area of the research?

QE2: Does the paper introduce a framework to address the research problem?

QE3: Is the method validated by proof of concept or implementation?

This SLR includes study papers that meet at least two of the three quality assessment criteria. Accordingly, 40 of the 44 studies met the criteria, as shown in Table 2.1. Figure 2.3 shows the study papers in a bar chart according to the year they were published.

Study Number	**QE1**	**QE2**	**QE3**
He, Lin, Li, *et al.* [45]	✓	✗	✓
Rezaeighaleh and Zou [46]	✓	✗	✓
Zhu, Chen, Wang, *et al.* [47]	✓	✓	✗
Liu, Li, Liu, *et al.* [48]	✓	✓	✗
Khan, Zahid, Hussain, *et al.* [49]	✓	✗	✓
Rezaeighaleh and Zou [50]	✓	✗	✓
Homoliak, Breitenbacher, Hujnak, *et al.* [51]	✓	✓	✓
Urien [52]	✓	✗	✗
Benli, Engin, Giousouf, *et al.* [53]	✓	✓	✗
Albakri and Mokbel [54]	✓	✗	✓
Marcedone, Pass, and Shelat [55]	✓	✓	✗
Gennaro, Goldfeder, and Narayanan [56]	✓	✓	✓
Boneh, Gennaro, and Goldfeder [57]	✓	✓	✓
Hu, Liu, Niu, *et al.* [58]	✓	✗	✓
Thota, Upadhyay, Kulkarni, *et al.* [59]	✓	✗	✓
Dai, Deng, Wang, *et al.* [60]	✓	✓	✓
Gentilal, Martins, and Sousa [61]	✓	✗	✓
Wang, Li, Gao, *et al.* [62]	✓	✓	✓
Das, Faust, and Loss [63]	✓	✓	✗
Di Luzio, Francati, and Ateniese [64]	✓	✓	✓
Perry [65]	✓	✗	✗
Praitheeshan, Xin, Pan, *et al.* [66]	✓	✗	✓
Volety, Saini, McGhin, *et al.* [67]	✓	✓	✓
Fan, Tseng, Su, *et al.* [68]	✓	✓	✗
Wang, Gao, and Li [69]	✓	✓	✓
Davenport and Shetty [70]	✓	✗	✓
Yin, Wen, Li, *et al.* [71]	✓	✓	✗
Guri [72]	✓	✓	✗
Gkaniatsou, Arapinis, and Kiayias [73]	✓	✓	✓
Biryukov and Tikhomirov [8]	✓	✗	✗
Dmitrienko, Noack, and Yung [74]	✓	✗	✓
Chan [75]	✓	✗	✓
Li and You [76]	✓	✓	✓
Holmes and Buchanan [77]	✓	✓	✓
Sung [78]	✓	✓	✗
Qi, Xu, Jiao, *et al.* [79]	✓	✓	✓
Zhang, Zou, Xie, *et al.* [80]	✓	✓	✗
Lehto, Halunen, Latvala, *et al.* [81]	✓	✗	✓
Lomazina, Surovtsova, and Ivanov [82]	✓	✗	✓
Jian, Ran, and Liyan [83]	✓	✓	✗
Hu, Wang, Tu, *et al.* [84]	✓	✓	✓
Dai, Wang, Wang, *et al.* [85]	✓	✓	✓
Chiu, Meng, and Li [86]	✓	✗	✓
Prashar *et al.* [87]	✓	✗	✗

Table 2.1: The three quality evaluation criteria

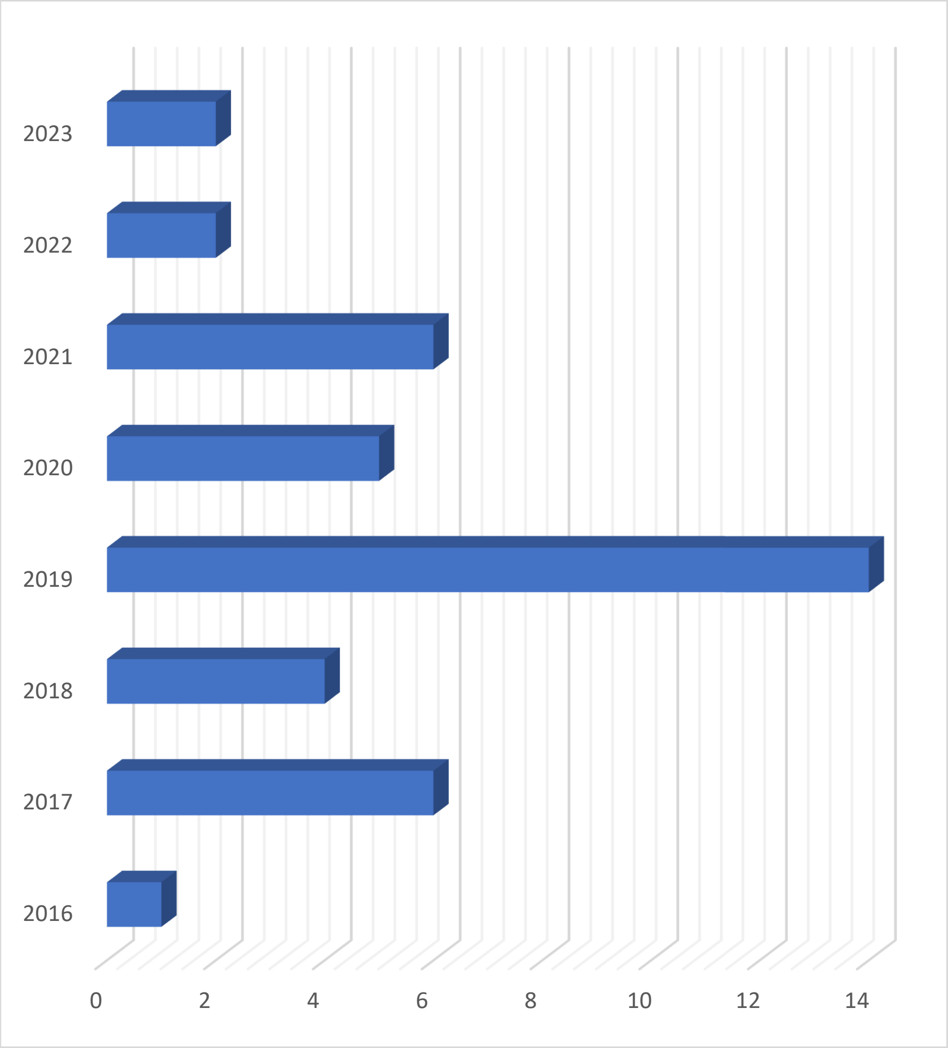


Figure 2.3: Primary study papers categorized by year of publication

2.3.4 Phase 4: Data analysis

The research scope, the topic area, and the summary of the research questions and solutions in each shortlisted article were examined. Then, the chosen papers were grouped into four broad categories to allow for a simplified classification of the primary studies' themes. These categories are key management techniques, authentication techniques and attacks against blockchain wallets, as shown in Table 2.2. The category of key management techniques discusses studies that employ various secure data storage and key generation approaches to maintain and retrieve the private key efficiently. The category of authentication techniques examines approaches that rely on authentication mechanisms to gain access to cryptocurrency wallets. The blockchain wallet attacks category discusses approaches that prevent attacks against blockchain wallets and address their vulnerabilities. Finally, the articles were reviewed to provide a summary, issues, and the limitations of each study.

Primary Paper	**Year**	**Title**	**Category**
Chiu, Meng, and Li [86]	2023	TPMWallet: Towards Blockchain Hardware Wallet using Trusted Platform Module in IoT	Key Management
Zhang, Zou, Xie, *et al.* [80]	2022	Blockchain Multi-signature Wallet System Based on QR Code Communication	Key Management
Li and You [76]	2021	A Consortium Blockchain Wallet Scheme Based on Dual-Threshold Key Sharing	Key Management
Lehto, Halunen, Latvala, *et al.* [81]	2021	CryptoVault-A Secure Hardware Wallet for Decentralized Key Management	Key Management
Dai, Wang, Wang, *et al.* [85]	2021	Trustzone-based secure lightweight wallet for hyperledger fabric	Key Management
Thota, Upadhyay, Kulkarni, *et al.* [59]	2020	Software wallet based secure participation in Hyperledger Fabric networks	Key Management
Rezaeighaleh and Zou [50]	2020	Multilayered Defense-in-Depth Architecture for Cryptocurrency Wallet	Key Management
He, Lin, Li, *et al.* [45]	2019	A Novel Cryptocurrency Wallet Management Scheme Based on Decentralized Multi-Constrained Derangement	Key Management
Khan, Zahid, Hussain, *et al.* [49]	2019	Security Of Cryptocurrency Using Hardware Wallet And QR Code	Key Management
Rezaeighaleh and Zou [46]	2019	New Secure Approach to Backup Cryptocurrency Wallets	Key Management
Dai, Deng, Wang, *et al.* [60]	2018	SBLWT: A Secure Blockchain Lightweight Wallet Based on Trust zone	Key Management
Zhu, Chen, Wang, *et al.* [47]	2017	Trust Your Wallet: A New Online Wallet Architecture for Bitcoin	Key Management
Liu, Li, Liu, *et al.* [48]	2017	An Efficient Method to Enhance Bitcoin Wallet Security	Key Management
Gentilal, Martins, and Sousa [61]	2017	TrustZone-backed Bitcoin Wallet	Key Management
Sung [78]	2021	A new key protocol design for cryptocurrency wallet	Authentication Techniques
Lomazina, Surovtsova, and Ivanov [82]	2021	Development of a Cryptocurrency IoT wallet with Automatic Authentication	Authentication Techniques
Hu, Liu, Niu, *et al.* [58]	2020	Securing the Private Key in Your Blockchain Wallet: A Continuous Authentication Approach Based on Behavioral Biometric	Authentication Techniques
Albakri and Mokbel [54]	2019	Convolutional Neural Network Biometric Cryptosystem for the Protection of the Blockchain's Private Key	Authentication Techniques
Marcedone, Pass, and Shelat [55]	2019	Minimizing Trust in Hardware Wallets with Two Factor Signatures	Authentication Techniques
Boneh, Gennaro, and Goldfeder [57]	2019	Using Level-1 Homomorphic Encryption to Improve Threshold DSA Signatures for Bitcoin Wallet Security	Authentication Techniques
Homoliak, Breitenbacher, Hujnak, *et al.* [51]	2018	SmartOTPs: An Air-Gapped 2-Factor Authentication for Smart-Contract Wallets	Authentication Techniques

Primary Paper	**Year**	**Title**	**Category**
Benli, Engin, Giousouf, *et al.* [53]	2017	BioWallet: A Biometric Digital Wallet	Authentication Techniques
Gennaro, Goldfeder, and Narayanan [56]	2016	Threshold-optimal DSA/ECDSA signatures and an application to Bitcoin wallet security	Authentication Techniques
Holmes and Buchanan [77]	2023	A framework for live host-based Bitcoin wallet forensics and triage	Blockchain Wallet Attacks
Qi, Xu, Jiao, *et al.* [79]	2022	A Comparative Study on the Security of Cryptocurrency Wallets in Android System	Blockchain Wallet Attacks
Jian, Ran, and Liyan [83]	2021	Securing blockchain wallets efficiently based on threshold ECDSA scheme without trusted center	Blockchain Wallet Attacks
Hu, Wang, Tu, *et al.* [84]	2020	Security threats from Bitcoin wallet smartphone applications: Vulnerabilities, attacks, and countermeasures	Blockchain Wallet Attacks
Chan [75]	2020	Android-based Cryptocurrency Wallets: Attacks and Countermeasures	Blockchain Wallet Attacks
Wang, Li, Gao, *et al.* [62]	2019	MOBT: A kleptographically-secure hierarchical-deterministic wallet for multiple offline Bitcoin transactions	Blockchain Wallet Attacks
Das, Faust, and Loss [63]	2019	A Formal Treatment of Deterministic Wallets	Blockchain Wallet Attacks
Di Luzio, Francati, and Ateniese [64]	2019	Arcula: A Secure Hierarchical Deterministic Wallet for Multi-asset Blockchains	Blockchain Wallet Attacks
Praitheeshan, Xin, Pan, *et al.* [66]	2019	Attainable Hacks on KeyStore Files in Ethereum Wallets A Systematic Analysis	Blockchain Wallet Attacks
Volety, Saini, McGhin, *et al.* [67]	2019	Cracking Bitcoin wallets: I want what you have in the wallets	Blockchain Wallet Attacks
Fan, Tseng, Su, *et al.* [68]	2019	Secure hierarchical Bitcoin wallet scheme against privilege escalation attacks	Blockchain Wallet Attacks
Wang, Gao, and Li [69]	2019	Efficient Bitcoin Password-protected Wallet Scheme with Key-dependent Message Security	Blockchain Wallet Attacks
Davenport and Shetty [70]	2019	Air-Gapped Wallet Schemes and Private Key Leakage in Permissioned Blockchain Platforms	Blockchain Wallet Attacks
Yin, Wen, Li, *et al.* [71]	2018	An Anti-Quantum Transaction Authentication Approach in Blockchain	Blockchain Wallet Attacks
Guri [72]	2018	BeatCoin: Leaking Private Keys from Air-Gapped Cryptocurrency Wallets	Blockchain Wallet Attacks
Gkaniatsou, Arapinis, and Kiayias [73]	2017	Low-Level Attacks in Bitcoin Wallets	Blockchain Wallet Attacks
Dmitrienko, Noack, and Yung [74]	2017	Secure Wallet-Assisted Offline Bitcoin Payments with Double-Spender Revocation	Blockchain Wallet Attacks

Table 2.2: Primary study papers

2.4 Analysis of Shortlisted Papers Against the Requirements to Facilitate a Blockchain-based wallet

In this section, the final selected papers are critically studied to identify the limitations, solutions, and research issues. Figure 2.4 illustrates the categorization of papers according to their subject areas and identifies the researchers' solutions and methods. These categories were selected as they correspond to the key requirements 2.2 that facilitate the development of BW solutions.

However, most of the literature is devoted to resolving issues related to key management techniques, authentication techniques and attacks. For key management issues, most of the studies employ various secure storage technologies, TrustZone technology, signature schemes, and key generation approaches to efficiently maintain and retrieve the private key. Additionally, digital signature technique solutions were investigated to facilitate the process of signing the transactions by entities. In the area of authentication techniques, most of the studies examined attribute authentication, which only relies on a password, and multi-factor authentication, which uses at least two verification techniques, such as biometrics and passwords, to gain access to blockchain-based wallets. In the attack category, researchers attempted to tackle the most commonly used attacks against blockchain-based wallets by applying security or threat models to identify vulnerabilities in the system and decrease attacks.

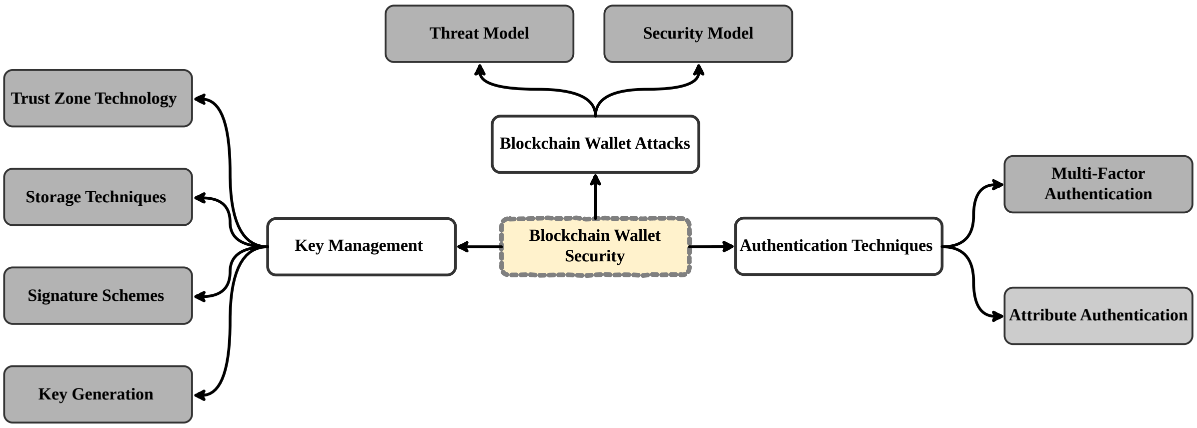


Figure 2.4: Categorization of papers by subject area

2.4.1 Key management techniques

The studies detailed in this section employ various secure data storage and key generation approaches to efficiently maintain and retrieve the private key of the BW solutions. Table 2.4 outlines the proposed security solutions using key management techniques for BWs.

He, Lin, Li, *et al.* [45] proposed a decentralized cryptocurrency wallet management scheme based on decentralized multi-constrained derangement (DMCD) to maintain the security and stability of private keys. They found that as DMCD has high data dispersion and it was able to balance space utilization and contribution, guaranteeing the security and stability of key storage and recovery. In this study, to solve the multi-constrained derangement (MCD) problem, they adopted the flow network strategy. In addition, to resolve the issue where nodes are constantly online and offline on a decentralized network, the Shamir-Kademlia-Neighbor (SKN) redundancy technique was applied to guarantee the availability of the stored key and improve the reliability of the proposed design. Also, to ensure anonymous communication during DMCD data distribution, they changed the client/server (C/S) mode of the Hordes protocol to a decentralized version denoted as D-Hordes, which serves as a decentralized anonymous communication protocol to guarantee the security of the data distribution. They evaluated the different aspects of the proposed model in a generally recognized primary management evaluation framework. They also conducted performance experiments and demonstrated that their design offers better data dispersion, stability, and availability than traditional methods. Furthermore, Li and You [76] proposed an improved consortium blockchain wallet scheme that manages private keys using a dual-threshold secret-sharing method to avoid multiple reconstructions of lost private keys. The study combines threshold cryptography and blockchain technology to solve private key management issues in consortium blockchain settings. The results show that the proposed consortium blockchain wallet scheme based on dual-threshold key sharing enhances blockchain wallets' security and improves the management of private keys. Khan, Zahid, Hussain, *et al.* [49] introduced a blockchain-based wallet management scheme for the Android operating system utilizing a QR code and a secure cold wallet to store private keys. Also, they implemented two Android applications, one known as a cold wallet and the other a hot wallet. The cold wallet is applied for offline storage and produces private key addresses for secure transaction verification, and the hot wallet is used to transfer currencies within the network. They claimed that the hot and cold wallet transactions become more reliable by applying QR code scanning for cross-identification, validation, and authentication between users. Zhang, Zou, Xie, *et al.* [80] introduced a multi-party signature method to address the challenges of managing private keys for blockchain wallets. It uses threshold signature technology and homomorphic encryption algorithms to avoid the influence of single malicious parties on digital currency transactions. It also provides secure key storage through a cold wallet that communicates through QR code scanning. Private keys were stored offline in cold wallets, and a visible light communication method based on a QR code was used to protect against electromagnetic side-channel attacks. Base45 coding scheme was used to increase QR code efficiency and optimize the GG18 multi-party signature process. Their experiment shows that this method enhances the communication efficiency of blockchain wallets and improved their design.

Lehto, Halunen, Latvala, *et al.* [81] introduced CryptoVault, a hardware wallet that securely generates and maintains the private key in an Intel Software Guard Extension (SGX) environment. It uses an end-to-end secure connection to an external repository to store and recover private keys securely. CryptoVault provides a solution for storing and managing the user's private keys and backing up these keys as independent shares stored in multiple locations. The study highlights the security assumptions and provided insights into the implementation of CryptoVault. Their results show that backing up keys provides a secure solution for managing and protecting private keys which is essential for secure blockchain transactions. Rezaeighaleh and Zou [46] proposed a cryptocurrency hardware wallet scheme based on Elliptic-Curve Diffie-Hellman key agreement for secure backup recovery, relying on side-channel human visual verification enabled on a hardware wallet display screen. They were able to securely convey the root of private keys from one hardware wallet to another wallet, including untrusted terminals, such as mobile phones. In their model, the users have two hardware wallets with the same private keys, one of which is used as the main wallet and the other as a backup wallet. As a proof-of-concept, they implemented a deterministic sub-wallet utilizing a smart card for a hardware wallet and mobile phones to understand the secure backup performance. They found that the wallet model decreases the refill cost and time, enhances security against a man-in-the-middle attack, and removes the sub-wallet backup demand. Liu, Li, Liu, *et al.* [48] proposed a key management solution that incorporates an easily remembered passphrase with a random number to generate private keys to protect the bitcoin software wallet. Furthermore, they added a function that enables users to retrieve the passphrase from personal questions which is a convenient way to recover their private keys. The scheme can be applied to sign and authorize transactions created by the users without professional knowledge and manage their private keys securely. Conceptually similar work was proposed by Zhu, Chen, Wang, *et al.* [47] who created a new online wallet management strategy called HA-eWallet which allows the transaction to be signed by multiple private keys, and the private keys to be stored separately in different places. They also improved their model's availability by implementing a disaster recovery approach to resolve data loss issues and constructed an active-active architecture. Their theoretical analyses demonstrated that the model is able to provide greater availability, and the users do not experience the loss of private keys unless more than 50% of the users' total private keys are lost. Rezaeighaleh and Zou [50] proposed a multilayered design for bitcoin wallets based on a defence-in-depth technique that employs layers to protect private keys while still offering usability. The user can apply three restricted layers, each of which is implemented with various use and protection techniques to balance usability and security. The protected layer is called a superior wallet containing the master seed, which generates the whole key tree and all associated addresses. The second layer is the offline layer, which has a backup wallet that is a clone of the superior wallet. Finally, the online layer utilizes multiple spending wallets to make routine daily transactions. The authors implemented the proposed architecture on a smart card hardware wallet and an Android smartphone wallet as a proof-of-concept. Also, they utilized two adversary models to assess the security of the proposed architecture.

Some studies utilize TrustZone technology, a hardware-based security mechanism, specifically as a trusted execution environment. This provides a secure environment for protecting critical operations and private keys in BW solutions. For instance, Thota, Upadhyay, Kulkarni, *et al.* [59] proposed a model that allows end-users to manage their identity by keeping their private keys in a safe zone while allowing a less trusted zone to communicate with the blockchain network. They claimed that the software wallet could be utilized on mobile devices to sign transactions and engage in the Hyperledger Fabric blockchain network without significantly impacting the device. Their results show that the software wallet can remove complex and transaction preparation logic to a server component running in the same (trusted) or different (untrusted) domain that effectively defines different trust levels and configures what gets verified. Gentilal, Martins, and Sousa [61] investigated how to significantly increase the security of bitcoin wallets using the TrustZone technology model to make it resilient against dictionary and side-channel attacks. They expanded a hardware cryptocurrency wallet by implementing a TrustZone system and enabling separate trusted and non-trusted environments while ensuring the integrity of the OS code. They stated that the utilization of the Global Platform APIs has made cryptographic operations more practical as platform-specific optimizations are applied, which compensates for the increased writing and reading times of encrypted storage used to enhance protection. Dai, Deng, Wang, *et al.* [60] designed a secure blockchain lightweight wallet (SBLWT) based on TrustZone which provides comprehensive protection for a private key in simplified payment verification (SPV). Their model can protect the verification process by validating transactions in a secure execution environment and encrypt the local block headers to make them invisible from the Rich OS. They implemented and evaluated their scheme on the RASPBERRY PI 3 MODEL B development board. Dai, Wang, Wang, *et al.* [85] proposed a Trustzone-based secure lightweight wallet (TSLWHF) to address the security challenges of blockchain wallets. The TSLWHF uses an unspent transaction output (UTXO) and a signature verification mechanism for transactions. It also applies the simple payment verification (SPV) mechanism to protect users' private keys, wallet addresses, block header information, and transaction verification process. The system is implemented in Hyperledger fabric and ARM's Trustzone. The experiments show that this scheme reduces the size of locally stored data while protecting the security of user assets. Chiu, Meng, and Li [86] introduced TPMWallet, a blockchain-based hardware wallet that uses the trusted platform module (TPM) to ensure secure communication and data preservation. It addresses the issue of the wallet being detached from the device in IoT-enabled networks, resulting in fraud and incorrect information propagated within the network. The proposed solution utilizes TPM to replace software wallets and is implemented on the Hyperledger platform. Also, it provides policies that enable TPMs to run under matching conditions, making it difficult to tamper with TPMWallet. The results show that TPMWallet integrates the functionality of the existing blockchain hardware wallet into a secure subsystem.

Primary Study	**Requirements of Blockchain Wallets**				
	Req1	**Req2**	**Req3**	**Req4**	**Req5**
Zhang, Zou, Xie, *et al.* [80]	✗	✗	✗	✓	✗
He, Lin, Li, *et al.* [45]	✗	✓	✗	✗	✗
Rezaeighaleh and Zou [46]	✗	✓	✗	✗	✗
Li and You [76]	✗	✓	✗	✓	✗
Lehto, Halunen, Latvala, *et al.* [81]	✗	✓	✗	✓	✗
Liu, Li, Liu, *et al.* [48]	✗	✓	✗	✗	✗
Zhu, Chen, Wang, *et al.* [47]	✗	✓	✗	✗	✗
Khan, Zahid, Hussain, *et al.* [49]	✗	✓	✗	✗	✗
Rezaeighaleh and Zou [50]	✗	✓	✗	✗	✗
Thota, Upadhyay, Kulkarni, *et al.* [59]	✗	✓	✗	✓	✗
Chiu, Meng, and Li [86]	✗	✓	✓	✓	✗
Gentilal, Martins, and Sousa [61]	✗	✓	✗	✓	✗
Dai, Wang, Wang, *et al.* [85]	✗	✓	✗	✓	✗
Dai, Deng, Wang, *et al.* [60]	✗	✓	✗	✓	✗

Table 2.4: Key management technique studies.

2.4.2 Authentication techniques

Many studies investigated and implemented different methodologies to secure private keys in blockchain-based wallets. Table 2.6 outlines the papers which propose security methods using authentication techniques for BWs. For instance, Homoliak, Breitenbacher, Hujnak, *et al.* [51] proposed SmartOTP, a smart-contract hardware wallet framework that provides 2-factor authentication (2FA) in two interaction steps with the blockchain. The framework utilizes OTPs designed by combining a pseudo-random function, Merkle trees, and hash chains that allow an air-gapped wallet to be set using mnemonic words or by scanning QR codes. The authors found that their flexible, usable model was able to securely manage cryptocurrencies in a self-sovereign fashion, protect against attackers who have a user private key, and demonstrate resilience against quantum cryptanalysis. The proof-of-concept was carried out based on the Ethereum platform, and the operational cost analysis reveals that a transfer is equivalent to existing 2FA solutions utilizing smart contracts with multi-signatures. Benli, Engin, Giousouf, *et al.* [53] introduced BioWallet, a conceptual model that incorporates biometric and password authentication mechanisms to secure digital currencies within mobile bitcoin wallets. The proposed model improves the security of cryptocurrencies stored in bitcoin wallets utilizing users' fingerprint-based access control. They compared their model with existing wallets and found their model was more secure because it did not store the fingerprint data on the cloud, rather it stored the data locally.Albakri and Mokbel [54] extended the techniques by proposing a cryptocurrency wallet model that applies biometric authentication techniques to protect the user's private keys. The neural network facial recognition scheme was used to extract biometric features and secure the keys in a key binding strategy. A convolutional neural network that includes two dense layers was trained and the output classification layer was used as biometric features. Three independent face datasets were used and the error rate between false acceptance and rejection was insignificant when testing samples of identical datasets. The authors stated that the results were satisfying and proved that biometric authentication is able to protect users' private keys in many cryptocurrency wallets. Hu, Liu, Niu, *et al.* [58] proposed a continuous authentication technique or the blockchain wallet using behavioural biometrics, such as mouse movements, to authenticate users' identities in real-time. The suggested solution incorporates user mouse behavioural biometrics and users' private keys, which can effectively prevent the leakage of the user's private key. Also, this solution employs the notion of users generating biometrics via a mouse, in conjunction with the CNN network training classification model, to provide continuous authentication. The experiment demonstrated that the technique can successfully re-authenticate users once every second, with high accuracy, and provides a way to tackle the issue of storing private keys securely in blockchain wallets.

Marcedone, Pass, and Shelat [55] introduced a cryptocurrency hardware wallet that is secure against attacks conducted by a malicious hardware manufacturer by implementing a two-factor signature scheme. Two-factor signatures (2FS) were introduced, a generalization of a two-out-of-two threshold signature scheme in which one party is a hardware token capable of holding a high-entropy secret, and the other party is an individual with a low-entropy password. In addition, the 2FS authentication (unforgeability) feature prevents an external adversary from building a signature by corrupting any side (a token or a computer). This fundamental is valuable in situations such as hardware cryptocurrency wallets in which a signature carries a transaction authorization. They developed and evaluated the performance of 2SF systems in the Random Oracle Model, which produces either the signature of Schnorr (assuming the DLOG assumption) or EC-DSSA (assuming the security of EC-DSA and the CDH assumption). Boneh, Gennaro, and Goldfeder [57] introduced new and improved DSA signature authentication techniques with an optimal reduced threshold wheel complexity. They stated that their implemented Level-1 FHE scheme and signature protocol achieves more effective runtime than the other methods. Gennaro, Goldfeder, and Narayanan [56] proposed a threshold-optimal signature scheme for the DSA to secure bitcoin wallets. They found that their scheme is both threshold optimal and efficient since it needs only n ≥ t + 1 servers to defend against an opponent that compromises up to t servers, and the protocol needs a constant number of rounds. Also, in terms of computation time, each player uses a constant amount of time and entities have a constant amount of storage. They implemented and evaluated their scheme to demonstrate that it is highly efficient and fully functional. Sung [78] proposed a method to enhance the authenticity of cryptocurrency wallets by replacing the conventional key storage scheme with a session key agreement protocol. The Federated Byzantine Agreement (FBA) protocol is used to enable the key exchange agreement among users while the session key is encoded in the blockchain data structure. It uses the session key authentication and the cluster key in a peer to perform multi-party computations. The study results indicate that the proposed key protocol enhances the authentication and security of cryptocurrency wallets and may offer a promising solution to wallet information theft issues. Lomazina, Surovtsova, and Ivanov [82] proposed a new architecture for cryptocurrency wallets with automatic authentication of devices in IoT networks. It implements a secure method for IoT devices to establish a secure data exchange channel. The authors use UTIM/UHOST libraries for authentication and the Obyte wallet for IoT devices. As a result, the proposed architecture provides a secure method for wallet initiation and a practical solution for personalizing IoT devices.

Primary Study	**Requirements of Blockchain Wallets**				
	Req1	**Req2**	**Req3**	**Req4**	**Req5**
Homoliak, Breitenbacher, Hujnak, *et al.* [51]	✗	✓	✓	✓	✗
Sung [78]	✗	✓	✓	✓	✗
Benli, Engin, Giousouf, *et al.* [53]	✗	✗	✓	✗	✗
Lomazina, Surovtsova, and Ivanov [82]	✗	✓	✓	✗	✗
Albakri and Mokbel [54]	✗	✗	✓	✗	✗
Marcedone, Pass, and Shelat [55]	✗	✓	✓	✓	✗
Boneh, Gennaro, and Goldfeder [57]	✗	✗	✓	✓	✗
Gennaro, Goldfeder, and Narayanan [56]	✗	✗	✓	✓	✗
Hu, Liu, Niu, *et al.* [58]	✗	✗	✓	✗	✗

Table 2.6: Authentication technique studies.

2.4.3 Blockchain wallet attacks

Many security and threat models have been introduced to prevent attacks against blockchain-based wallets. For instance, Wang, Li, Gao, *et al.* [62] proposed a secure offline hierarchical deterministic wallet (HDW) that relies on a master public key property called MOBT. Their model is able to resist a kleptographic attack that enables the intruder to acquire the user's private keys by injecting the user's offline wallet storage with the Secretly Embedded Trapdoor with Universal Security (SETUP) algorithm. Also, they applied the blacklist mechanism that holds a blacklist to monitor all wallets associated with a double spender, thereby freezing all assets in these accounts to overcome a double-spending attack in an offline transaction. They found that their scheme is able to execute multiple offline bitcoin transactions with high productivity between payers and only needs to store and back up the master's private keys, reducing the wallet's storage burden. They demonstrated the security of their wallet in the random oracle model based on the one-more discrete-logarithm. Das, Faust, and Loss [63] designed a security model for hot/cold wallets that guarantees unlinkability and unforgeability using specific signature schemes. They stated their scheme is an extension of a secure ECDSA-based hot/cold wallet and can be integrated into different cryptocurrency environments such as bitcoin. In a similar context, Di Luzio, Francati, and Ateniese [64] proposed Arcula, a security model of HDWs that incorporates identity-based signatures into blockchain and secures it against privilege escalation attack. They stated that their wallet allows them to receive payments in an entirely untrusted environment using dynamically derived new addresses and verifying signatures on arbitrary messages. They developed a deterministic hierarchical key assignment scheme, a popular cryptographic primitive to generate the set of cryptographic keys and validate the model in a real-world scenario on the Bitcoin Cash network.Praitheeshan, Xin, Pan, *et al.* [66] conducted a systematic review of the hacking methods in the existing literature and studied how the Ethereum wallet KeyStore file is subject to attacks. The Ethereum wallet's password was cracked using brute force and a dictionary attack since the KeyStore file is encrypted with a password. Their results show that the dictionary attack outperformed the brute-force attack in hacking the KeyStore file. In addition, if complex password credentials are used, the KeyStore file is less insecure. Similarly, Volety, Saini, McGhin, *et al.* [67] analyzed the security of two popular bitcoin wallets to demonstrate the system's vulnerability. Specifically, they illustrated how known implementation vulnerabilities in Multibit HD and Electrum wallets can be exploited to obtain the stored bitcoins. Their experiment found that the Electrum wallet does not have a timestamp, so the attacker will obtain unauthorized access to the currency deposited in the wallet if allocated to a user.

Fan, Tseng, Su, *et al.* [68] implemented a new HDW model to prevent privilege escalation attacks generated by an insecure child key derivation to some wallet schemes within blockchain. They claimed that the architecture guarantees unforgeability by adopting a Schnorr signature with trapdoor hash functions. It also ensures the unlinkability between two public keys to achieve the user's anonymity and scalability to the derivations of a massive number of keys. Wang, Gao, and Li [69] proposed KDM-CCA, a new password-protected wallet scheme to resist attacks in local storage by utilizing a semi-trusted cloud backup strategy to store and manage personal wallet files. Users can upload symmetrically encrypted backup files to the cloud to ensure files are protected from information disclosure and local data loss. They provided a detailed security and efficiency analysis and showed that the scheme is efficient and practical. Yin, Wen, Li, *et al.* [71] proposed a novel anti-quantum authentication scheme that resists the quantum algorithm's attack in the blockchain network. They leveraged the bonsai tree signature scheme to build lightweight nondeterministic wallets and ensure the master private key's randomness. Their scheme is secure against user signature forgery under the chosen message attack and reduces the lattice's SIS hard problem. They stated that the model emphasizes the theoretical significance of anti-quantum blockchain technology. Guri [72] evaluated and demonstrated various techniques that attackers could utilize to exfiltrate and infiltrate the private keys in air-gapped wallets using covert channels such as electromagnetic, electric, and magnetic acoustic. The attack threat model illustrates how an attacker can exploit the wallet's computer by installing malware with malicious code using removable media. They declared that while isolated cold wallets provide a high level of protection, they are not beyond the attackers' capability to compromise the wallet's private keys. Davenport and Shetty [70] examined the threat surface of air-gapped wallet schemes over channels for permissioned blockchains and presented a quantitative understanding of the security risk associated with private key leakage. They discussed the Markov-based mathematical model that illustrates the life cycle of an attack, starting with private key extraction and ending with the exfiltration of funds from air-gapped wallets. Their results show that it is possible to determine the influence each parameter has on transitions, helping the users find the vulnerability in their air-gapped wallet system and implement adequate measures to appropriately secure their private keys.

Gkaniatsou, Arapinis, and Kiayias [73] highlighted how low-level communication protocols that implement hardware wallets can be exploited to launch side-channel attacks against hardware bitcoin wallets. They also introduced a threat model using a lightweight approach that can be implemented by various technologies to address the lack of a well-defined security functionality that every hardware wallet should maintain. They analyzed the LEDGER wallet communication protocol, which is the only EAL5+ certified against side-channel attacks and demonstrated how to attack it successfully in practice. Dmitrienko, Noack, and Yung [74] proposed security mechanisms for bitcoin payments that enable secure transactions in offline environments and situations where payments need to be accepted immediately. Their approach relies on an offline wallet instantiated by applying secure hardware and utilizes a wallet deposit system to prevent double-spending attacks. They also presented a risk analysis and implemented the solution on mobile Android clients using a microSD security card. Their results demonstrate that offline and online payments are able to co-exist practically and smooth integration over a standard mobile platform (Android) is feasible. Chan [75] applied a systematic methodology to analyze the security of popular Android-based cryptocurrency wallet applications. They discovered multiple cryptocurrency wallet vulnerabilities in Android backup files, clipboards, accessibility services, and permission management. Also, they developed an adversary model to evaluate the attack surface and conduct several attacks against many popular digital wallets available on the Google Play Store to steal the user's sensitive information via the secure keyboard input. They validated the effectiveness of their experiments by designing proof-of-concept attacks based on the identified vulnerabilities and provide several corresponding security measures to decrease the attack surface. The studies in this category focus on implementing several defence techniques to overcome various security attacks against blockchain-based wallets. Similarly, Qi, Xu, Jiao, *et al.* [79] proposed a security assessment framework for cryptocurrency wallets based on Android application security detection. The paper presented a systematic attack-based weighting framework for cryptocurrency wallet security evaluation and conducted a comparative study of ten popular Android cryptocurrency wallet applications. The findings suggest that cryptocurrency wallet audits are critical to mitigate security risks and increase user confidence.

Jian, Ran, and Liyan [83] proposed a scheme that provides a secure and efficient way to protect blockchain wallets against single-point failure without needing a trusted center. It applies a threshold elliptic curve digital signature to generate public and private keys without the participation of a trusted center. Participants cooperate to share the private key, and those exceeding the threshold can sign transactions. The result shows that the completion time of the system only needs constant rounds, which improves the efficiency and scalability of the scheme. Moreover, this robust, anonymous, and unforgeable scheme effectively protects the blockchain wallet's privacy and security. Hu, Wang, Tu, *et al.* [84] investigated the security of the ten most popular bitcoin wallet smartphone applications and identified three vulnerabilities that can lead to financial fraud attacks. A phone-based bitcoin security rectifier was developed to protect against bitcoin deanonymization, spamming, and fraud attacks. The rectifier is written in Java and developed on Android smartphones. The proposed bitcoin security rectifier does not require modifications to the existing bitcoin protocol standards, wallet applications, libraries, or wallet service operations. The results show that the rectifier intercepts the bloom filter with a low false positive rate. Holmes and Buchanan [77] discussed the use of bitcoin by organized crime and cyber-criminals to launder money and transfer funds across borders.

The researchers proposed a live host-based bitcoin wallet forensics and triage framework. It includes two proof-of-concept dictionary-attack tools in Python and OpenCL. They stated that using legislation such as the Proceeds of Crime Act (POCA), countries like the UK can recover proceeds from criminal activity, including cryptocurrency assets. They evaluated the framework using a low-cost cluster of public cloud-based graphics processing unit (GPU) instances. Also, they examined the Electrum software wallet and the Ledger Nano S hardware wallet to establish what artifacts could be recovered. Their analysis revealed a weakness in Electrum's storage of encrypted private keys in RAM, which the researchers leveraged to make around 2.4 trillion password guesses. They also demonstrated that they can conduct 16.6 billion guesses against a password-protected Ledger seed phrase. These findings emphasize the need for more robust bitcoin wallet security to prevent attacks and seizures by law enforcement.

Primary Study	**Requirements of Blockchain Wallets**				
	Req1	**Req2**	**Req3**	**Req4**	**Req5**
Wang, Li, Gao, *et al.* [62]	✓	✓	✗	✗	✗
Qi, Xu, Jiao, *et al.* [79]	✓	✗	✗	✓	✗
Das, Faust, and Loss [63]	✓	✗	✗	✓	✗
Holmes and Buchanan [77]	✗	✓	✗	✗	✗
Di Luzio, Francati, and Ateniese [64]	✓	✗	✗	✓	✗
Praitheeshan, Xin, Pan, *et al.* [66]	✗	✓	✗	✗	✗
Volety, Saini, McGhin, *et al.* [67]	✓	✗	✗	✗	✗
Jian, Ran, and Liyan [83]	✗	✗	✗	✓	✗
Hu, Wang, Tu, *et al.* [84]	✗	✗	✓	✗	✗
Fan, Tseng, Su, *et al.* [68]	✓	✗	✗	✓	✗
Wang, Gao, and Li [69]	✓	✓	✗	✗	✗
Yin, Wen, Li, *et al.* [71]	✗	✗	✓	✓	✗
Guri [72]	✓	✓	✗	✗	✗
Davenport and Shetty [70]	✓	✗	✗	✗	✗
Gkaniatsou, Arapinis, and Kiayias [73]	✓	✗	✗	✗	✗
Dmitrienko, Noack, and Yung [74]	✓	✗	✗	✗	✗
Chan [75]	✗	✓	✓	✗	✗

Table 2.8: Attacks and security models.

2.5 Research Gaps in the existing studies

As shown in Tables 2.4, 2.6 and 2.8 the comprehensive and detailed literature review identified the following research gaps:

2.5.1 There is a lack of approaches that integrates hard and soft security methods to secure BW solutions

There are no approaches that combine hard and soft security measures for a secure and trustworthy BW framework. The current BW studies tends to treat hard and soft security as separate aspects, analyzing them separately instead of considering them as interconnected components of a comprehensive security strategy. Furthermore, the majority of existing studies focused on implementing hard security measures and neglected soft security measures. They employ hard security measures to safeguard BW owners' digital assets, such as public-private key pairs, hashing algorithms, and secure encryption. For example, [64], [68], [71], [83] developed a practical signature predicate that protects the private key from forgeability issues and privilege escalation attacks. Also, threshold signature wallets were proposed in [56], [57] to improve the performance of the digital signature technique in BWs. Furthermore, [85], [86] discussed how to apply secure authentication techniques to secure private keys in a hardware or software wallet using TrustZone technology to provide hardware-based security.

However, focusing on hard security undermines other crucial security considerations in BW solutions. In a comprehensive security framework, hard and soft security measures should be integrated seamlessly to create an effective defence against various potential threats. Soft security strategies including trust models, reputations, and ranking systems strengthen the overall resilience of the blockchain ecosystem by fostering trust among BW users. Acknowledging and bridging the gap between these security measures is crucial for developing reliable and trustworthy BW solutions.

2.5.2 A limited number of studies use biometrics to enhance the authentication techniques of the blockchain-based digital wallet

A limited number of studies used sophisticated authentication techniques for BW solutions. The authentication system contains sensitive user data; therefore, it is critical to provide a strong access control mechanism to avoid unauthorized access to confidential financial information. Factor-based protocols appear to be the most promising ones to apply, and two-factor authentication protocols ensure cryptocurrency wallet security without incurring a massive computing overhead. Accordingly, [51], [55] study two-factor authentication procedures to improve the security of cryptocurrency wallets and prevent unauthorized entities from accessing the system. The work in [53], [54], [58] incorporates biometric factors with passwords or hardware wallets to improve the accuracy and reliability of the authentication process in blockchain wallets.

However, there are limited studies on integrating different MFA factors, including biometric and facial recognition, into BW solutions. Despite the increasing recognition of the importance of MFA in enhancing digital asset security, there is a notable gap in understanding how specific factors, such as biometrics and facial recognition, can be effectively implemented within the context of BW solutions. Additionally, current research examining the integration of MFA factors into BW solutions is limited and lacks a comprehensive assessment of the security levels associated with each factor. Thus, further research and documentation must be conducted to clarify how MFA factors affect BW solutions. Addressing this gap advances secure digital asset management and provides a foundation for developing standardized and reliable practices within the blockchain ecosystem.

2.5.3 There is a lack of approaches that enables an entity to carry out a trust-based assessment on BW solutions.

According to [60], [61], the trustworthiness of the BW solution can be attributed to the security of the cryptographic keys and hardware components. However, there is no approach to address trustworthiness in the context beyond technical and hardware-based security measures. Despite the advancements in cryptographic and hard security, current studies ignore the complex interactions and trust dynamics inherent in a community-driven, decentralized environment. This gap highlights the need for a human-centric approach and trust framework, introducing a structured method and algorithms to establish, evaluate, and manage trust among BW participants. It should consider the social dynamics, various security factors, and trust criteria in this decentralized and trustless environment.

2.5.4 There is a lack of approaches that uses AI to assess and rank BW solutions based on a general and customized mode.

Soft security measures, such as trust models and ranking systems, are crucial to evaluating and managing the trustworthiness of BW solutions. This system uses various trust criteria to evaluate and rank BW solutions transparently and efficiently. Therefore, BW users can make informed decisions, increasing security within the blockchain ecosystem. However, a noticeable gap exists in the current literature as there is a lack of recognized and standardized

AI-based ranking systems specifically designed for assessing the security, trustworthiness, and overall performance of BW solutions. Traditional evaluation methods fail to provide a dynamic and adaptive approach to the rapidly evolving blockchain ecosystem. The use of AI becomes imperative to bridge this gap because of its capacity to analyze vast datasets and adapt to emerging trends. Addressing this gap through AI-driven assessment mechanisms will result in accurate, efficient, and future-oriented evaluations, ultimately enhancing user confidence and facilitating well-informed decisions in selecting BW solutions.

2.6 Chapter Summary

- This chapter identifies and analyzes the current security challenges in cryptocurrency wallets through a systematic literature review (SLR). First, the relevant studies were divided into three categories: key management techniques, authentication techniques and attacks on blockchain wallets. Then, the research studies in each category were overviewed, including a discussion of their strengths and limitations. Finally, a summary of the gaps identified by the SLR was presented.
- The next chapter (Chapter 3) outlines the keywords and concepts used in this thesis and identifies the research questions and objectives.

CHAPTER

3 Research Questions and Objectives

3.1 Chapter Overview

Chapter 1 highlighted the importance of integrating hard and soft security measures for secure and trustworthy blockchain wallet solutions. In Chapter 2, the systematic literature review presented the different techniques applied to improve the security of blockchain wallet solutions and identified the research gaps in the current literature. Based on the extensive systematic literature review, this chapter formulates the research questions that set the foundation for defining our research objectives to be addressed in this thesis. This chapter is organized as follows: Section 3.2 defines the key terms and definitions used throughout the thesis. Section 3.3 and Section 3.4 explain the research questions and the research objectives, respectively. Section 3.5 presents the chapter summary.

3.2 Keywords and Definitions

This section provides formal definitions of key terms and concepts that will be used to introduce, explain, and formalize the research problem addressed in this thesis.

3.2.1 Hard Security

Hard security is described as traditional security techniques or infrastructure level security, such as encryption, cryptography protocols, authentications, and access control methods [4].

3.2.2 Soft Security

Soft security methods apply social norms to manage and advance the environment's security. They are derived from social science that is controlled by two mechanisms: laws and social standards. Social norms exert a great deal of social control and define the social behavior that most individuals find acceptable, such as trust systems [31].

3.2.3 Blockchain Wallet Solutions

BW solutions are applications and services that allow BW users to manage digital assets and interact with a blockchain network. The applications manage basic wallet functionalities like storing private keys, sending and receiving digital assets, and tracking transaction history. At the same time, the services offer additional support and infrastructure, such as security features and integration with multiple decentralized applications to enhance the overall BW user experience [88].

3.2.4 Blockchain Wallet Developers and Providers

BW developers create and develop BW solutions for interacting with blockchain networks. They code the essential features that make BW solutions reliable and ensure the secure storage and management of digital assets. Additionally, BW providers offer convenient and effective BW solutions, delivering enhanced functionality, security, and ongoing support [89].

3.2.5 Two-factor Authentication (2FA:)

Two-factor authentication (2FA) is a two-step verification mechanism that adds an extra layer of protection by enabling the user's identity to be authenticated and verified using a secondary means (ownership or inheritance factors) [90].

3.2.6 Multi-factor Authentication (MFA:)

MFA is a security mechanism that strengthens the authentication process of BW solutions and prevents unauthorized access to wallets. It provides this protection by requiring several factors before granting access to BW accounts, including OTPs, TOTP and biometrics data [91].

3.2.7 Biometrics Authentication Technique

Biometrics is the automatic utilization of particular human physiological or behavioural features to establish or validate a person's unique identity. It is a measured physiological or behavioural characteristic that can be recorded and then linked to a known, earlier database [92].

3.2.8 Trust Modeling

Trustworthiness is the amount of trust the entity provides to other entities on the grounds of prior experiences between them. If an entity regularly meets other entity's standards by offering accurate and trustworthy information or transactions, other entities can improve the entity's credibility. Similarly, the inability to satisfy other entity's standards due to either negligence or maliciousness could reduce the entity's credibility with other entities. It also addresses the quality of services and entities based on several criteria [93].

3.2.9 Ranking Systems for BW Solutions

The blockchain-based wallet ranking system plays an indispensable role in building trust among all the cryptocurrency ecosystem entities. The ranking can be determined from specific quantitative factors such as the security level of wallets, the number of supported currencies, and the age of wallets. These ranking models might help in the fundamental decision-making to select satisfactory blockchain-based wallets. Such systems must also allow honest wallet filtration in the ecosystem and an incentive structure to minimize defrauding [94].

3.3 Research Questions

This section outlines the research questions after identifying the research gaps in the existing literature. This thesis addresses the following main research question: ***How can BW solutions be a secure, intelligent, and trustworthy platform by integrating hard and soft security mechanisms?***

The main question is divided into the following sub-questions:

1. ***Research Question 1***: How can we develop a secure, intelligent, and trustworthy framework to strengthen the security of BW solutions and assess BW solution trustworthiness?

2. ***Research Question 2***: How can we use 2FA, MFA and biometric authentication mechanisms to enhance the security of BW solutions?

3. ***Research Question 3***: How can we develop a trustworthiness model that enables BW users to make trust-based decisions regarding BW solutions?

4. ***Research Question 4***: How can we develop an intelligent trust-based ranking system that allows BW users to get general and personalized rankings based on the trustworthiness model?

5. ***Research Question 5***: How can we evaluate and validate the proposed model using a prototype?

3.4 Research Objectives

This thesis examines how blockchain-based wallets can be enhanced by integrating ”hard security” and ”soft security” techniques. It offers a complete methodology for improving blockchain wallet security and trustworthiness by analyzing and integrating sophisticated authentication techniques as hard security and trust-based ranking systems as soft security. The specific objectives of the thesis are:

1. ***Objective 1:*** To develop a secure, intelligent, and trustworthy framework to enhance the security and trustworthiness of BW solutions.

2. ***Objective 2:*** To investigate and develop different MFA and 2FA mechanisms to capture their effectiveness in securing BW solutions.

3. ***Objective 3:*** To propose an intelligent trust-based ranking system that uses AI to predict the ranking of BW solutions in general and customized modes.

4. ***Objective 4:*** To evaluate and validate the prototype developed to achieve objectives 1 to 3.

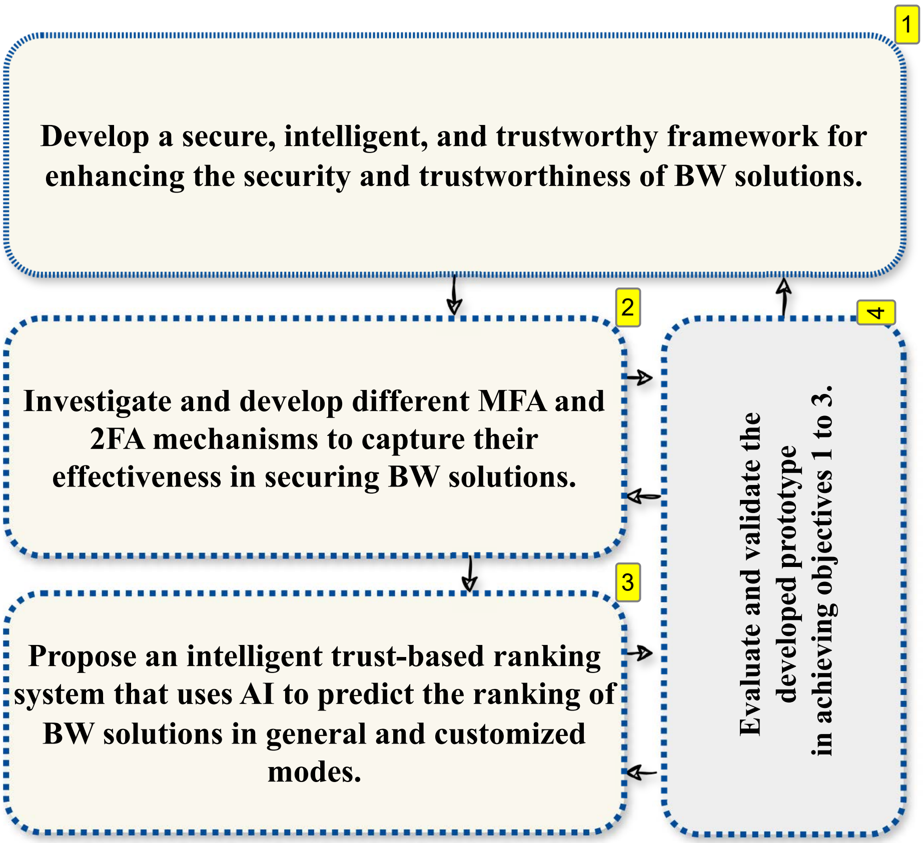

1
Develop a secure, intelligent, and trustworthy framework for enhancing the security and trustworthiness of BW solutions.
2
Investigate and develop different MFA and 2FA mechanisms to capture their effectiveness in securing BW solutions.
3
Propose an intelligent trust-based ranking system that uses AI to predict the ranking of BW solutions in general and customized modes.
4
Evaluate and validate the developed prototype in achieving objectives 1 to 3.

Figure 3.1: Research objectives

3.5 Chapter Summary

- This chapter outlined the key terms used throughout the thesis. It also identified the research questions and objectives to address how BW solutions can be secure, intelligent, and trustworthy by integrating hard and soft security mechanisms.
- The next chapter (Chapter 4) defines the methodology adopted to achieve the research objectives. It describes the proposed solutions using the design science research methodology.

CHAPTER

4

Research Methodology and Solution Overview

4.1 Chapter Overview

Chapter 1 highlighted the importance of incorporating hard and soft security mechanisms to strengthen the security and trustworthiness of BW solutions. Chapter 2 described the systematic literature review which was conducted to identify the gaps in the current studies. It was noted that considerable advances have been made by various researchers in the area of BW security. However, none of the existing proposals offer a complete methodology for integrating hard and soft security methods to secure BW solutions. Thus, four gaps were identified in the existing literature which should be addressed to develop a complete methodology for a secure and trustworthy BW solution. This chapter discusses the methodology that is applied to address the identified gaps in the literature review. Moreover, the chapter presents the proposed solution and how the research objectives will be achieved. The chapter is organized into the following sections: Section 4.2 presents the research methodology. Section 4.3 provides an overview of solutions for the proposed system. Finally, Section 4.4 concludes the chapter.

4.2 Research Methodology

A research methodology is a systematic approach encompassing a range of techniques and strategies to conduct research in multidisciplinary fields[95]. This section describes the research methodology employed to achieve the research objectives defined in Section 3.4.

4.2.1 Design Science Research Methodology (DSRM:)

The research methodology utilized in this thesis is called the design science research methodology. The DSRM approach is a commonly adopted methodology in computer science and software engineering fields for research problem-solving [96]. Figure 4.1 shows the six phases of design science and their iteration, as applied in this thesis. The following are the phases of the methodology:

4.2.1.1 *Phase 1:* Problem identification and motivation

The primary research problem identified in this thesis is the lack of a framework that integrates hard security measures, such as authentication techniques, with soft security measures, such as trust-based ranking systems. Existing research considers these two categories of security measures in isolation, resulting in the absence of a comprehensive security solution.

4.2.1.2 *Phase 2:* Define the objectives for a solution

This phase describes the solutions that are applied to achieve the thesis objective of enhancing the security and trustworthiness of BW solutions using hard and soft security approaches.

4.2.1.3 *Phase 3:* Design and Development

In this phase, the artifact is designed and developed to build a comprehensive security framework for BW solutions. The artifact is systematically assessed in later phases to determine the effectiveness of incorporating hard and soft security models for improving security and trustworthiness.

4.2.1.4 *Phase 4:* Demonstration

For demonstration purposes, a prototype is developed to measure the security levels of different 2FA and MFA techniques and incorporate the results into a trust-based ranking system for BW solutions.

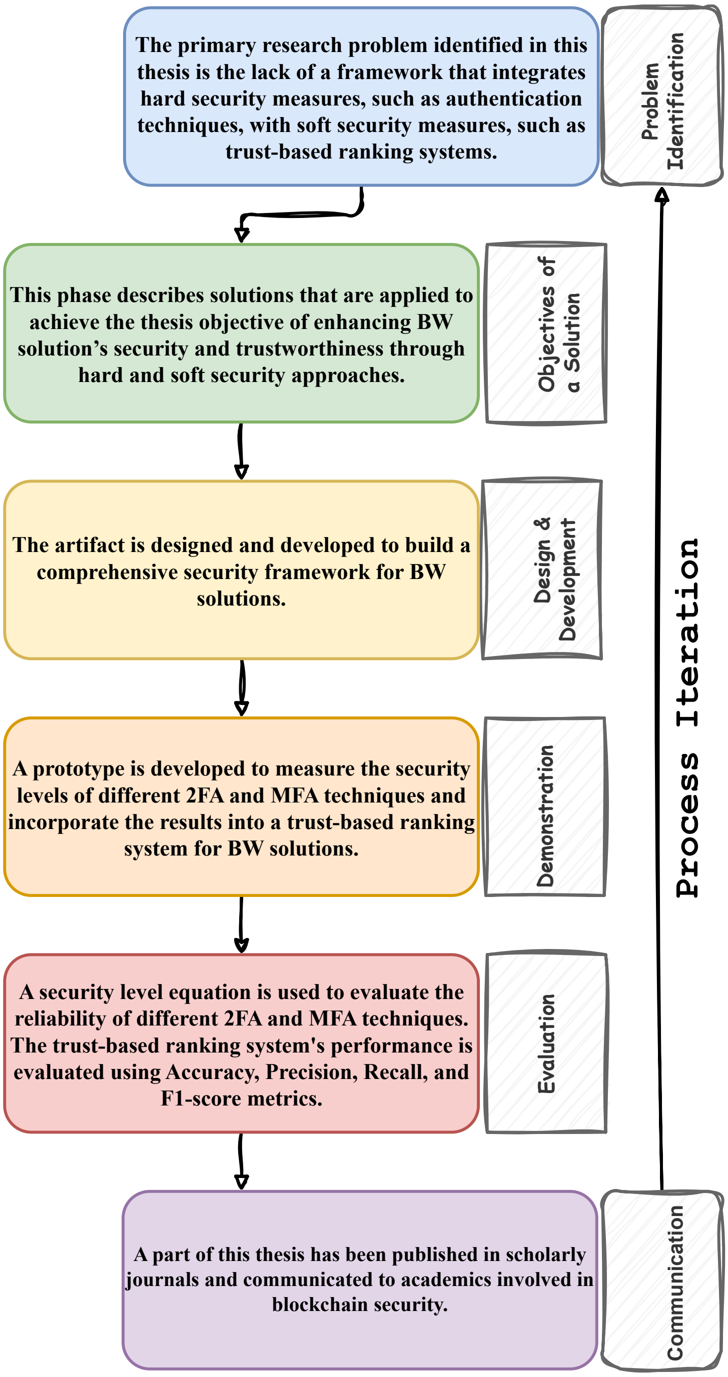

The primary research problem identified in this thesis is the lack of a framework that integrates hard security measures, such as authentication techniques, with soft security measures, such as trust-based ranking systems.
Problem Identification
This phase describes solutions that are applied to achieve the thesis objective of enhancing BW solution's security and trustworthiness through hard and soft security approaches.
Objectives of a Solution
The artifact is designed and developed to build a comprehensive security framework for BW solutions.
Design & Development
A prototype is developed to measure the security levels of different 2FA and MFA techniques and incorporate the results into a trust-based ranking system for BW solutions.
Demonstration
A security level equation is used to evaluate the reliability of different 2FA and MFA techniques. The trust-based ranking system's performance is evaluated using Accuracy, Precision, Recall, and F1-score metrics.
Evaluation
A part of this thesis has been published in scholarly journals and communicated to academics involved in blockchain security.
Communication
Process Iteration

Figure 4.1: Design Science Research Methodology

4.2.1.5 *Phase 5:* Evaluation

A security level equation is used to evaluate the reliability of different 2FA and MFA techniques. The trust-based ranking system's performance is evaluated using accuracy, precision, recall, and F1-score metrics.

4.2.1.6 *Phase 6:* Communication

A part of this thesis has been published in scholarly journals and communicated to academics involved in blockchain security.

4.3 Solution overview

As blockchain technology continues to advance, a new era of virtual transactions is emerging, with BW solutions serving as the cornerstone. However, the current body of research still lacks studies that effectively integrate both hard and soft security measures to enhance the security and trustworthiness of BW solutions. The research gaps discussed in Chapter 2 indicate that while a significant body of research has been conducted on hard security measures, such as cryptographic techniques, authentication techniques, and hardware security modules, their standalone application has proven insufficient to address the security challenges of the modern distributed computing environment. Conversely, soft security measures such as trust models have also been studied, but separately from hard security methods. These measures are intended to mitigate the risks associated with human factors, which are the weakest link in the security framework. Therefore, this section presents an overview of the proposed approach to develop a secure, intelligent, and trustworthy BW solution by combining sophisticated authentication methods and a trust-based ranking model, as shown in Figure 4.2. This section presents the overall architecture of the proposed secure and trustworthy BW framework (STBWF). Furthermore, it describes how 2FA and MFA techniques can be implemented to build a secure BW website (BWW). It provides an overview of the attack simulations used to evaluate the proposed BWW. It also provides an overview of how AI can be implemented to develop a trust-based ranking system for BW solutions (TBW-RAnk).

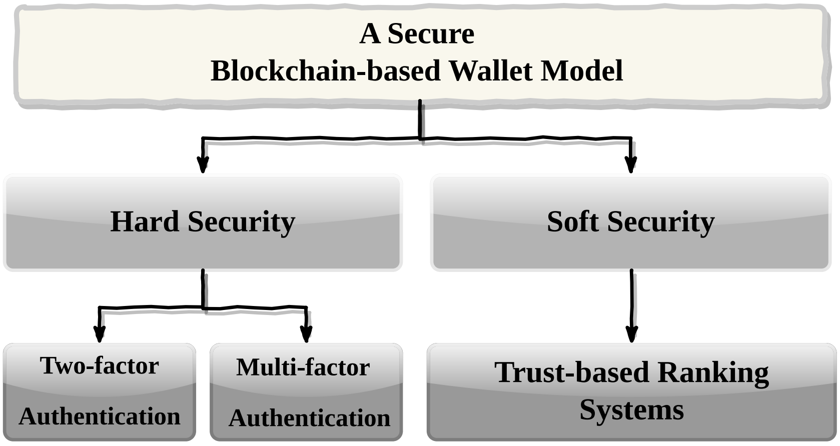


Figure 4.2: A model incorporating soft and hard security measures to secure the BW solution

4.3.1 Architecture of the proposed secure and trustworthy BW framework (STBWF:) *(Objective 1)*

The main outcome of this thesis is to design and develop a secure, intelligent, and trustworthy BW solution that not only incorporates multi-factor authentication (for hard security) but also ranks BW solutions based on their trustworthiness (for soft security). This objective introduces the proposed STBWF that facilitates prototype implementation and development, as shown in Figure 4.3. It provides abstraction layers that allow for working at a higher level of functionality to create efficient and responsive BW solutions. Detailed explanations of each layer are provided in Chapter 5.

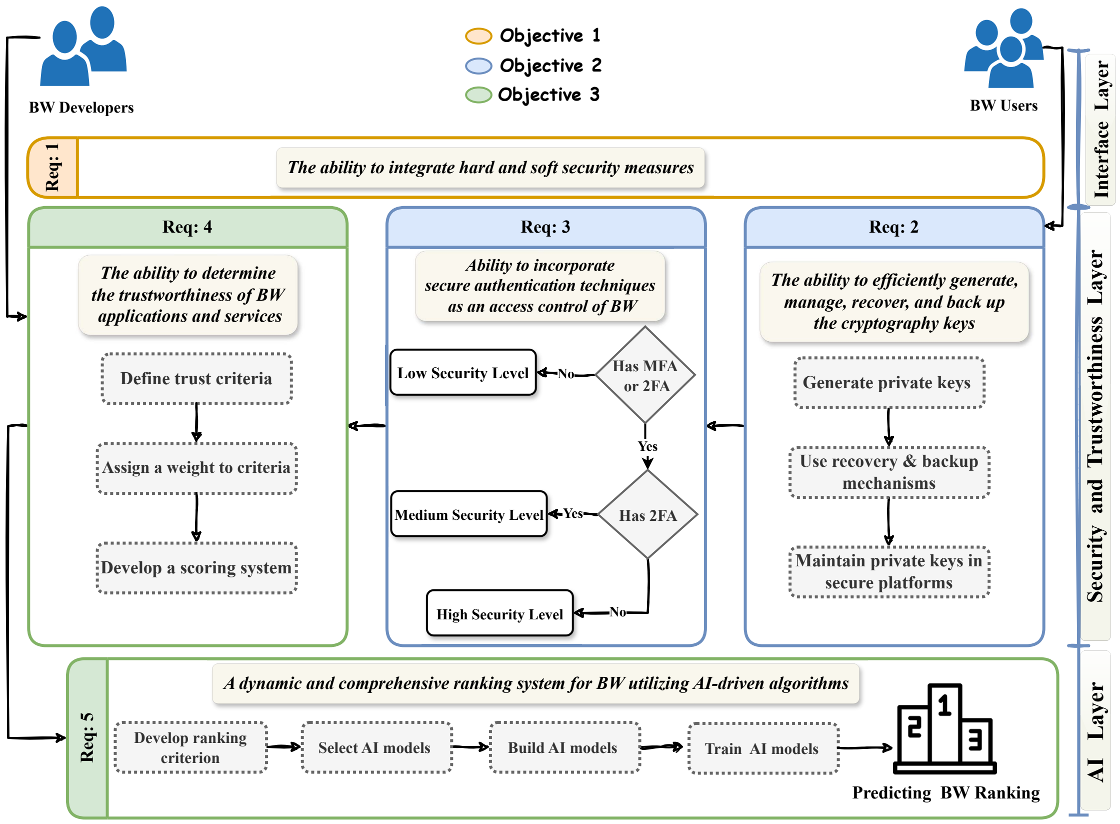

BW Developers
Objective 1
Objective 2
Objective 3
BW Users
Interface Layer
Req: 1
The ability to integrate hard and soft security measures
Req: 4
The ability to determine the trustworthiness of BW applications and services
Define trust criteria
Assign a weight to criteria
Develop a scoring system
Req: 3
Ability to incorporate secure authentication techniques as an access control of BW
Low Security Level
No
Has MFA or 2FA
Yes
Medium Security Level
Yes
Has 2FA
High Security Level
No
Req: 2
The ability to efficiently generate, manage, recover, and back up the cryptography keys
Generate private keys
Use recovery & backup mechanisms
Maintain private keys in secure platforms
Security and Trustworthiness Layer
Req: 5
A dynamic and comprehensive ranking system for BW utilizing AI-driven algorithms
Develop ranking criterion
Select AI models
Build AI models
Train AI models
1
2
3
Predicting BW Ranking
AI Layer

Figure 4.3: The proposed STBWF.

4.3.2 Solution overview of building a secure BW website (BWW:) by applying MFA techniques *(Objective 2)*

The blockchain wallet's private key is the only way to prove ownership of the wallet's valuable assets. Consequently, if these private keys are lost or stolen, the assets within the wallet become vulnerable to exploitation by malicious actors. Moreover, of the most concerning threats to BW solutions are account takeover attacks, which take advantage of human weaknesses to trick users into disclosing sensitive credentials[97]. Some account takeover attacks exploit vulnerabilities in the authentication process or compromise a user's login credentials to gain access to a BW solution. A variety of techniques can be used to execute these attacks, such as social engineering, malware, and keyloggers. Hence, due to the significant risks and potential financial loss associated with compromised BW private keys, secure authentication measures for BW solutions have become crucial. This resulted in the introduction of MFA as a security mechanism that adds layers of protection to significantly strengthen the blockchain wallet's authentication process and prevent access by unauthorized parties. Thus, developing comprehensive approaches that implement MFA in a BW solution is essential for preventing unauthorized access and protecting sensitive information.

4.3.2.1 Building and implementing the BWW:

This subsection presents a solution to the traditional (hard) security part of developing a secure, intelligent, and trustworthy BW solution. The solution introduces the BWW which incorporates four different 2FA and MFA settings to determine their effectiveness in securing the BW solutions. To accomplish this objective, a system model was developed to illustrate how the different components interact within the BW solutions. The system model consists of a user interaction and management component and a BWW component. Interaction between the BW user and the BWW is controlled by the user interaction and management component. Users can manage and control their BW solutions through the BWW component. Through this BWW, BW users can choose four different authentication settings as follows:

a) **Setting-1 (S1):** An attribute-based authentication method was implemented (only passwords).

b) **Setting-2 (S2):** A two-factor authentication method that incorporates (S1 & TOTPs) was implemented.

c) **Setting-3 (S3):** A two-factor authentication method that incorporates (S1 & face recognition) was implemented.

d) **Setting-4 (S4):** A multi-factor authentication method that incorporates S1, S2 and S3 was implemented.

The BWW was implemented using Python 3.9 and Flask to build the web application framework. The (eth_keys) libraries are used to generate cryptographic keys for the BW solutions. Authentication settings are implemented using PyOTP, a Python library that supports time-based one-time passwords. A face recognition model is also implemented using SSD MobileNet and TensorFlow for biometric authentication. A detailed explanation of each component of the system model and the experiment setup is provided in Chapter 6.

4.3.2.2 The evaluation and validation of the BWW

The evaluation and validation of this objective occurred through attack simulations. The first step is to develop a threat model to determine what scenarios might compromise BW solutions. Unauthorized access to BW solution's credentials and private keys poses a significant threat to legitimate users. Thus, it requires understanding the actors involved and the potential attack vectors. In this scenario, the user represents an authorized party with a BW account and locally stores private keys on the device. In contrast, the attacker represents a malicious party who intends to gain unauthorized access to the user's BW account. Then, a simulated account takeover attack was conducted against each authentication setting to quantitatively measure their effectiveness and resilience. The attack success rate (ASR:) metric was used to quantitatively evaluate the authentication setting's ability to withstand security attacks (see Equation 4.1). ASR is the percentage of attempts that succeed in gaining access to the BW account. A high success rate indicates vulnerabilities in a particular authentication setting and may increase the risk of BW account takeover attacks.

$$ASR = \frac{S}{S+F} \times 100 \tag{4.1}$$

where:

- S is the number of successful attack attempts.
- F is the number of failed attack attempts.

Moreover, the level of security (LS:) of each authentication setting is calculated to assess its reliability (see Equation 4.2). LS refers to the degree to which a specific authentication setting protects against BW account takeover attacks.

$$LS = \left(1 - \frac{S}{S + F}\right) \times 100 \tag{4.2}$$

where:

- S is the number of successful attack attempts.
- F is the number of failed attack attempts.

4.3.3 Solution overview of developing a trust-based ranking of BW solutions (TBW-RAnk:) using AI models *(Objective 3)*

4.3.3.1 *Stage 1:* Define trustworthiness criteria

In this stage, the factors contributing to the trustworthiness of BW solutions are determined using CCCI metrics. These factors are the characteristics or features responsible for evaluating the overall quality or performance of BW solutions. Our features include supporting MFA, accepting multiple cryptocurrencies, wallet age, currency control, user rating and security level.

4.3.3.2 *Stage 2:* Assign a weight to criteria

After identifying the criteria for assessing the quality or trustworthiness of BW solutions, each criterion is weighed based on its modes. The TBW-RAnk has two ranking modes: general ranking and customized ranking. The general ranking has an equal weight of 0.1 for all features. The customized ranking assigns a weight of 0.25 to one specific creation, while the weight for other criteria is 0.11.

4.3.3.3 *Stage 3:* Develop a scoring system

A scoring system is developed to quantify and evaluate trustworthiness and quality of the BW solutions. The weighted aggregate mathematical function, as shown in equation 4.3, determines a BW solution's overall trustworthiness score $(Trust_{(Score)})$.

$$Trust_{(Score)} = \sum_{i=1}^{n} w_i \times f_i = w_1 \times f_1 + w_2 \times f_2 + \cdots + w_n \times f_n \tag{4.3}$$

where:

- n is the number of features to be aggregated.
- w_i is the weight for the i^{th} feature.
- f_i is the value of the i^{th} feature.

4.3.3.4 *Stage 4:* Rank the BW solutions

The BW solution ranking is interpreted based on the calculated $(Trust_{(Score)})$ from equation 4.3. Five ranges are established based on specific $(Trust_{(Score)})$ threshold values, as shown in Equation 4.4.

$$Rank_{(Trust_{(Score)})} = \begin{cases} 0 & \text{if } 0 \leq Trust_{(Score)} < 0.2, \\ 1 & \text{if } 0.2 \leq Trust_{(Score)} < 0.4, \\ 2 & \text{if } 0.4 \leq Trust_{(Score)} < 0.6, \\ 3 & \text{if } 0.6 \leq Trust_{(Score)} < 0.8, \\ 4 & \text{if } 0.8 \leq Trust_{(Score)} \leq 1. \end{cases} \tag{4.4}$$

where:

- $Rank_{(Trust_{(Score)})}$ represents the ranking derived from the $Trust_{(Score)}$ value, with $Trust_{(Score)}$ being a real number in the interval [0, 1].
- The conditions in the piecewise function specify the threshold for $Trust_{(Score)}$ and the associated ranking R.

4.3.3.5 *Stage 5:* Data Generation

Synthetic datasets are generated with 10,000 BW solution records and diverse features representing various scenarios. The synthetic dataset is generated using the rule-based generation technique which defines specific rules and logic to mimic real-world BW solutions [98]. It simulates various features of BW solutions, such as support for TOTP, facial recognition, multiple cryptocurrencies, and whether the BW is custodial or non-custodial. Also, it generates a random rating for each BW solution.

4.3.3.6 *Stage 6:* Pre-process the collected data

1. **Data cleaning:** Data preprocessing involves transforming the raw dataset to ensure consistency, removing irrelevant or redundant records and converting the data into a format suitable for training AI models. This model applies normalization and scaling methods to bring features to a standard scale. Also, categorical variables holding binary choices (YES/NO) are converted to numerical values (1/0) appropriate for AI modeling.
2. **Feature engineering:** There are eight features for each BW solution, namely support TOTP, support facial recognition, multiple cryptocurrencies, wallet age, non-custodial, custodial, rating and security level. Support TOTP, support facial recognition and security level are correlated. In addition, there is a correlation between non-custodial and custodial columns. More details are provided in Section 7.3.

3. **Labeling data:** This model is designed to handle simultaneous predictions of multiple outputs. For supervised learning, nine target columns are chosen and labeled. Each labeled column has five classes. These five classes represent the trustworthiness of BW solutions based on their ranking scores. The five trustworthiness levels and their semantics are as follows: 0 is ”trustworthiness level cannot be determined,” 1 is ”significantly bad trustworthiness level,” 2 is ”bad trustworthiness level,” 3 is ”good trustworthiness level,” and 4 is ”significantly good trustworthiness level”. There is a labeled column for general ranking called ranking. There are eight labeled columns for customized ranking, namely ranking by Support TOTP, facial recognition, multiple cryptocurrencies, wallet age, non-custodial, custodial, rating, and security level.

4.3.3.7 *Stage 7:* Select AI models

The TBW-RAnk ranks BW solutions based on nine features: one for general and eight for customized ranking modes. The prediction results are nine outputs, each with five classifications representing the trustworthiness of a BW solution. This task requires the simultaneous prediction of multiple target variables. A multi-output prediction problem is commonly referred to as a multi-target prediction problem. Hence, AI model selection needs a strategic approach due to the inherent complexity of the problem. An analysis of the characteristics and requirements of the issue led to the selection of RFC, SVC and DNN models.

4.3.3.8 *Stage 8:* Building and training the models

Following the preprocessing of the dataset, it is ready for training. The dataset for RFC and SVS is divided into 80% for training and 20% for testing. For RFC, at each split in the training process, a bootstrapped sample of the training data is used to build each decision tree in the forest. Also, hyperparameter tuning techniques such as grid search or randomized search are used to identify the ideal combination of hyperparameters that maximize the model’s performance. The SVC model identifies the hyperplane that optimally separates the classes in the feature space while maximizing the margin. A hyperparameter tuning technique is used to determine the best values for the C, gamma, and kernel (radial basis function). For DNN, the dataset is divided into 80% training, 10% validation, and 10% testing. Because the problem relates to classification, categorical cross-entropy is selected as a loss function. In addition, the Adam optimizer is utilized since it is widely recognized as a method of optimization for its flexibility to massive datasets and complex designs. The softmax activation, a categorical cross-entropy loss, is used to ensure that the model can accurately predict the probability distribution over the categories. This architecture is significant for its capacity to predict many outputs simultaneously.

4.3.3.9 *Stage 9:* Evaluation and testing of the models

The models are assessed based on their accuracy, precision, recall, and F1 score, aiding in identifying and optimizing the most suitable model for multi-output problems, where each output comprises five classification classes. These metrics are crucial as they provide an extensive understanding of the model's ability to detect class imbalances, precisely classify data, and balance recall and precision and will inform the choice of the best model for the multi-output scenario. The performance metrics are as follows:

- **Accuracy:** Accuracy assesses the model's accuracy by calculating the overall proportion of correct results (including true positives and negatives) across all instances examined [99].

$$\text{Accuracy} = \frac{\text{Number of Correct Predictions}}{\text{Total Number of Predictions}} \tag{4.5}$$

- **Precision:** Precision evaluates the accuracy of the model's positive predictions that are actually true [100].

$$\text{Precision} = \frac{\text{True Positives}}{\text{True Positives + False Positives}} \tag{4.6}$$

- **Recall:** Recall assesses the model's ability to detect all relevant instances by measuring the proportion of true positives that were correctly identified [101].

$$\text{Recall} = \frac{\text{True Positives}}{\text{True Positives + False Negatives}} \tag{4.7}$$

- **F1 Score:** The F1 score combines precision and recall to provide a balanced perspective of the model's performance by calculating their harmonic mean [102].

$$\text{F1 Score} = \frac{2 \times \text{Precision} \times \text{Recall}}{\text{Precision + Recall}} \tag{4.8}$$

4.3.4 Solution overview of evaluating and validating the proposed methods *(Objective 4)*

To this end, a proof of concept prototype is developed for the proposed BW solution. The prototype validates the research questions and evaluates the approaches developed for all the previous objectives 3.4.

- For Objective 1, after designing the proposed STBWF, it is tested by developing a prototype. The prototype is incorporated, evaluated, and improved until satisfactory results that achieve the research objectives are reached.
- For Objective 2, the BWW that employs different authentication settings is implemented using Python. Attack simulations are conducted against the developed BW solution to evaluate and validate this objective. The ASR equation (Eq 4.1) is used to assess the authentication setting's ability to withstand security attacks. Also, the LS equation (Eq 4.2) is calculated for each authentication setting to quantify its reliability.
- For Objective 3, the TBW-RAnk which ranks the BW solutions based on the trustworthiness criteria is built. The model has a general and customized mode for a personalized ranking that satisfies different decision-making needs. The models are evaluated using their accuracy, precision, recall, and F1 score equations (see equations 4.5, 4.6, 4.7 and 4.8).

4.4 Chapter Summary

- This chapter discussed the research methodology used to address the research questions outlined in Chapter 3. The design science research methodology was applied. Moreover, it elaborated on the proposed solutions, processes, stages, and strategies used to achieve the research objectives.
- The next chapter (Chapter 5) proposes a trustworthy and secure BW solution framework (STBWF) and provides a detailed explanation of its components.

CHAPTER

5

A Secure and Trustworthy Blockchain-based Wallet Framework (STBWF)

5.1 Chapter Overview

Chapter 3 identifies four objectives to enhance the security and trustworthiness of BW solutions by integrating hard and soft security measures. This chapter outlines the procedures for building a secure and trustworthy BW solution framework (STBWF). The STBWF is evaluated by a BW solution prototype and the performance of the developed prototype is tested using various metrics or benchmarks. The STBWF is created in two phases, each explained and described in the following sections. The structure of this chapter is as follows: in Section 5.2, the (STBWF) is explained, along with its components. Section 5.3 presents the first phase, which is implementing four authentication settings in a BW website (BWW). Section 5.4 presents the second phase, which is building intelligent AI models that rank BW solutions in general and personalized modes based on identified criteria (TBW-RAnk). Finally, Section 5.5 concludes this chapter.

5.2 The proposed secure and trustworthy blockchain-based wallet framework

This section discusses the methodological approach used to address the gaps identified in the literature. The STBWF is designed to meet the five requirements identified in Section 2.2 to ensure the security and trustworthiness of BW solutions. The identified key requirements are considered to facilitate the development of the STBWF and achieve the thesis objectives. As shown in Figure 5.1, the STBWF consists of three layers: the interface layer, the security and trustworthiness layer, and the AI layer.

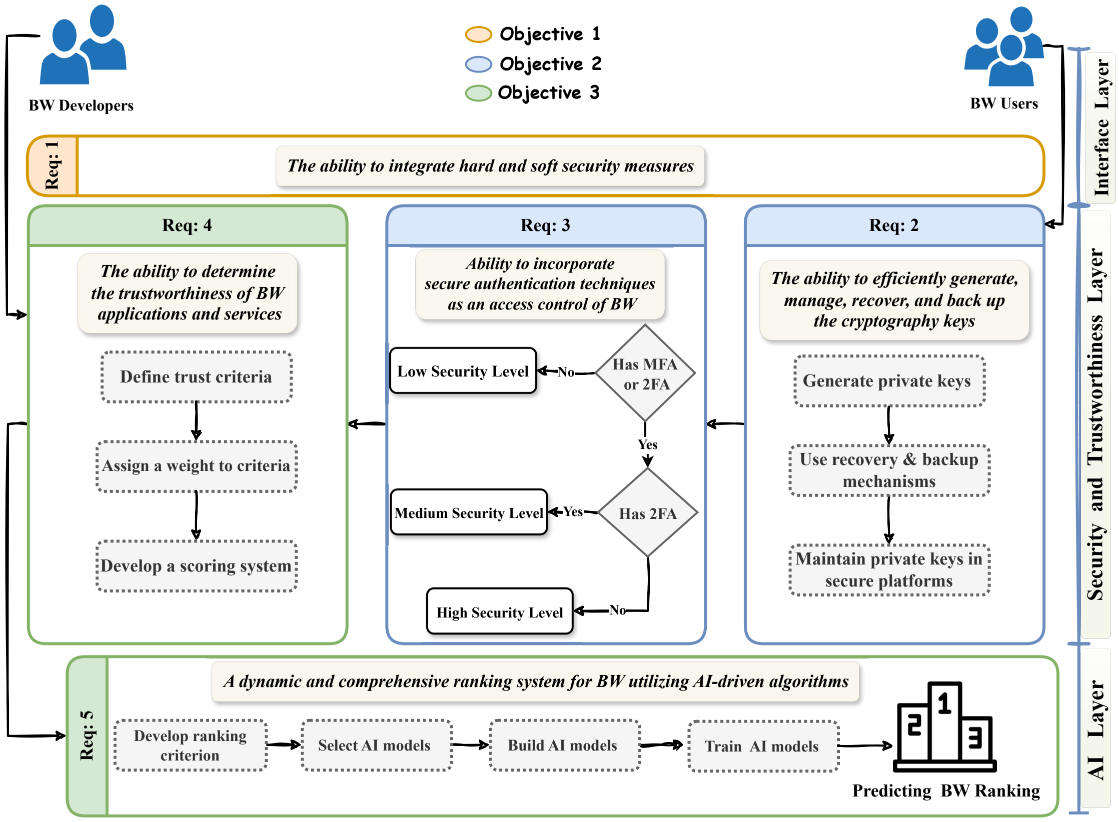

BW Developers
Objective 1
Objective 2
Objective 3
BW Users
Interface Layer
Req: 1
The ability to integrate hard and soft security measures
Req: 4
The ability to determine the trustworthiness of BW applications and services
Define trust criteria
Assign a weight to criteria
Develop a scoring system
Req: 3
Ability to incorporate secure authentication techniques as an access control of BW
Low Security Level
No
Has MFA or 2FA
Yes
Medium Security Level
Yes
Has 2FA
High Security Level
No
Req: 2
The ability to efficiently generate, manage, recover, and back up the cryptography keys
Generate private keys
Use recovery & backup mechanisms
Maintain private keys in secure platforms
Security and Trustworthiness Layer
Req: 5
A dynamic and comprehensive ranking system for BW utilizing AI-driven algorithms
Develop ranking criterion
Select AI models
Build AI models
Train AI models
2 1 3
Predicting BW Ranking
AI Layer

Figure 5.1: The proposed STBWF.

5.2.1 The Interface Layer

This layer includes the STBWF entities who are BW users and BW developers. It demonstrates hard and soft security measures to address Req: 2.2.1 for all platform users.

1. *BW users* are individuals or entities who create and use BW solutions to manage, store, and transfer digital assets. BW users who successfully create BW accounts gain the status of *BW Owners*, indicating ownership rights and administrative responsibilities. Managing BW solutions includes maintaining its cryptographic keys, monitoring the transaction history, and ensuring BW solutions are regularly updated for optimal security and functionality. Additionally, BW users can view BW solutions' ranking and customize it according to their specific preferences. This process involves selecting the appropriate type of BW solution, such as software, hardware, or paper wallet, and setting it up following the recommended security protocols.

2. *BW developers* are businesses or companies that design, develop and offer wallet applications, services, and solutions. They focus on implementing robust security measures, including encryption, authentication, and key management mechanisms. Their primary role is registering BW solutions and identifying their features for ranking.

5.2.2 The Security and Trustworthiness Layer

This layer ensures the security and trustworthiness of BW solutions, thus, it addresses (Req: 2.2.2 ,Req: 2.2.3 and Req: 2.2.4). A security measure is a mechanism used to protect BW solutions against unauthorized access, attacks, or other threats that may compromise its integrity, confidentiality, or privacy. The concept of trustworthiness encompasses many qualities, including determining the trust factor of BW solutions, which involves a comprehensive assessment of several critical factors. Also, the STBWF employs secure mechanisms to generate public-private key pairs using proven cryptographic algorithms such as elliptic curve cryptography and RSA. In addition, managing private keys is an essential component of BW solutions as it ensures the security of cryptographic keys. Additionally, the STBWF applies effective fundamental recovery mechanisms, allowing BW users to restore access using recovery phrases or seed words in case of private key loss or device failure. A reliable key backup mechanism is implemented to enhance the resilience of STBWF. BW users can retrieve their keys securely in the case of hardware failure or loss using encrypted backups stored online and offline.

Moreover, BW solutions can be made highly secure and trustworthy by carefully examining the security features, including encryption methods and multi-factor authentication. As part of this layer, 2FA and MFA are introduced with different factors, such as TOTP and facial recognition, to prevent unauthorized access. This mechanism adds different security levels (low, medium, high) and ensures that the BW authentication process is enhanced and strengthened. These multiple factors significantly reduce the possibility of malicious actors gaining access to BW accounts, even if account passwords are compromised.

In addition, in the STBWF, a standard scoring mechanism is developed that objectively evaluates different BW solutions. The first step is identifying key trust factors to assess the security and trustworthiness of a BW solution. These factors include authentication security level, wallet age, number of supported cryptocurrencies, and cryptocurrency control. Once the criteria are identified, the next step is to assign weightings to each criterion based on its relative importance.

5.2.3 The AI Layer

A generalized and personalized ranking system that addresses the complexity and dynamic nature of BW solutions requires AI models to be capable of identifying patterns and adapting to emerging changes. To address Req: 2.2.5, AI models are implemented to accurately predict the ranking of BW solutions based on the trustworthiness score from Req: 2.2.4. Thus, a new level of intelligence is introduced, which enables the STBWF to recognize context, understand user preferences and refine rankings in real time. Also, a strategic approach to model selection is needed to personalize the STBWF and predict multiple target variables simultaneously. After an analysis of the characteristics and requirements of the issue, DNN, RFC and SVC models are identified as the most appropriate solution to this problem [103]. They can capture complex relationships and patterns within the dataset and they align well with the diverse aspects of BW solutions interactions. In the context of personalized ranking for BW solutions, the STBWF enables different features to be assigned varying levels of importance. It can continuously learn and adapt to changing user behavior and market conditions. In contrast to static ranking algorithms, these AI models provide BW users with the most relevant and suitable options in real time. The dynamic nature of this approach is instrumental in the rapidly evolving field of blockchain technology and cryptocurrencies.

5.2.4 The STBWF Implementation Phases

To implement the STBWF efficiently, the implementation is divided into two phases:

1. **Phase One:** In this phase, objective 2 is addressed by building a blockchain wallet website (BWW) with 2FA and MFA techniques. The BWW allows BW owners to configure four authentication settings that suit their security needs. This personalized approach grants BW owners control, offering primary, 2FA or advanced MFA through TOTP and biometrics. The BWW establishes a secure and accessible BW solution for interacting with blockchain networks. More details regarding this phase are in Section 5.3.

2. **Phase Two:** In this phase, objective 3 is addressed by developing a trust-based ranking system for BW solutions called TBW-RAnk using AI models. BW users can make informed decisions on which BW solution to use based on the BW-Rank, which considers security measures, BW features, and user experience. The TBW-RAnk has two operational modes. A general mode, which provides standard evaluations for BW solutions, is designed to meet the needs of broader BW users. A customized or personalized mode allows BW users to adjust the ranking criteria in accordance with their security preferences, desired features, and virtual asset interests. This ensures a tailored experience that aligns with broader BW users' interests and requirements within the blockchain community. This phase is explained in Section 5.4.

5.3 *Phase One:* Building the BWW with four authentication settings

In this phase, objective two is addressed through the identified key requirements (Req: 2.2.2 and Req: 2.2.3) to build a reliable BW solution with sophisticated authentication settings. The BWW allows BW users to engage with blockchain networks. Building a secure BWW represents the first phase of the STBWF. Req: 2.2.2 is a core component that should be considered when building BW solutions. Req: 2.2.3 is the additional security mechanism for controlling access to a BW solution. As shown in Figure 5.2, the following procedures occur in this phase:

i) **Step 1:** BW users visit the BWW and choose their rules.

ii) **Step 2**: If they are new users, they must register to create an account by entering their email addresses and passwords.

iii) **Step 3:** While creating an account, the wallet system automatically generates the BW address and private key.

iv) **Step 4:** When generating a wallet, the wallet users are given the backup procedure which includes creating a backup phrase or mnemonic, a word list serving as a backup for private keys.

v) **Step 5:** The BW owners securely maintain their private keys and backup phrases in offline locations and avoid sharing them.

vi) **Step 6:** If they are BW owners, they can log in by providing the required information, such as email address and password, and follow any additional verification steps, such as entering TOTP or facial data.

vii) **Step 7:** After logging in, BW owners can configure their authentication settings and select different factors, such as passwords, TOTP, and facial recognition.

viii) **Step 8:** BW owners can evaluate and rate BW solutions using a 5-star rating system.

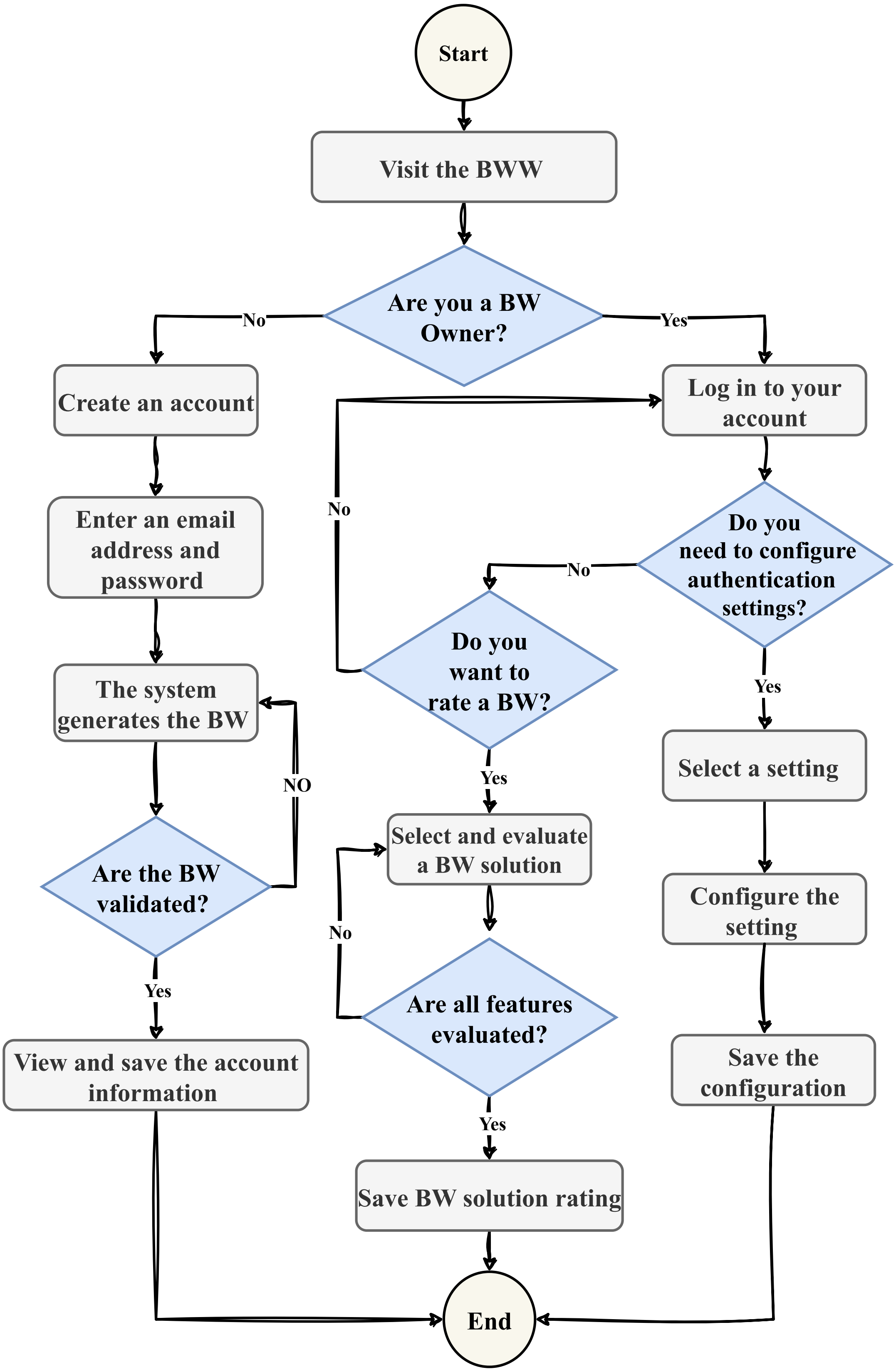

Start
Visit the BWW
Are you a BW Owner?
No
Yes
Create an account
Log in to your account
Enter an email address and password
No
Do you need to configure authentication settings?
No
Do you want to rate a BW?
The system generates the BW
Yes
Yes
Select a setting
NO
Select and evaluate a BW solution
Are the BW validated?
Configure the setting
No
Are all features evaluated?
Yes
View and save the account information
Save the configuration
Yes
Save BW solution rating
End

Figure 5.2: Phase One: Building the BWW

5.4 *Phase Two: Building the TBW-RAnk*

In this phase, objective three is addressed through the identified key requirements (Req: 2.2.4 and Req: 2.2.5) for ranking BW solutions in general and in customized modes. The ranking system allows BW users to carefully evaluate and select wallets in accordance with their security and trustworthiness needs. Ranking BW solutions is the second phase of the framework. Req: 2.2.4 identifies the trustworthiness factors that are considered when ranking the BW solutions. Req: 2.2.5 is the intelligent AI model that allows BW users to view general rankings or personalize them by selecting the most relevant security and trustworthiness features. This phase involves the following procedures, as shown in Figure 5.3:

i) **Step 1:** BW developers register BW solutions and identify their features.

ii) **Step 2:** The AI model uses the identified features for each BW solution to predict the ranking.

iii) **Step 3:** BW users can view the general ranking mode if they do not have a specific feature.

iv) **Step 4:** BW users can select the customized ranking mode if interested in a specific feature.

v) **Step 5:** BW users select from the BW solution features, including support TOTP, facial recognition, multiple cryptocurrencies, wallet age, non-custodial, custodial, rating and security level.

vi) **Step 6:** The AI model takes the entered feature, generates a personalized ranking prediction, and presents it to the BW users for review.

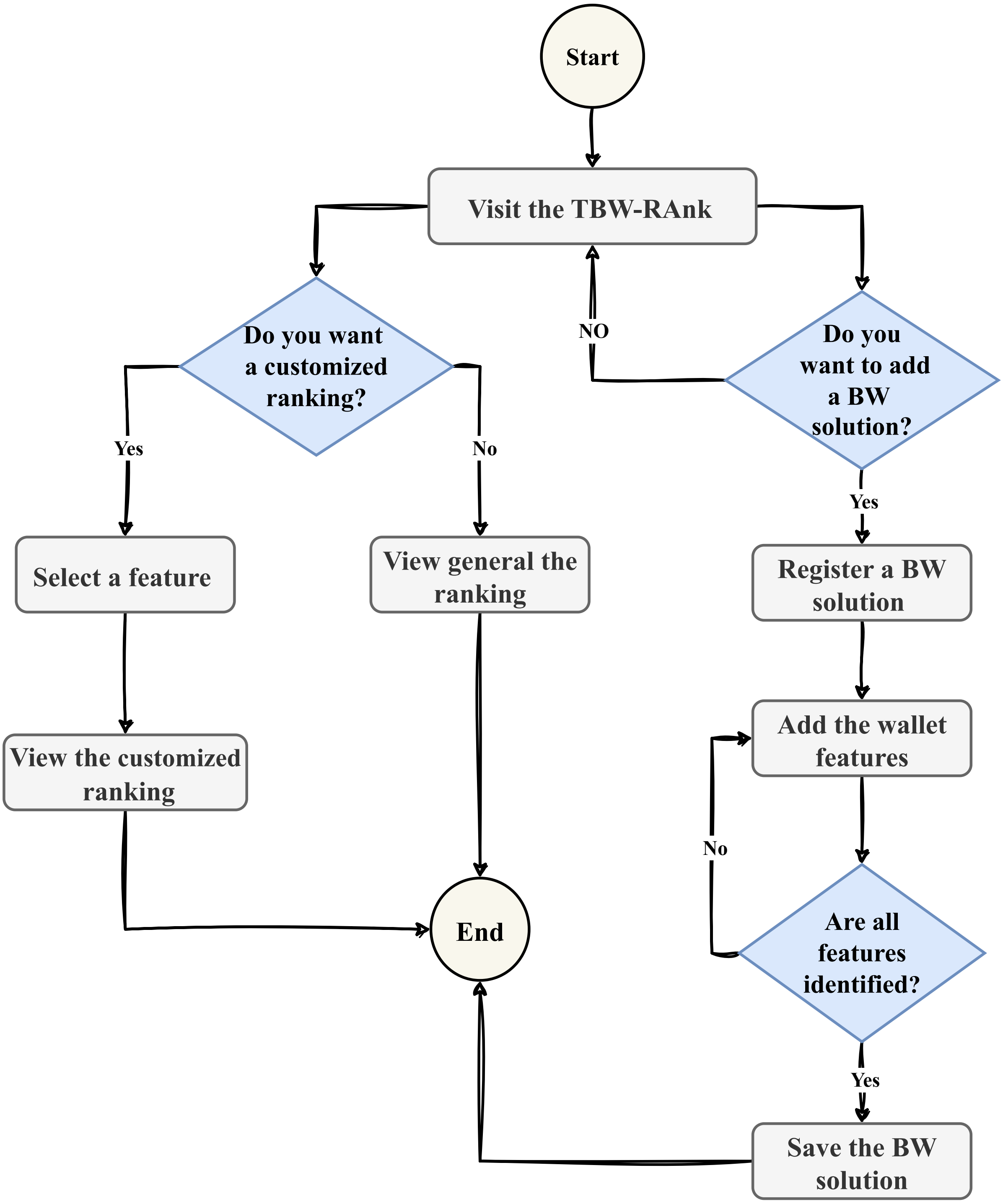


Figure 5.3: Phase Two: Building the TBW-RAnk

5.5 Chapter Summary

- This chapter describes the processes for creating a reliable and secure BW solution framework called STBWF to achieve objective 1. Five requirements were identified to facilitate the development of BW solutions. The proposed STBWF consists of three layers: the interface layer, the security and trustworthiness layer, and the AI layer. Each layer was illustrated and discussed in detail.
- The next chapter (Chapter 6) describes the creation of the BWW with four different authentication settings to develop an effective BW solution for managing private keys and digital assets.

Chapter

6 Building a Secure BW Website (BWW) with 2FA and MFA Mechanisms

6.1 Chapter Overview

Chapter 4 outlined the methodology that was applied to achieve the thesis objectives. Chapter 5 introduced the STBWF to implement a secure and trustworthy BW solution. The framework integrates hard security measures as authentication techniques and soft security measures as trust-based ranking systems, ensuring a robust defence mechanism while fostering BW user trust. This chapter details the implementation of the hard security measures for BW solutions. A systematic approach is employed to facilitate the integration and implementation of the four 2FA and MFA into a BW website (BWW:), including TOTP and face recognition. Additionally, the chapter outlines the validation and evaluation results of the proposed STBWF. The environment, software, and framework employed throughout the implementation, validation, and evaluation processes are as follows:

- **Python [1]:** Python is a high-level, interpreted programming language known for its simplicity, flexibility and readability. It supports a variety of programming paradigms, including procedural, object-oriented, and functional programming. Also, it is a prominent language for web development, data analysis, artificial intelligence and other applications [104].

- **Flask [2]:** Flask is a lightweight WSGI (Web Server Gateway Interface) framework that facilitates web application development in Python. Its simplicity and fine-grained control make it relevant for small to medium-sized web applications and services [105].

[1] https://www.python.org

[2] https://flask.palletsprojects.com

- **PyCryptodome [3]:** PyCryptodome is a standalone Python module that offers cryptographic services. It is a fork of PyCrypto that improves the original package in several ways, such as adding new cryptographic primitives and more secure modules. It is employed for safe communication, authentication, and data storage [106].

- **Eth_keys [4]:** Eth_keys is a Python library that manages cryptographic keys inside the Ethereum ecosystem. It offers resources for generating, modifying, and utilizing public and private keys, essential for securing transactions and interactions on the Ethereum network. It is a component of an extensive toolkit for Ethereum's public-key cryptography system [107].

- **PyOTP [5]:** PyOTP is a Python library that generates and verifies one-time passwords (OTPs). It implements a time-based one-time password and the HMAC-based one-time password algorithms. It is commonly employed in MFA systems to provide an additional layer of security [108].

- **SSD MobileNet:** The single shot multiBox detector (SSD) MobileNet is an architecture for object detection in images and video streams utilizing a deep neural network. MobileNet is a lightweight deep neural network architecture for mobile and embedded applications. SSD and MobileNet provide an efficient framework for object detection suitable for real-time processing [109].

- **TensorFlow [6]:** TensorFlow is an open-source machine learning and deep learning application developed by Google. It is a powerful tool used by many professionals, including data scientists, software developers, and researchers, to simplify the process of building, training, and deploying AI models [110].

- **SET :** The Social Engineering Toolkit is an open-source penetration testing framework for social engineering. It provides diverse tools to simulate attacks leveraging human psychology and social tactics to gain unauthorized access to systems, sensitive data, or information. It is utilized for security training and testing the human factor of security approaches [111].

- **Metasploit Framework [7]:** The Metasploit Framework is an open-source platform for developing, testing, and executing exploits. It provides extensive tools and resources

[3] https://pypi.org/project/pycryptodome
[4] https://pypi.org/project/eth-keys
[5] https://pypi.org/project/pyotp
[6] https://www.tensorflow.org
[7] https://www.metasploit.com

for security experts and researchers to conduct penetration testing and security audits. Metasploit identifies vulnerabilities, developing and executing exploit code, and testing defence mechanisms in a controlled and legal environment [112].

The structure of this chapter is as follows: Section 6.2 describes the development of a detailed system model for the BWW. The primary goal is to build a resilient architecture that integrates enhanced authentication mechanisms and addresses the critical concerns in BW solutions. Section 6.3 discusses the implementation of the BWW and the integration of advanced authentication methods, such as 2FA and MFA, which serve as a defence against unauthorized access. Section 6.4 evaluates and validates the proposed BWW. Risk analysis, threat modeling, and attack simulation approaches are used to identify potential vulnerabilities and determine the system's resilience against sophisticated phishing attacks. Section 6.5 presents a detailed discussion of the results obtained from our security evaluation and highlights the level of security of each authentication setting identified during the assessment. Section 6.6 concludes this chapter.

6.2 The development of the proposed BWW:

Systematic and comprehensive approaches are required to facilitate the integration and implementation of MFA in BW solutions, preventing malicious access and protecting sensitive data [113]. Unfortunately, a limited number of comprehensive studies have been conducted to explain how MFA, specifically biometrics, can be implemented in BW solutions. The methodology and procedures associated with this implementation are not well documented for either businesses or developers. This section aims to fill this knowledge gap by investigating the implementation of MFA in BWs. It proposes a BWW that provides a secure platform for users to effectively manage and control their cryptographic keys and digital assets. A key component of the design process is to develop a detailed system model that incorporates four authentication settings. This system model provides a conceptual representation of how the different components of the BWW interact.

6.2.1 The system model of the proposed BWW:

A system model provides a conceptual representation of how the different components of a system interact with one another, which assists developers in understanding how future changes to the system will affect it [114]. The proposed system model comprises a user interaction and management component and a BWW component, as shown in Figure 6.1. The user interaction and management component controls BW users' interactions with the BWW. On the other hand, the BWW component provides a secure platform for users to manage and control their BW solutions. Following is a detailed explanation of each component:

6.2.1.1 User Interaction and Management

This section discusses the ways in which BW users interact with the system to manage and maintain their cryptographic keys. This includes explaining the process to be followed by the BW users to register, log in and store BW data, and for private keys to be stored securely. The section explains the following two components:

1. **User Interface (UI):** The front-end application is used for BW users' registration, login, key generation, and authentication. Furthermore, users can view their transaction history and check their BW balances. Through this interface, users have access to the following features:

   a) *User Registration and BW Creation:* Users initiate the registration process by providing the necessary information. After verifying the information provided and ensuring its validity, the system creates a BW user account containing cryptographic keys. The

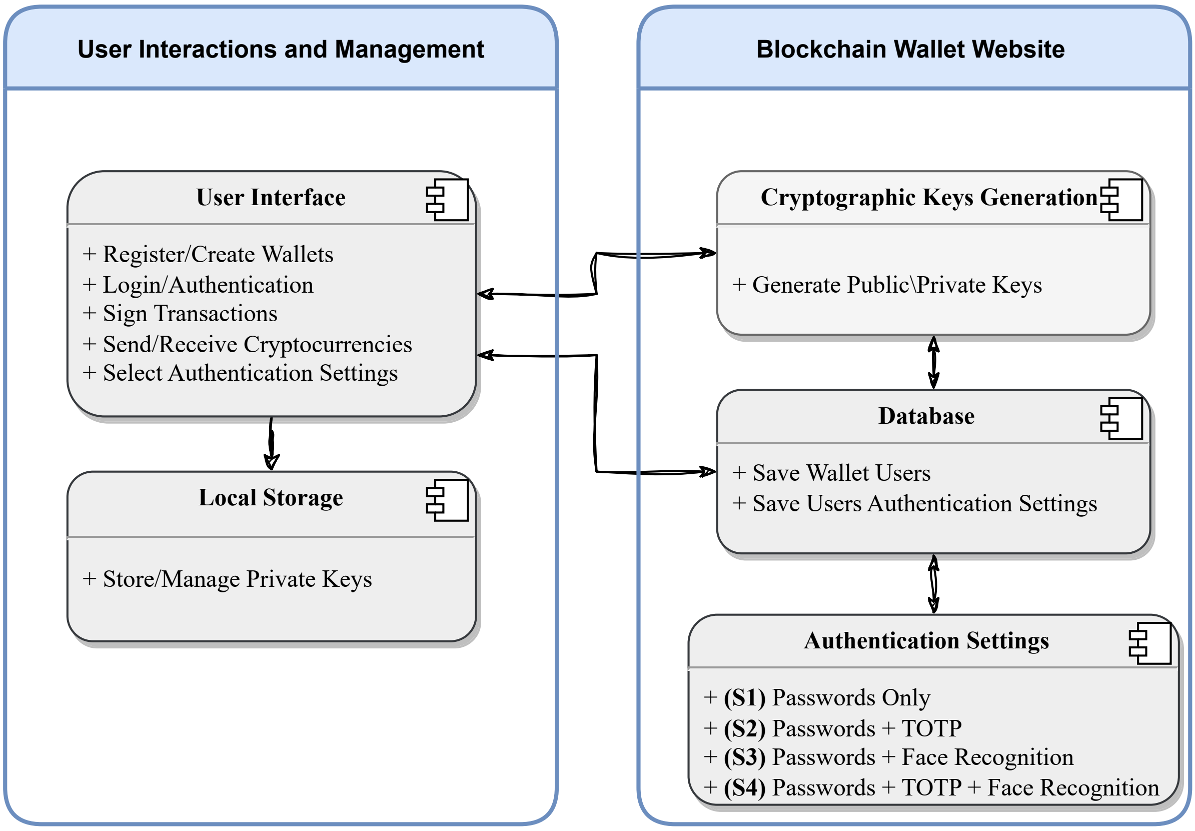

User Interactions and Management
User Interface
+ Register/Create Wallets
+ Login/Authentication
+ Sign Transactions
+ Send/Receive Cryptocurrencies
+ Select Authentication Settings
Local Storage
+ Store/Manage Private Keys
Blockchain Wallet Website
Cryptographic Keys Generation
+ Generate Public\Private Keys
Database
+ Save Wallet Users
+ Save Users Authentication Settings
Authentication Settings
+ (S1) Passwords Only
+ (S2) Passwords + TOTP
+ (S3) Passwords + Face Recognition
+ (S4) Passwords + TOTP + Face Recognition

Figure 6.1: System model components of the BWW

system also creates a new BW for the registered user and saves it to the database. Public and private keys are generated during BW creation. The users' private keys, on the other hand, provide access and control over their BWs and digital assets. The public key serves as an address for receiving digital assets, which allows seamless transfers between BWs. Algorithm 1 outlines the steps in generating a BW for a user, securely managing the BW's sensitive components, and storing it in a database.

b) *Select authentication settings:* An easy-to-use interface allows users to manage their authentication methods, including setting up two-factor or multi-factor authentication, such as passwords, time-based one-time passwords (TOTP), or facial recognition.

c) *Login and authentication:* The user initiates the login process by accessing the BWW login page. Depending on the user's authentication settings, the user provides their email address and password in the designated input fields. After receiving the login credentials, the web server performs a series of checks to verify the user's identity. The user can access the BW account if the entered credentials match those in the database.

Algorithm 1 Create a Blockchain Wallet

```
Require: User registration with a valid email address
Ensure: Wallet object containing a $privateKey, publicKey, BWaddress$
Validate the provided email address for registration
Register the BW user and associate the email address with the new BW account
Import secrets, eth_keys, and eth_utils or pycryptodome
Generate a secure random 32-byte hexadecimal string for the private key using secrets.token_hex(32).
$privateKey \leftarrow$ ”0x” + secrets.token_hex(32)
Create a PrivateKey object from the hexadecimal private key using
    $account \leftarrow$ eth_keys.keys.PrivateKey(bytes.fromhex($privateKey[2:]$))
Derive the public key from the private key object using
    $publicKey \leftarrow$ account.public_key.to_bytes().hex()
Apply the Keccak-256 hash function to the public key bytes using eth_utils.keccak
Extract the last 40 characters of the hash as the account address using
    $address \leftarrow$ ”0x” + keccak($publicKey$).hex()[-40:]
Save the user’s wallet account (public key and BW address) in the database.
Securely save the private key to a file.
Make the private key file available for a one-time download by the BW owner.
return BW object associated with the user’s registered email address, confirming the successful storage and availability of the private key for download.
```

Algorithm 2 details the steps in authenticating a BW owner based on the authentication settings.

d) *Sign and send transactions:* The sender creates a transaction by entering the recipient’s address and the amount to be sent. After processing the transaction data, a hash function creates a unique transaction hash that serves as a digital fingerprint and is used as a reference. A digital signature is generated with the user’s private key, mathematically binding the transaction data to the private key to prove the transaction is authentic and legitimate. Then, the digitally signed transactions are broadcast to the blockchain network for verification.

2. **Local Storage:** Users can securely store their private keys locally on their devices, enabling them to have full control of their cryptocurrencies and sign transactions without the involvement of third parties.

Algorithm 2 User Login and Authentication Process

```
Require: Provide the email and password
Validate the email and password:
if form is submitted and valid then
    Proceed to authenticate the user.
else
    Keep on login page for correction.
end if
User Lookup:
Attempt to find user by email in the database.
if no user found or password incorrect then
    Flash error message and redirect to login.
end if
authentication_setting handling:
if user's authentication_setting == S1 (Standard Login) then
    Log user in.
else if user's authentication_setting == S2 (TOTP) then
    Redirect to OTP authentication page.
else if user's authentication_setting == S3 (Biometric) then
    Redirect to biometric authentication page with Face Recognition.
else if user's authentication_setting == S4 (TOTP + Face Recognition) then
    Redirect to OTP and biometric authentication pages.
else
    Log user in.
end if
```

6.2.1.2 The BWW:

This section describes the functionalities provided by the BWW. An individual can communicate with a blockchain network through a BW, which serves as a bridge between users and the blockchain network. The BWW has the following features:

1. **Generate Public & Private Keys:** BWs generate private and public key pairs by employing asymmetric cryptography algorithms, such as elliptic curve cryptography. A secure random number generator is used to create a private key, which is then multiplied by an elliptic curve function to calculate a public key. The BW address is then derived from the public key utilizing a cryptographic hash function like SHA-256 or RIPEMD-160, transforming the public key into a compressed, fixed-length string.

2. **Database:** Databases that are well-designed and adequately secured store and manage the BW users' information, including email addresses, encrypted passwords, authentication settings, and BW addresses.

3. **Authentication Settings:** After receiving the login credentials, the web server verifies the user's identity based on their authentication settings stored in the database. Figure 6.2 shows a flowchart of the workflow of each authentication setting. Users can use single-factor authentication (only passwords) or multi-factor authentication (TOTP or face recognition). When only passwords are utilized, the email address and password are compared against the stored user data. Access is granted if the password is correct; otherwise, access is denied. Additionally, when TOTP is applied, the user is required to enter a verification code sent to their device. The verification code is generated using a secret key shared between the authentication server and the user's device. After the code is entered, the authentication process is validated, and the user is granted access to the BW account. Access is denied if the verification code is incorrect, requiring another attempt. When the face recognition method is implemented, the user is required to provide a facial scan for verification. If the scanned face matches the face data stored in the database, the authentication process is successful, granting access to the BW account. However, if the scanned face fails to correspond with the stored data, the authentication process is denied, restricting access to the BW account.

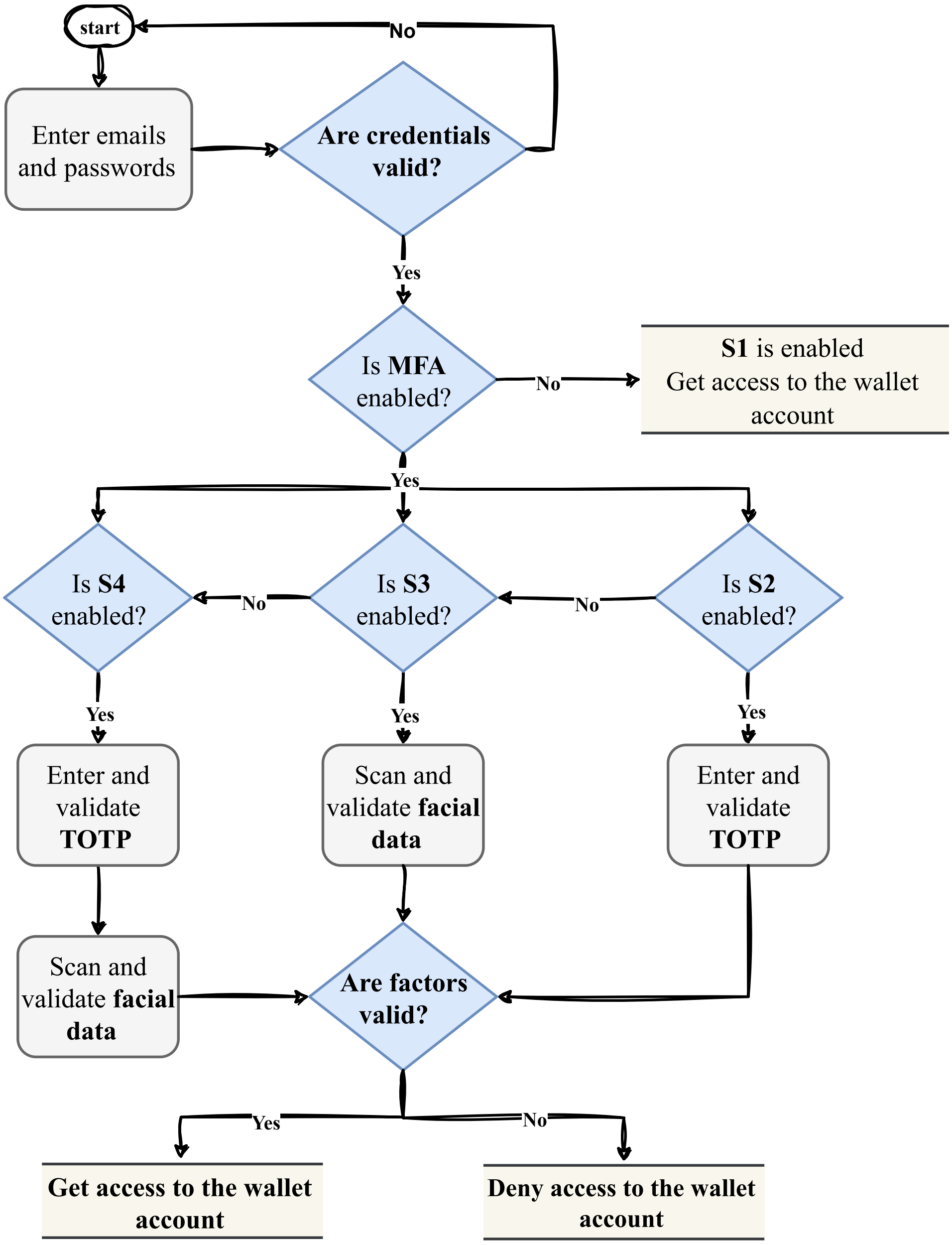


Figure 6.2: The workflow of the authentication settings

6.3 Experiment Setup and Implementation of the proposed BWW

This section outlines the experiment's configuration process and the BWW's operational environment. It also details the implementation and testing of each authentication setting, incorporating algorithms for a detailed analysis and providing visual evidence through screenshots to demonstrate their functionality.

6.3.1 Experiment Setup

We created a BWW with different authentication settings to capture their effectiveness in securing BW solutions. The following is a detailed description of the experiment setup used.

6.3.1.1 Building the BWW

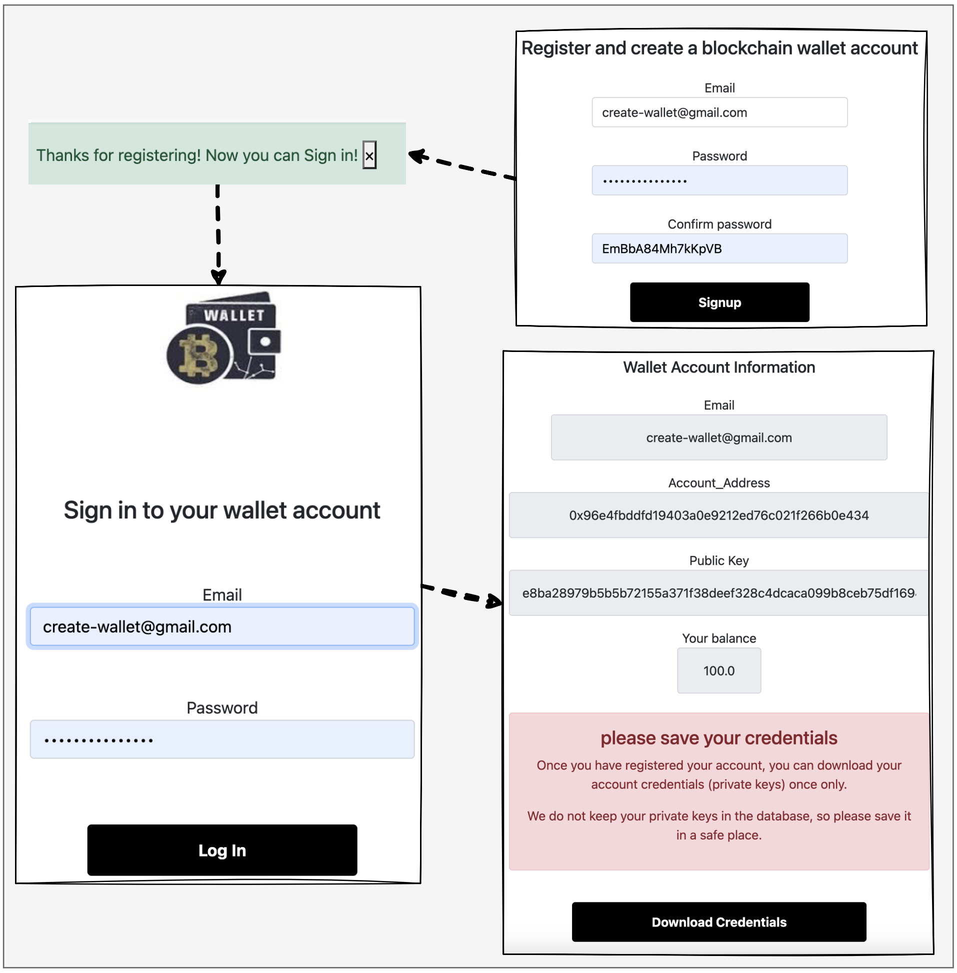
1. *The BWW framework:* We created the BWW in a virtual environment using Python 3.9 as a programming language and Flask 2.2 as a web framework. Python was chosen since it has extensive libraries and frameworks that can be used to build various aspects of the BWW. For example, PyCryptodome is used to perform cryptographic operations, and HTTP requests are used to interact with blockchain networks. The BBW code link can be found in Appendix A.4.

2. *Generating BWs (public&private key pairs):* We used Ethereum and public-key cryptography packages to ensure that the integration of the blockchain functionalities into our applications is convenient. Furthermore, we utilized the Ethereum Keys library (eth_keys), an Ethereum-based software package for working with cryptographic keys. It provides various functions such as creating BW accounts, generating public keys from private keys, signing transactions, and verifying signatures. The screenshot for registering and creating a BW account for users is shown in Figure 6.3.

6.3.1.2 Implementing authentication settings

As shown in Figure 6.4, BW users can select four different authentication settings after registering on the BWW. Details on how each setting is implemented are as follows:

1. **Setting-1 (S1):** We implemented an attribute-based authentication method (only password). We utilized Flask-Login, a Python library that simplifies the implementation



Register and create a blockchain wallet account

Email
create-wallet@gmail.com

Password
•••••••••••••••

Confirm password
EmBbA84Mh7kKpVB

Thanks for registering! Now you can Sign in!

Sign in to your wallet account

Email
create-wallet@gmail.com

Password
••••••••••••••••

Wallet Account Information

Email
create-wallet@gmail.com

Account_Address
0x96e4fbddfd19403a0e9212ed76c021f266b0e434

Public Key
e8ba28979b5b5b72155a371f38deef328c4dcaca099b8ceb75df169

Your balance
100.0

please save your credentials

Once you have registered your account, you can download your account credentials (private keys) once only.

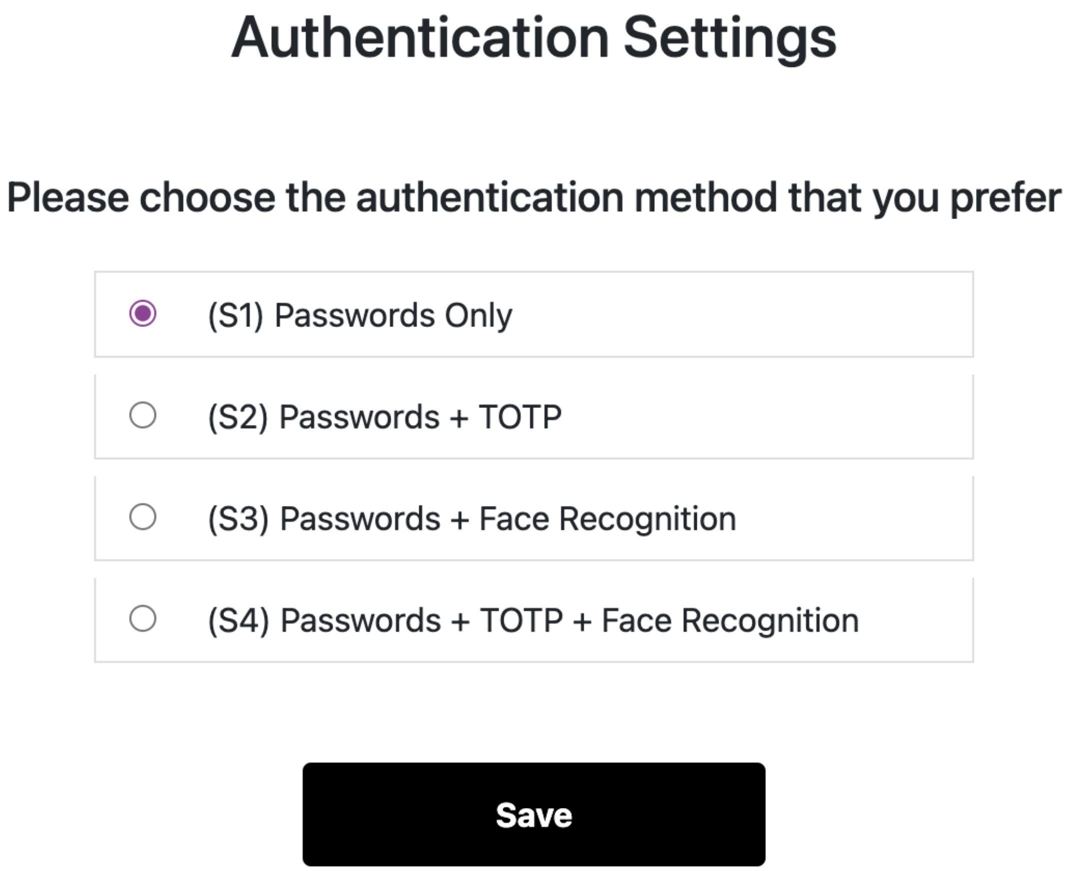
We do not keep your private keys in the database, so please save it in a safe place.

Figure 6.3: A screenshot of registering and creating a BW account for users.

of user authentication and provides an intuitive and secure method of managing user sessions.

2. **Setting-2 (S2):** We implemented a multi-factor authentication method that includes S1 & TOTPs. To generate and validate OTPs, we used PyOTP, a Python library that supports TOTPs. We also used Pyqrcode, a Python library, to generate QR codes to make it easy for users to authenticate themselves. It is necessary for users to install Google Authenticator or Auth on their devices to configure the authentication settings.

3. **Setting-3 (S3):** We implemented a multi-factor authentication method that includes S1 & face recognition. We used SSD MobileNet and TensorFlow for biometric authentication to implement our face recognition model. As part of the face recognition authentication, users are typically required to provide access to their faces through a camera. This can be done by taking a picture of their face and securely saving their feature vector values in



Authentication Settings

Please choose the authentication method that you prefer

● (S1) Passwords Only

○ (S2) Passwords + TOTP

○ (S3) Passwords + Face Recognition

○ (S4) Passwords + TOTP + Face Recognition

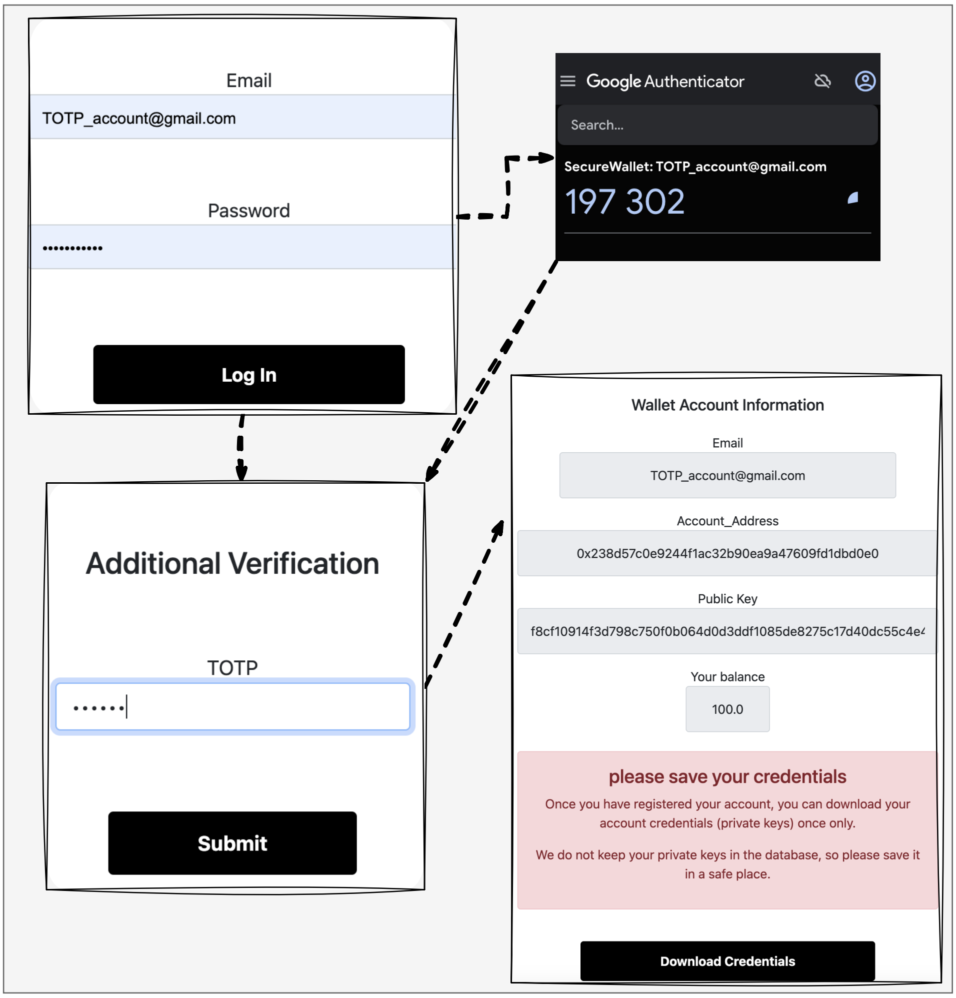
Figure 6.4: A screenshot of authentication settings

the database.

4. **Setting-4 (S4):** We implemented a multi-factor authentication method that includes S1, S2 and S3.

6.3.2 Testing the functionality of the authentication settings

We conducted a practical test for each authentication setting to ensure the authentication mechanisms are consistent and functioning as expected. *T*he S1 setting was tested by entering a valid email and password, an invalid email and password, a valid email and invalid password, and an invalid email and valid password. We expect the BWW will allow access only if the email address and password are valid and will display appropriate error messages for all other cases. The outcome was in accordance with what was expected.



Email
TOTP_account@gmail.com

Password
•••••••••••

SecureWallet: TOTP_account@gmail.com
197 302

Additional Verification

TOTP
••••••

Wallet Account Information

Email
TOTP_account@gmail.com

Account_Address
0x238d57c0e9244f1ac32b90ea9a47609fd1dbd0e0

Public Key
f8cf10914f3d798c750f0b064d0d3ddf1085de8275c17d40dc55c4e4

Your balance
100.0

please save your credentials

Once you have registered your account, you can download your account credentials (private keys) once only.

We do not keep your private keys in the database, so please save it in a safe place.

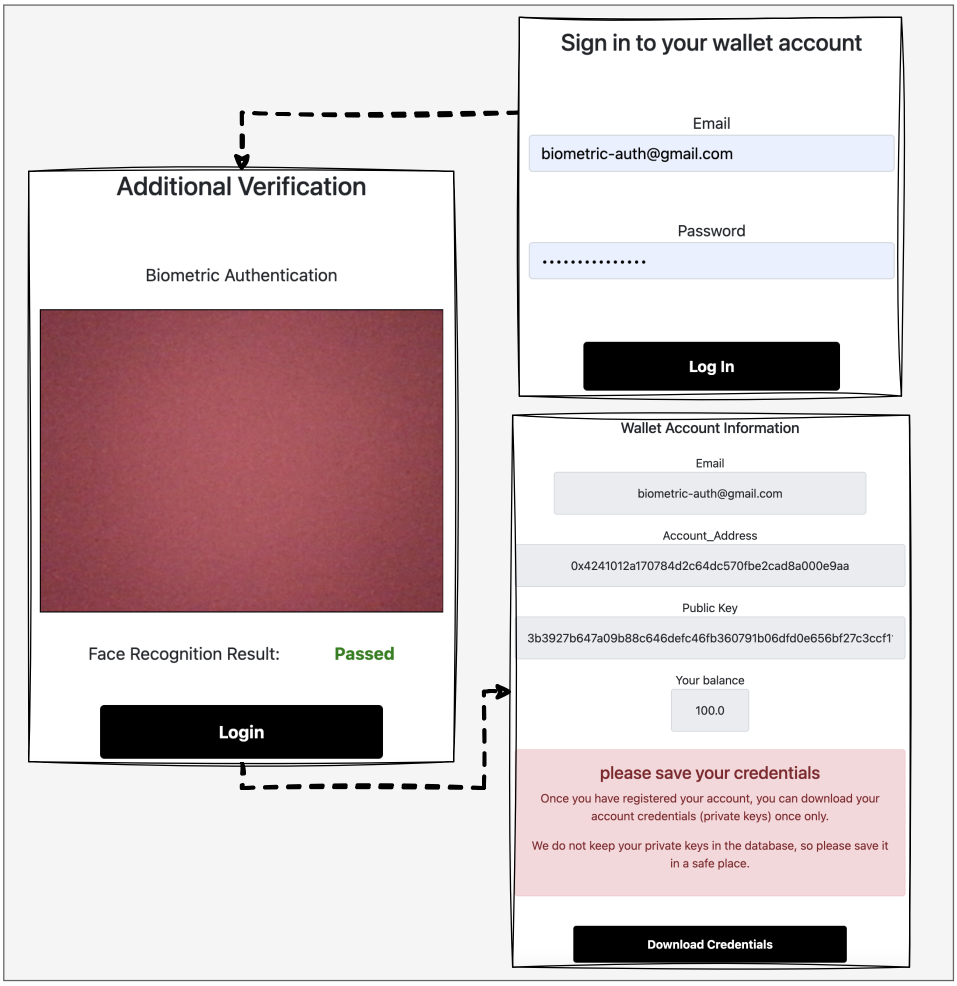
Figure 6.5: A screenshot of the S2 setting

*T*he S2 setting was tested by entering a valid email, password, and TOTP, and a valid email, password, and an invalid TOTP. The BWW should only allow access when the username, password, and TOTP are valid. The outcome was as expected. Figure 6.5 illustrates the testing of the S2 setting from sign-in to accessing the BW credentials.

We tested the *S3 setting* by entering a valid email address, password, and face scan and a valid email address, password, and an invalid face scan. The BWW should only allow access when the username, password, and face scan are valid. The results were as expected. The screenshot for testing the functionality of the S3 setting is shown in Figure 6.6.

For *t*he S4 setting, since previous settings were tested separately, we entered a valid email address, password, face scan, and TOTP to test the password, TOTP, and face recognition authentication. Users should be able to access the BWW only if their username, password, TOTP, and face scan are valid. The expected results were achieved. The functionality testing of

S4 is illustrated in Figure 6.7.



Sign in to your wallet account

Email: biometric-auth@gmail.com

Password: •••••••••••••••

Additional Verification

Biometric Authentication

Face Recognition Result: Passed

Wallet Account Information

Email: biometric-auth@gmail.com

Account_Address: 0x4241012a170784d2c64dc570fbe2cad8a000e9aa

Public Key: 3b3927b647a09b88c646defc46fb360791b06dfd0e656bf27c3ccf1

Your balance: 100.0

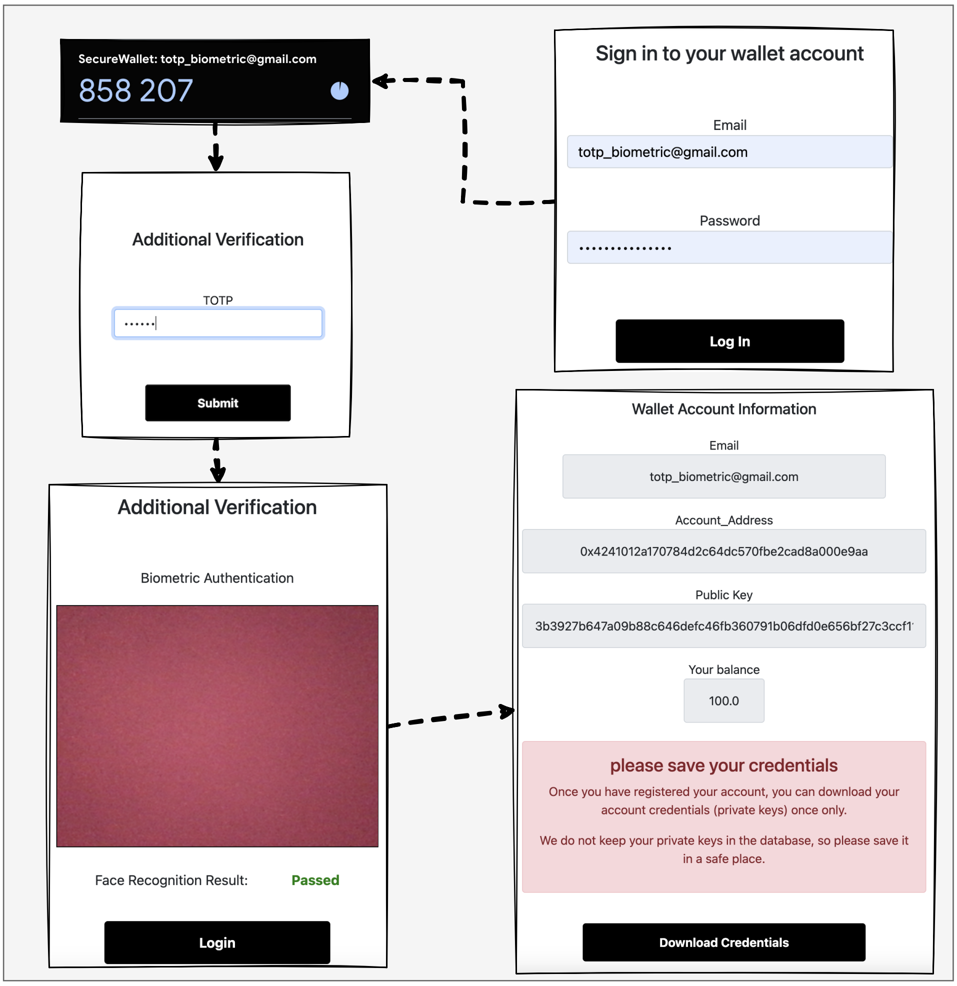
please save your credentials

Once you have registered your account, you can download your account credentials (private keys) once only.

We do not keep your private keys in the database, so please save it in a safe place.

Figure 6.6: A screenshot of the S3 setting

Throughout the testing process, we found that the BWW's performance remained reliable and efficient, despite the addition of multiple authentication factors. In addition, this finding demonstrates the robustness of the system's architecture and its capacity to handle increased complexity without compromising performance. Thus, multiple authentication settings significantly enhanced the system's security. With each additional factor, unauthorized users are increasingly powerless to perform account takeover attacks, thereby providing an extra layer of protection. However, adding multiple authentication factors escalated the complexity of the authentication process. This was expected, as each factor creates additional overheads for developers and BW users.



Sign in to your wallet account

Email

totp_biometric@gmail.com

Password

•••••••••••••••

SecureWallet: totp_biometric@gmail.com

858 207

Additional Verification

TOTP

••••••

Additional Verification

Biometric Authentication

Face Recognition Result: Passed

Wallet Account Information

Email

totp_biometric@gmail.com

Account_Address

0x4241012a170784d2c64dc570fbe2cad8a000e9aa

Public Key

3b3927b647a09b88c646defc46fb360791b06dfd0e656bf27c3ccf1

Your balance

100.0

please save your credentials

Once you have registered your account, you can download your account credentials (private keys) once only.

We do not keep your private keys in the database, so please save it in a safe place.

Figure 6.7: A screenshot of the S4 setting

6.4 Evaluation and Validation of the Proposed BWW:

This section evaluates the BWW's performance and its robustness against threats. This is achieved through risk analysis, developing a threat model, and conducting attack simulations tailored to each authentication setting scenario to measure their effectiveness using the level of security and attack success rate metrics.

6.4.1 Risk Analysis

Risk analysis identifies potential vulnerabilities and implements secure authentication measures that are effective for BW accounts. The assessment evaluates mechanisms designed to protect the private key and authentication credentials [115]. The BW's private key is the only way to prove ownership of the BW's valuable assets. Consequently, if these private keys are lost or stolen, the assets within the BW become vulnerable to exploitation by malicious actors. Thus, enhancing the access control mechanisms of BW solutions through risk analysis to protect private keys is crucial. Four authentication settings are introduced in the proposed system model of the BWW, each with potential risks. Risk analysis and management involves risk identification, assessment and mitigation. Following is an explanation of risk identification, assessment and mitigation for our proposed system model of the BWW:

- **Risk Identification:** One of the most concerning identified risks to BWs is account takeover attacks, which take advantage of human weaknesses to trick users into disclosing sensitive credentials [97]. A phishing attack, which is a type of social engineering attack, is one of the most prevalent techniques employed by attackers to gain access to BWs [116]. The risk of theft of private keys or unauthorized access also include threats such as malware attacks capturing keystrokes or making screenshots during the typing process. Some account takeover attacks exploit vulnerabilities in the authentication process or compromise a user's login credentials to gain access to a BW solution. A variety of techniques can be used to execute these attacks, such as social engineering, malware, and keyloggers.

- **Risk Assessment:** The likelihood of phishing attacks against BW solutions is high and consequential because of the rising value and wide adoption of cryptocurrencies, making them attractive targets for cyber criminals [117]. Furthermore, phishing techniques have developed significantly and have become sophisticated and challenging to identify, increasing the attack's success rate. Moreover, the impact of phishing attacks on BW solutions is significant and multifaceted for individuals and organizations. The most direct and immediate effect is the potential loss of funds associated with a BW solution. Successful attacks can undermine trust in BW solutions, deter entities from adopting blockchain technologies and hinder the development of the cryptocurrency market. Furthermore, the anonymity and irreversible nature of blockchain transactions make recovery from such attacks challenging.

- **Risk Mitigations:** The aforementioned threats resulted in introducing 2FA and MFA in the proposed BWW. These security mechanisms add layers of protection to significantly strengthen the BW's authentication process and prevent access by unauthorized parties. It provides this protection by requiring multiple factors, such as one-time passwords (OTPs) and biometrics, before granting access to the BW account [118]. These multiple factors significantly minimize the possibility that malicious actors can gain access to BW accounts, even if they manage to obtain the account holder's password. Therefore, MFA in BWs mitigates the risks of unauthorized access, strengthens authentication techniques, and protects individuals' digital assets.

6.4.2 Threat Model

The threat model evaluates the resilience of the developed solution and analyzes the security aspects of each MFA setting in terms of vulnerabilities and risks. It contributes to developing and improving secure and trusted BWs by understanding the strengths and weaknesses of MFA settings. Threat modeling is a systematic process for identifying, assessing, and addressing the security risks associated with applications or systems [119]. This study discusses unauthorized access to BW credentials and private keys as a significant threat to legitimate users. Thus, it requires an understanding of the actors involved and the potential attack vectors. In this scenario, the user represents an authorized party who has a blockchain account and stores private keys on the device locally. In contrast, the attacker represents a malicious party who intends to gain unauthorized access to the user's BW, as shown in Figure 6.8. The attacker can access the user's BW through the following potential attack:

- The attacker might conduct a social engineering attack using phishing techniques to manipulate users and take over their accounts. Thus, the attacker might mislead the user into providing login credentials and private keys to a fraudulent website that mimics a legitimate service. As a first step, an attacker crafts an email with a malicious link that appears to be from a legitimate BW provider. After the email is sent, the malicious link redirects the user to a fraudulent website that looks identical to the BW provider's login page. However, when users enter their login credentials, the attacker harvests them and gains access to the user's BW account.

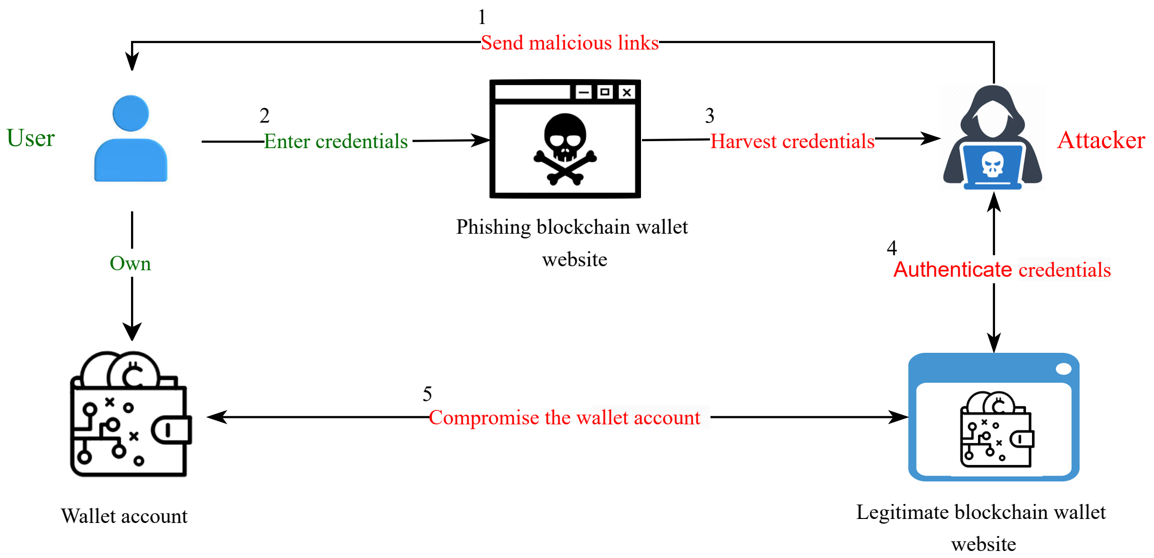


Figure 6.8: The threat model

6.4.3 Attack Simulation

For attack simulations, we used a Kali 2022.2 (64-bit) virtual machine with 22 GB of RAM and 17 GB of storage. Also, we used an Ubuntu 22.04.2 LTS (64-bit) virtual machine with 25 GB of RAM and 30 GB of storage as a website server. Virtual machines were configured to use a NAT network that allowed them to communicate with each other and access the internet while being isolated from the external network. After preparing the environment, we used SET in Kali to assist in the creation and management of phishing campaigns and to trick users into providing sensitive information, such as login credentials. The tool captures the user's credentials, which can be utilized to compromise the BW account. Then, we exploited several vulnerabilities, such as weak encryption, insecure communication, and server misconfigurations, using the Metasploit Framework to bypass MFA authentication. We performed the attack scenario ten times against each authentication setting S1, S2, S3 and S4. Tests were conducted based on the availability of time and resources. Ten tests per setting provide a practical balance between comprehensiveness and feasibility that can be effective in identifying patterns without being excessive.

To measure the effectiveness of each authentication setting, we used the success attack rate metric (see Equation 6.1) to quantitatively capture the setting's ability to withstand security attacks. An attack success rate (ASR) can be defined as the percentage of attempts that succeed in gaining access to the BW account. A high success rate indicates vulnerabilities in a particular authentication setting and is likely to increase the risk of BW account takeover.

$$ASR = \frac{S}{S+F} \times 100 \tag{6.1}$$

where:

- S is the number of successful attack attempts.
- F is the number of failed attack attempts.

In addition, to measure the reliability of each authentication setting, we calculated the security level for each setting using Equation 6.2. This level of security (LS) refers to the degree to which a specific authentication setting protects against BW account takeover.

$$LS = \left(1 - \frac{S}{S+F}\right) \times 100 \tag{6.2}$$

where:

- S is the number of successful attack attempts.
- F is the number of failed attack attempts.

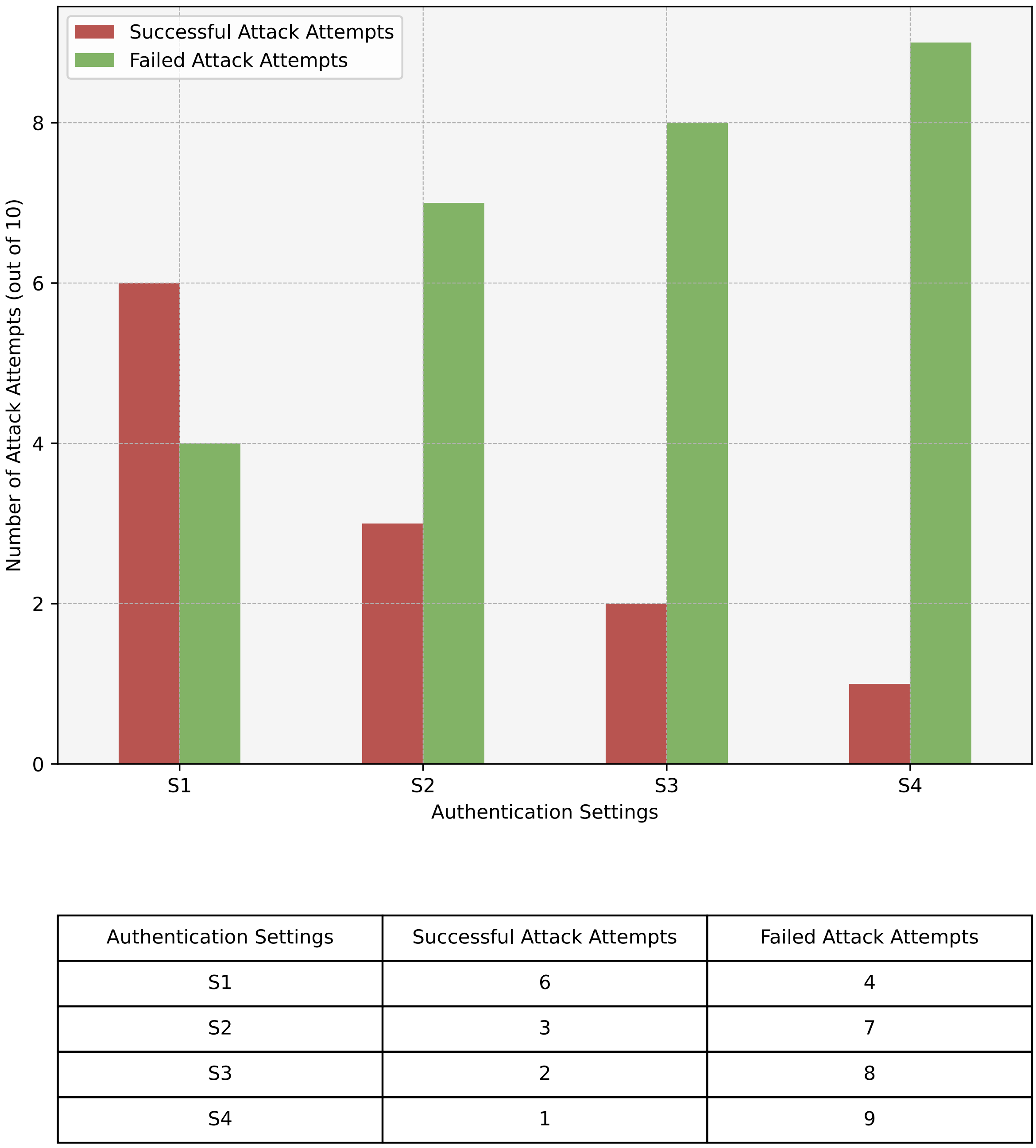
6.5 Results and Discussion

Based on LS and ASR equations, we made reliable judgments and assessments about which setting performed better to prevent the maximum number of attempted attacks. Figure 6.9 illustrates the successful and failed attack attempts using the authentication settings. Also, Figure 6.10 shows the results we obtained in terms of LS and ASR of each authentication setting as a percentage. Based on the evaluation of each authentication setting, it can be seen that S1 is highly vulnerable to phishing attacks, with an ASR of 60% and an LS of 40%. Despite its convenience and wide adoption, this setting is considered to be the least secure of all alternatives. As a result of adding a second authentication factor TOTP, S2 increases the LS to 30% and decreases the likelihood of the ASR in phishing attacks to 30%, which is a significant improvement in security over S1. Even though the system's security has been enhanced, the user is required to manage another authentication factor, which increases the complexity of the login process. In addition, S3 integrates face recognition technology providing a different authentication factor that relies on unique biometric data, making it more challenging for attackers to impersonate the user. Compared with S1 and S2, S3 has an increase in LS to 80% and a decrease in the ASR to 20%, reflecting the difficulty attackers face when replicating unique biometric data, making it more secure than using S1 or S2. Finally, S4, which combines all authentication settings, has the lowest ASR of 10% and hence the highest LS of 90%, providing the most robust defence against unauthorized access attempts using phishing techniques of all the settings.

6.5.1 Implementation challenges and costs for developers

6.5.1.1 Coding

A number of factors contributed to the choice of Python as a programming language, including its ease of use, rapid prototyping and intuitive nature. It resulted in faster development and debugging, and we were able to spend less time in understanding the code. However, the choice of the programming language that the developers will use is a crucial decision. BWs can be coded in a variety of programming languages, including Solidity, Rust, Go, Java, Python, C++ and JavaScript. Thus, the choice of the programming language will be determined by several factors, including the BW's specific requirements, the blockchain platform it will interact with, and the expertise of the development team. For instance, BW developers should consider Solidity if they are developing advanced smart contract codes that will run on the Ethereum Virtual Machine (EVM). On the other hand, if they intend to interact with cross-platform applications, JavaScript, Java and Python should be applied since they have Web3.py,



Authentication Settings	Successful Attack Attempts	Failed Attack Attempts
S1	6	4
S2	3	7
S3	2	8
S4	1	9

Figure 6.9: Successful and failed attack attempts by authentication settings

Python-bitcoinlib, Web3.js, BitcoinJS, Web3j, and BitcoinJ libraries for interacting with various blockchain platforms. Hence, developing a BW involves complex processes that require a deep understanding of cryptography, security, and blockchain technology. This procedure is heavily influenced by the programming language chosen since it affects BW efficiency, security, and scalability. Furthermore, it is difficult to find and train experts in the blockchain industry due to a shortage of experienced developers. Blockchain is a relatively emerging and complex

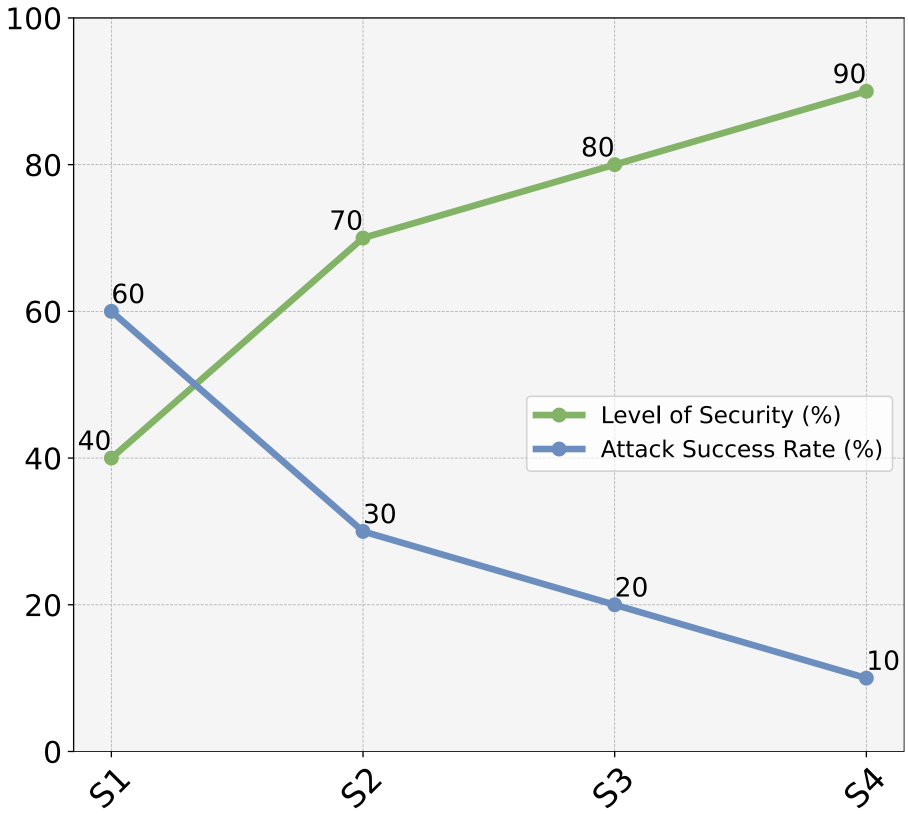


Figure 6.10: LS and ASR of the authentication settings

domain, and so businesses often need to invest heavily in training and development to remain competitive.

6.5.1.2 Developing authentication settings

Several implementations, tools and services are available for TOTP, including Google Authenticator, Authy, and Yubico Authenticator. Thus, implementing TOTP requires integration with a TOTP service or building a customized system. These third-party services can incur significant development and operational costs. Moreover, it is crucial to have accurate facial recognition systems to prevent unauthorized access and prevent legitimate users from being locked out of their BWs. The accuracy of facial recognition systems is primarily determined by the algorithm used. For example, deep learning algorithms provide higher accuracy but require more computational resources. Some tools offer features to prevent spoofing attacks, such as liveness detection, which can also affect accuracy. Thus, it can be challenging for developers and businesses to achieve an optimal level of accuracy because advanced AI algorithms may require qualified expertise in AI, blockchain technology, and security, and this may result in a higher cost associated with the development process, the integration of facial recognition services, and ongoing maintenance.

6.6 Chapter Summary

- This chapter introduced a secure BWW, which provides four authentication settings to develop an efficient platform for managing cryptographic keys and digital assets. A system model for the BWW was developed to describe the complex interactions between the system and its components. Furthermore, an overview of the experiment setup, testing and evaluation was presented. Simulated phishing attacks against each setting were performed to determine attack success rates and security levels. The findings indicate that system models play a crucial role in enhancing MFA implementation in the BWW by facilitating an understanding of the system's architecture. Also, the results provide valuable information regarding the relationship between the complexity of MFA settings and their corresponding level of security.

- The next chapter (Chapter 7) describes the implementation of a general and customized ranking system (TBW-RAnk) for BW solutions using AI.

CHAPTER

7

Developing a Trust-based Ranking Model for Blockchain Wallets Using AI Models (TBW-RAnk)

7.1 Chapter Overview

Chapter 6 focused on the development of hard security measures for BW solutions. A methodical strategy was utilized to simplify the incorporation of four different authentication settings into the BWW. The outcome of evaluating and quantifying the security level provided by each authentication setting is a crucial component of credibility within the trust-based ranking system (TBW-RAnk:). This chapter defines the criteria for trust-based ranking, detailing the factors considered vital for assessing the trustworthiness of BW solutions. In addition, it explores the development of a trust-based ranking system by building, training, and evaluating three AI models. Then, we select the most effective deployment model based on comprehensive accuracy metrics. The following are the environments and libraries used in the implementation, validation, and evaluation:

- **Python [1]:** Python is a high-level, interpreted programming language known for its simplicity, flexibility and readability. It supports a variety of programming paradigms, including procedural, object-oriented, and functional programming. Also, it is a prominent language for web development, data analysis, artificial intelligence and other applications [104].
- **Scikit-learn [2]:** Scikit-learn is an open-source machine-learning library in Python. It is widely used for machine learning tasks such as classification, regression, clustering and

[1] https://www.python.org

[2] https://scikit-learn.org

dimensionality reduction. It provides a consistent and flexible interface for implementing standard machine learning algorithms. Also, its simplicity and accessibility have made it a popular framework for developers and researchers in machine learning and data science [120].

- **Keras [3]:** Keras is an open-source neural network library in Python. It efficiently builds many models, from simple feedforward neural networks to complex deep-learning models. It supports the developers in creating deep learning models, such as layers, objectives, and activation functions. Also, it offers a functional API, which allows models to be built with more flexibility, such as multi-output models and models with shared layers. It is popular among researchers and industry professionals because of its simplicity, allowing for fast prototyping [121].

The structure of this chapter is as follows: Section 7.2 proposes the methodology for determining the trustworthiness score of a BW solution. This foundational approach develops a comprehensive BW security and trustworthiness evaluation. Section 7.3 provides the implementation of the proposed TBW-RAnk through its development to the rigorous assessment of the three advanced AI models. Section 7.4 discusses the outcomes using cross-validation techniques to compare the effectiveness and accuracy of the models in predicting the BW solution's trustworthiness. Section 7.5 concludes the chapter.

[3] https://keras.io

7.2 The Proposed Trustworthiness and Ranking Measurement Methods

This section defines the trustworthiness score of BW solutions to build the TBW-RAnk which ranks BW solutions in a general and personalized mode. The proposed TBW-RAnk can assess and calculate the trustworthiness value of BW solutions based on their features. The primary goals of establishing this trustworthiness value are as follows:

- to measure the direct trustworthiness value of the BW solution, enabling BW users to make informed decisions about ongoing and future interactions with a BW solution.

- to share the assigned direct trustworthiness value as a recommendation, helping a newcomer to the blockchain community who has not used a BW solution in the specific context and timeframe. This recommendation empowers BW users to make trust-based decisions when considering an interaction with a specific BW solution.

7.2.1 Defining the trustworthiness of BW solutions

Trustworthiness refers to the quality or features of being dependable, reliable, and trustworthy. It encompasses the features and behaviors that make entities, organizations, or systems credible and honest. Building and maintaining trust in interactions is fundamentally dependent on the quality of trustworthiness, whether personal, professional, or technological [122], [123]. In BW solutions, trustworthiness is not merely a single attribute but a dynamic combination of qualities that enhance security and inspire trust. A key aspect of trustworthiness in BW solutions is the multifaceted aspects of trustworthiness due to the unique characteristics of blockchain technology [28].

To determine the trustworthiness value of BW solutions, this research follows the methodologies explained in Chang, Hussain, and Dillon [124]. The proposed TBW-RAnk uses CCCI metrics to determine the overall trustworthiness score of each BW solution. The trustworthiness score or value helps produce a trustworthy ranking system that ranks BW solutions globally. A set of criteria is developed to assess the trustworthiness of BW solutions, aiming to quantify their quality. The primary metric for evaluating wallet trustworthiness involves identifying the features the trusted entity (wallet providers) delivers to the trusting entity (BW users). The level of trustworthiness in BW solutions is positively correlated with the presence of more advanced features. Figure 7.1 provides an overview of the BW solution trustworthiness measurement methodology in four steps.

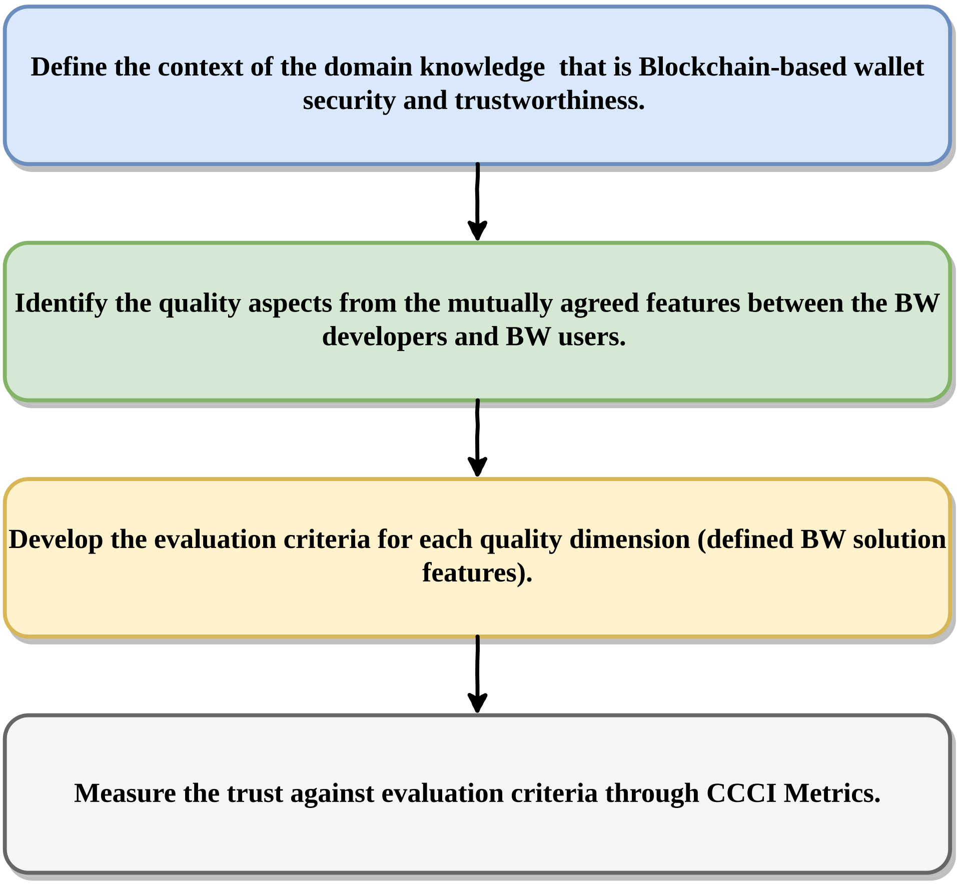

Define the context of the domain knowledge that is Blockchain-based wallet security and trustworthiness.
Identify the quality aspects from the mutually agreed features between the BW developers and BW users.
Develop the evaluation criteria for each quality dimension (defined BW solution features).
Measure the trust against evaluation criteria through CCCI Metrics.

Figure 7.1: Steps for determining the trustworthiness of BW solutions.

1. *Step One: Defining the context domain*

   A context identifies a particular domain by assigning a domain name and provides a distinct function(s) for a given context. The ’context’ can be further broken down into ’criteria’ that can be arranged in a hierarchy. Context is an entity or agent function, a business function, or a product function. The context has three parts: name, type, and function description. The context name is the service, the type of context is the service type, and the context specification is a descriptive detail of the service. Table 7.1 presents the proposed model context domain.

2. *Step Two: Identifying the quality aspects*

   The quality aspect is the quality component of a context for quality assessment. The quality dimension identifies the quality of the context and clarifies whether the specified criteria are provided. The mutually agreed functionalities capture quality aspects that

Context Parts	Our context domain
Name	Blockchain-based wallets or Cryptocurrencies wallets
Type	Storage
Function description	Store and secure the wallet private keys

Table 7.1: Defining the context domain

BW developers have delivered to BW users. It explains the trusting agent's (BW users) expectations of the trusted agent (BW developers).

3. *Step Three: Developing the quality assessment criteria*

   Quality evaluation criteria describe the quality metric for each quality feature to determine quality. The quality metric is characterized as a set of requirements or laws by which each quality dimension produced is correlated, compared, quantified, and ranked. They set quality standards and guidelines for trusted agents (BW developers) to follow when developing and delivering BW solutions. This research considers the original criteria or delegation of the BW developers and the actual provided functionalities.

4. *Step Four: Measuring the trustworthiness with CCCI metrics*

   The assessment criteria (trust criteria for BW solutions) determine whether the wallet is reliable or unreliable and measure each wallet's trustworthiness value. CCCI metrics are applied to determine the trust value and develop the TBW-RAnk for BW solutions. In addition, different levels of trustworthiness semantics are proposed to model the numerical values for the trustworthiness level of BW solutions in the domain [0-4]. The values from 0 to 4 are the ordinal scale. The semantics are illustrated in Table 7.2.

Ranking Levels	Semantics
0	Trustworthiness level cannot be determined
1	Significantly bad trustworthiness level
2	Bad trustworthiness level
3	Good trustworthiness level
4	Significantly good trustworthiness level

Table 7.2: The five ranking levels and their semantics description.

The CCCI metrics are as follows:

a) **Correlation of an Interaction (CorrInteraction):** BW developers should identify the features of BW solutions to calculate a trust score and determine its actual functionality.

b) **Correlation of a Criterion (CorrCriteria):** The assessment criteria are as follows:

- Support TOTP
- Support facial recognition
- Number of cryptocurrencies
- Wallet age
- Cryptocurrencies control (custodial vs non-custodial)
- Users' feedback (rating)
- Security level

c) **Clarity of the Criterion (ClearCriteria):** The BW developers should clearly state the above criteria or features.

d) **Importance of the Criterion (ImpCriteria):** The importance of BW features is divided into categorical and value encoding methods. The features in a categorical encoding method are equally important, using binary values (1 or 0) to represent the presence or absence of features. The importance of features in the value encoding method varies, as different numerical values are assigned to features based on their significance. Table 7.3 shows the importance of each BW feature.

BW Features (Criteria)	Encoding Methods	Feature Importance
Support TOTP	binary values	[0,1]
Support Facial Recognition	binary values	[0,1]
Multiple Cryptocurrencies	binary values	[0,1]
Wallet Age	numerical values	Range [0-15]
Custodial	binary values	[0,1]
Non-custodial	binary values	[0,1]
Rating	numerical values	Range [0-5]
Security Level	numerical values	[0.4,0.7,0.8,0.9]

Table 7.3: The importance of each feature of the BW solution

7.2.2 Develop trustworthiness score and ranking systems

After identifying the importance associated with each BW solution feature, the trustworthiness score and the ranking equations are developed to rank BW solutions based on their trustworthiness scores.

7.2.2.1 Develop a scoring system

For general ranking, each feature has the same weight of 0.1. In contrast, the feature selected by BW users is more significant for customized ranking than other features. For example, if the user selects the security level to rank the wallet, the security level feature weight is 0.25, and the other feature weight is 0.11. After this, a scoring system is developed to quantify and evaluate the trustworthiness and quality of the BW solution. **The weighted aggregate mathematical function**, as shown in Equation 7.1, determines the overall trustworthiness score ($Trust_{(Score)}$) of a BW solution .

- **Trustworthiness Score Calculation:** Given a set of features F where $F = \{f_1, f_2, \ldots, f_n\}$, and a corresponding set of weights W where $W = \{w_1, w_2, \ldots, w_n\}$, the score $Trust_{(Score)}$ is defined as:

$$Trust_{(Score)} = \sum_{i=1}^{n} w_i \times f_i = w_1 \times f_1 + w_2 \times f_2 + \cdots + w_n \times f_n \tag{7.1}$$

  In the formula above, each feature f_i from set F has an associated weight w_i from set W. Each feature value is shown in Table 7.3. The score $Trust_{(Score)}$ is the weighted sum of the product of each feature's value and its corresponding weight

  where:

  - n is the number of features to be aggregated.
  - w_i is the weight for the i^{th} feature.
  - f_i is the value of the i^{th} feature.

7.2.2.2 Rank BW solutions

The BW solution ranking is interpreted based on the calculated ($Trust_{(Score)}$) from Equation 7.1. Five ranges are established based on specific ($Trust_{(Score)}$) threshold values, as shown in Equation 7.2.

- **Ranking Calculation:** Let the ranking function $Rank_{(Trust_{(Score)})}$ be defined as:

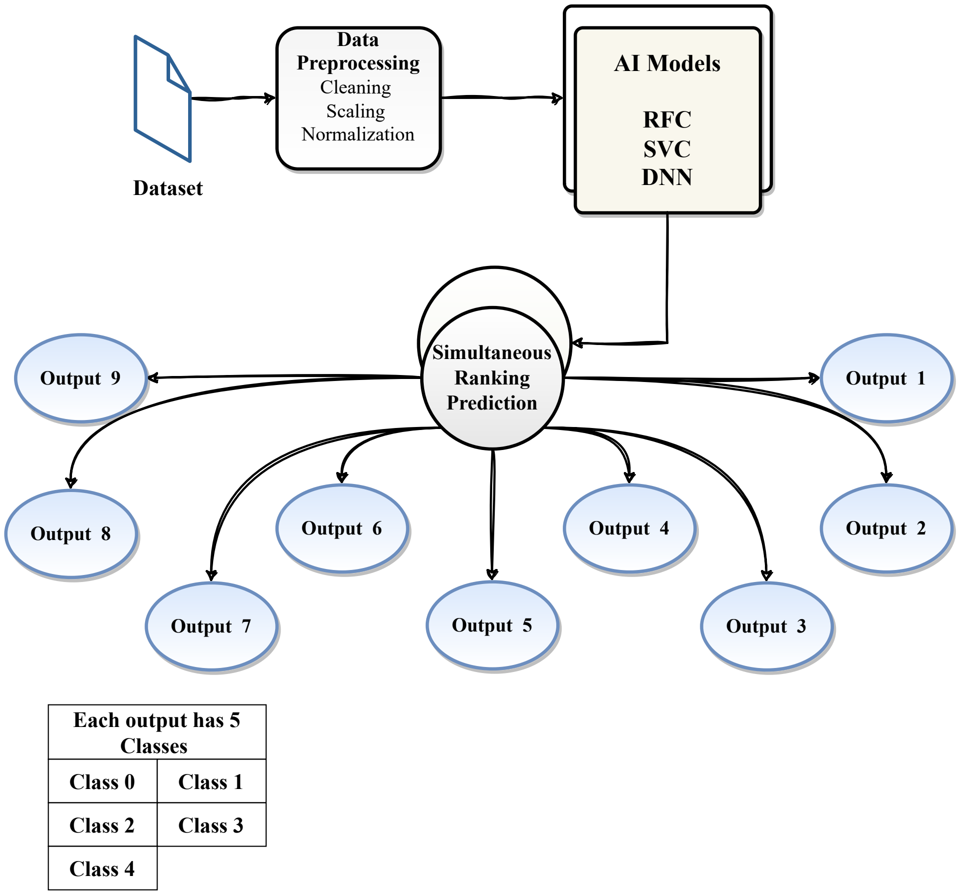
$$Rank_{(Trust_{(Score)})} = \begin{cases} 0 & \text{if } 0 \leq Trust_{(Score)} < 0.2, \\ 1 & \text{if } 0.2 \leq Trust_{(Score)} < 0.4, \\ 2 & \text{if } 0.4 \leq Trust_{(Score)} < 0.6, \\ 3 & \text{if } 0.6 \leq Trust_{(Score)} < 0.8, \\ 4 & \text{if } 0.8 \leq Trust_{(Score)} \leq 1. \end{cases} \tag{7.2}$$

where:

  - $Rank_{(Trust_{(Score)})}$ represents the ranking derived from the $Trust_{(Score)}$ value, with $Trust_{(Score)}$ being a real number in the interval [0, 1].
  - The conditions in the piecewise function specify the threshold for $Trust_{(Score)}$ and the associated ranking $Rank$.

7.3 Experiment Setup, Implementation, Evaluation and Validation of the TBW-RAnk using AI models

This section provides a detailed description of the implementation of the proposed TBW-RAnk. It includes developing and evaluating three AI models and facilitating the selection of the optimal deployment model. It offers robust AI model architecture designed for multi-output learning, enabling the simultaneous processing and prediction of multiple outputs. Through carefully crafted design and optimization, this architecture demonstrates the capability to handle diverse sets of outputs efficiently and effectively. Figure 7.2 illustrates the experiment setup and the implementation of the three AI models. Algorithm 3 details the implementation steps of the TBW-RAnk. Appendix A.4 contains the code link for the AI models.



Each output has 5 Classes	
Class 0	Class 1
Class 2	Class 3
Class 4	

Figure 7.2: The experiment framework for building the AI models for TBW-RAnk

Algorithm 3 The implementation steps of the TBW-RAnk

```
Require: Set of blockchain wallets $BWs$
Ensure: A trustworthiness score and ranking for each $BW$
  Define trustworthiness criteria:
      Measuring the trustworthiness with *CCCI Metrics*. Let $F$ denote the set of features
      associated with BWs, where each feature represents a characteristic of the BW contributing
      to its trustworthiness.
      $Trustworthiness_{(Criteria)} \leftarrow F = \{\mathrm{f}_1, \mathrm{f}_2, \ldots, \mathrm{f}_8\}$
  Assign a weight to criteria:
      Let $W$ be the set of weights for each metric in $F$.
      In general mode, $W = \{w | w = 0.1 \, \forall \, w \in F\}$.
      In customized mode, select one $f \in F$ for a weight of 0.25, and assign 0.11 to the rest.
  Develop a scoring system:
      Let $n$ be the number of BW features in set $F$.
  for $i = 1$ to $n$ do
      $Trust_{(Score)} \leftarrow w_i \times f_i$            ▷ The weighted aggregate mathematical function
  end for
  Rank the BW solutions:
      Rank wallets based on $Trust_{(Score)}$                ▷ The ranking threshold values
  if $0 \leq Trust_{(Score)} < 0.2$ then $Rank_{(Trust_{(Score)})} \leftarrow 0$
  else if $0.2 \leq Trust_{(Score)} < 0.4$ then $Rank_{(Trust_{(Score)})} \leftarrow 1$
  else if $0.4 \leq Trust_{(Score)} < 0.6$ then $Rank_{(Trust_{(Score)})} \leftarrow 2$
  else if $0.6 \leq Trust_{(Score)} < 0.8$ then $Rank_{(Trust_{(Score)})} \leftarrow 3$
  else if $0.8 \leq Trust_{(Score)} \leq 1$ then $Rank_{(Trust_{(Score)})} \leftarrow 4$
  end if
  Data Generation:
      A synthetic dataset is generated using the *rule-based generation technique*.
  Model building and training:
      Build AI models using *RFC*, *SVC*, and *DNN*.
  Model evaluation and testing:
      Measure the AI model's performance using $accuracy, precision, recall, andF1score$.
  return Trustworthiness scores and rankings for each $BW$,with *9 outputs*, each output
  classified into *5 classes*
```

7.3.1 Data collection and preparation

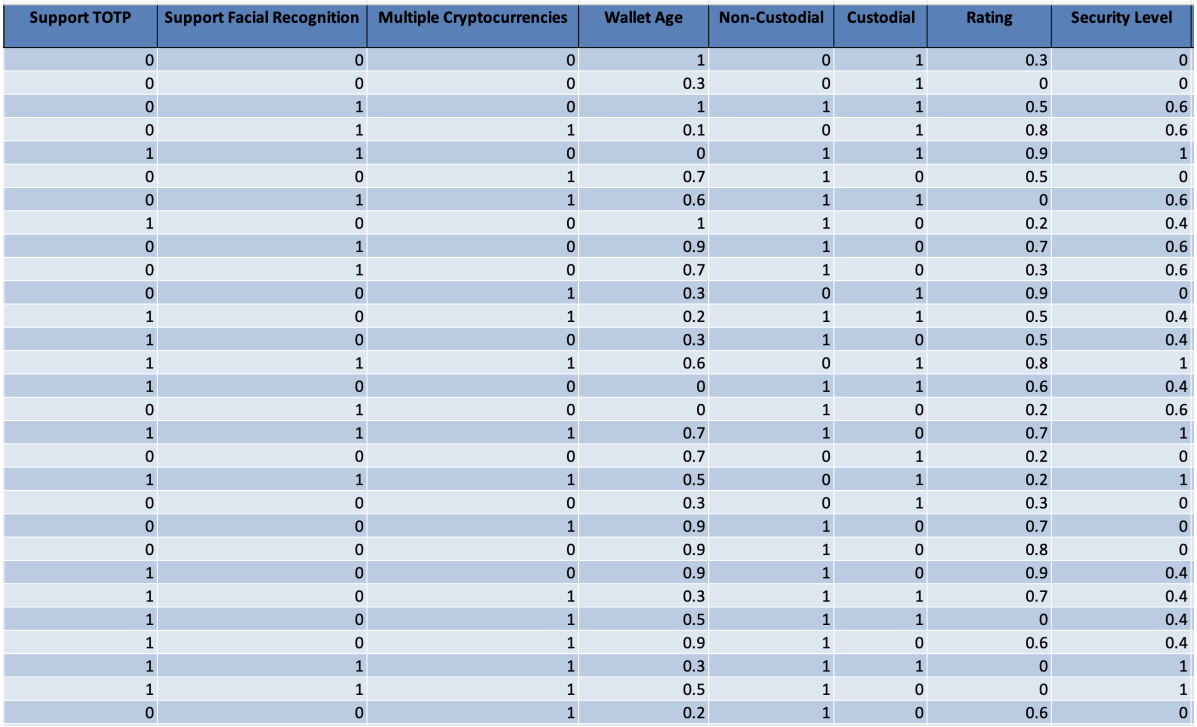
This section outlines the data collection process for the BW solutions. Given the nature of the model's multi-output problems, a substantial volume of data is crucial. Therefore, a synthetic dataset is generated to ensure adequate data for training and analysis purposes.

7.3.1.1 The Generation of Synthetic dataset

Synthetic datasets were created based on specific requirements. The rule-based generation technique is used to generate synthetic data by establishing a set of rules and logic that simulate the relationships and structures of real-world datasets [98]. The dataset comprises 10,000 BW solution records with various features representing diverse scenarios and conditions. The rules use deterministic and probabilistic models to generate datasets that mimic the diversity and complexity of real-world BW solutions. BW features, such as support for TOTP, facial recognition, and multiple cryptocurrencies, are determined by random choice with equal probability. This simulates a realistic distribution of features across different BW solutions. The logic was used to ensure a BW cannot be both non-custodial and custodial simultaneously to maintain data integrity and reflect realistic scenarios. The BW solution's ratings are created using a triangular distribution, which is more practical than a basic uniform or normal distribution because it models the tendency of ratings to cluster around a mode while allowing for diversity. The wallet age feature ranges from 0 to 15 years because blockchain was invented in 2009 [1]. The wallet age feature adds a layer of realism to the synthetic dataset. The synthetic data was created using Python with NumPy and Faker libraries; the code link is presented in Appendix A.4. The dataset is structured as follows:

- Total records: 10,000 blockchain wallet solutions.
- Total columns: 27 columns in total.
- Feature columns: The eight columns detail the different features of each blockchain wallet application (see Figure 7.3).
- Targeted columns: Nine dataset columns are selected as target variables, which were the primary focus of our predictive models (see Figure 7.4).
- Deleted columns: 10 columns were considered unnecessary for our modeling purposes and were therefore omitted.

A description of each column in the data set are as follows:



Support TOTP	Support Facial Recognition	Multiple Cryptocurrencies	Wallet Age	Non-Custodial	Custodial	Rating	Security Level
0	0	0	1	0	1	0.3	0
0	0	0	0.3	0	1	0	0
0	1	0	1	1	1	0.5	0.6
0	1	1	0.1	0	1	0.8	0.6
1	1	0	0	1	1	0.9	1
0	0	1	0.7	1	0	0.5	0
0	1	1	0.6	1	1	0	0.6
1	0	0	1	1	0	0.2	0.4
0	1	0	0.9	1	0	0.7	0.6
0	1	0	0.7	1	0	0.3	0.6
0	0	1	0.3	0	1	0.9	0
1	0	1	0.2	1	1	0.5	0.4
1	0	0	0.3	1	0	0.5	0.4
1	1	1	0.6	0	1	0.8	1
1	0	0	0	1	1	0.6	0.4
0	1	0	0	1	0	0.2	0.6
1	1	1	0.7	1	0	0.7	1
0	0	0	0.7	0	1	0.2	0
1	1	1	0.5	0	1	0.2	1
0	0	0	0.3	0	1	0.3	0
0	0	1	0.9	1	0	0.7	0
0	0	0	0.9	1	0	0.8	0
1	0	0	0.9	1	0	0.9	0.4
1	0	1	0.3	1	1	0.7	0.4
1	0	1	0.5	1	1	0	0.4
1	0	1	0.9	1	0	0.6	0.4
1	1	1	0.3	1	1	0	1
1	1	1	0.5	1	0	0	1
0	0	1	0.2	1	0	0.6	0

Figure 7.3: The feature columns in the dataset

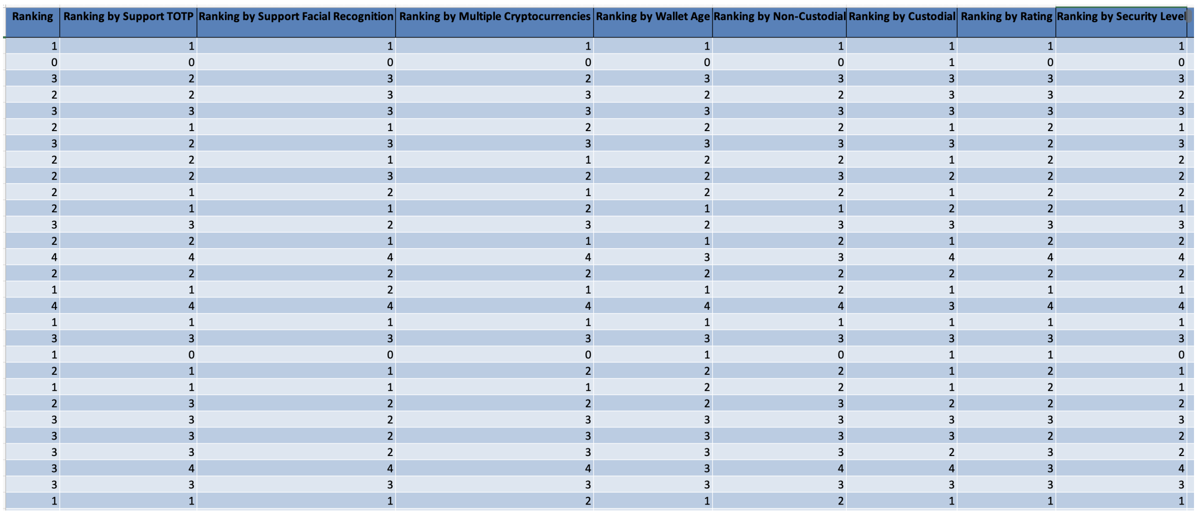
a) **Feature Columns:**

1) **Support TOTP:** This criterion determines whether the wallet has TOTP or not. If it has TOTP, it receives a value of 1; otherwise, it receives a value of 0.

2) **Support facial recognition:** This criterion determines whether the wallet has a facial recognition feature or not. If it has, it receives a value of 1; otherwise, it receives a value of 0.

3) **Number of cryptocurrencies:** This criterion determines the number of cryptocurrencies that blockchain wallets support. Wallets that support multiple cryptocurrencies increase user trust and provide more flexibility. The more cryptocurrencies that are supported by a blockchain wallet, the higher the user's trust in the wallet, as they can ensure that their digital assets are secure since the wallet is recognized by a variety of blockchain networks [125].

4) **Wallet age:** This criterion considers the age or longevity of the wallet. Values are assigned based on the perceived reliability and trustworthiness associated with BW solutions that have been in operation for a longer time. It enables a broad definition of



Ranking	Ranking by Support TOTP	Ranking by Support Facial Recognition	Ranking by Multiple Cryptocurrencies	Ranking by Wallet Age	Ranking by Non-Custodial	Ranking by Custodial	Ranking by Rating	Ranking by Security Level
1	1	1	1	1	1	1	1	1
0	0	0	0	0	0	1	0	0
3	2	3	2	3	3	3	3	3
2	2	3	3	2	2	3	3	2
3	3	3	3	3	3	3	3	3
2	1	1	2	2	2	1	2	1
3	2	3	3	3	3	3	2	3
2	2	1	1	2	2	1	2	2
2	2	3	2	2	3	2	2	2
2	1	2	1	2	2	1	2	2
2	1	1	2	1	1	2	2	1
3	3	2	3	2	3	3	3	3
2	2	1	1	1	2	1	2	2
4	4	4	4	3	3	4	4	4
2	2	2	2	2	2	2	2	2
1	1	2	1	1	2	1	1	1
4	4	4	4	4	4	3	4	4
1	1	1	1	1	1	1	1	1
3	3	3	3	3	3	3	3	3
1	0	0	0	1	0	1	1	0
2	1	1	2	2	2	1	2	1
1	1	1	1	2	2	1	2	1
2	3	2	2	2	3	2	2	2
3	3	2	3	3	3	3	3	3
3	3	2	3	3	3	3	2	2
3	3	2	3	3	3	2	3	2
3	4	4	4	3	4	4	3	4
3	3	3	3	3	3	3	3	3
1	1	1	2	1	2	1	1	1

Figure 7.4: The targeted columns in the dataset

BW solutions, from newly established to long-standing ones. Newer BW solutions can still receive high scores if they demonstrate strong features and positive user feedback.

5) **Cryptocurrency control (custodial vs non-custodial):** This criterion distinguishes between custodial and non-custodial wallets. Custodial wallets hold users' private keys and manage their funds, while non-custodial wallets give users full control over their private keys and funds. There is a correlation between non-custodial and custodial columns. BW solutions can be non-custodial and custodial, only non-custodial or only custodial.

6) **Users' feedback (Rating) (0-5):** This criterion involves gathering BW user feedback and reviews about each wallet. Values are assigned based on the average or aggregate user rating. This allows the real-world experiences of BW users to be considered when evaluating the wallets.

7) **Security Level:** (none, TOTP only, face recognition only, TOTP + face recognition): This criterion assesses the security features offered by BW solutions. Different levels of security values are assigned to each authentication technique based on the results in Section 6.5. When MFA is provided as TOTP, the value is 0.7, however when MFA is provided as face recognition, the value is 0.8. In addition, when both MFA authentication techniques are supported, the value is 0.9. When no MFA authentication techniques are supported, the value is 0.4.

b) **Targeted Columns:** Nine dataset columns, the primary focus of our predictive models, have been selected as target variables. Equations 7.1 and 7.2 are applied to rank BW solutions in these columns.

7.3.1.2 Data preprocessing

Data preprocessing involves transforming the raw dataset to prepare it for model training.

- **Data cleaning:** The feature columns include support TOTP, support facial recognition, multiple cryptocurrencies, wallet age, non-custodial, custodial, rating and security level. For normalization, the five categorical columns containing binary choices (YES/NO), namely support TOTP, support facial recognition, multiple cryptocurrencies, non-custodial and custodial, are converted to numerical values (1/0) suitable for AI modeling. Each value for the columns wallet age, security level and rating is normalized between 0 and 1 utilizing the min-max normalization technique. Scaling the numerical features ensures they are on the same scale, which is especially useful for AI algorithms sensitive to varying scales (see Equation 7.3). In addition, the dataset was examined to look for anomalies or outliers that may indicate errors in data generation, such as removing erroneous data points to prevent them from corrupting the models.

$$X_{\text{norm}} = \frac{X - X_{\text{min}}}{X_{\text{max}} - X_{\text{min}}} \tag{7.3}$$

  where X_{norm} is the normalized value of feature X, X_{min} is the minimum value of feature X, and X_{max} is the maximum value of feature X.

- **Feature engineering:** The security level column is generated depending on the support TOTP and support facial recognition columns. Different security level values are assigned for different scenarios. If no TOTP or facial recognition is supported, the value is 0.4, whereas if both are supported, the value is 0.9. If only TOTP is provided, the value is 0.7, whereas if only face recognition is provided, the value is 0.8. In addition, there is a correlation between the non-custodial and custodial columns. The BW solutions can be non-custodial and custodial, only non-custodial or only custodial. For the wallet age column, the wallet age ranges from 0 to 15 years. The multiple cryptocurrencies column has a value of 1 if the BW solution supports more than one cryptocurrency. Otherwise, it has a value of 0. The user rating column ranges from 0, which indicates that the BW solution has significant problems, to 5, which suggests that BW solutions are outstanding from every perspective and are highly recommended.

- **Data labeling:** The AI models are constructed to predict multiple outputs simultaneously. For a supervised learning purpose, nine target columns are selected and labeled. Each labeled column has five classes, as described in Table 7.2. The labeled columns for general and customized rankings are detailed in Table 7.4.

Outputs	labeled columns	Ranking Modes
Output 1	Ranking	General Ranking
Output 2	Ranking by Support TOTP	Customized Ranking
Output 3	Ranking by Support Facial Recognition	
Output 4	Ranking by Multiple Cryptocurrencies	
Output 5	Ranking by Wallet Age	
Output 6	Ranking by Non-Custodial	
Output 7	Ranking by Custodial	
Output 8	Ranking by Rating	
Output 9	Ranking by Security Level	

Table 7.4: The labeled columns for each output

7.3.2 Select AI models

Blockchain wallet solutions can be ranked on various criteria. These AI models rank them based on nine features, each having five classification labels. Due to the inherent complexity of the problem, a strategic approach to model selection is essential. As part of this task, it is necessary to predict multiple target variables simultaneously. This situation is commonly referred to as a multi-output or multi-target prediction problem. An analysis of the characteristics and requirements of the issue led to the selection of RFC, SVC and DNN models as the most appropriate solution. With multi-output problems involving complicated relationships between input features and multiple outputs, RFC, SVC and DNN excel at capturing sophisticated non-linear relationships. Regularization parameters provide a mechanism for controlling overfitting in these models, enabling fine-tuning bias and variance to optimize the performance of unseen data. In addition, RFC model architecture is flexible because of its ensemble nature, in which numerous decision trees collaborate to increase overall prediction accuracy while minimizing the risk of overfitting. Also, by maximizing the margin between classes, SVC can achieve a global optimization goal, resulting in effective class separation and better performance. The architecture of DNN can be customized to meet the needs of multi-output problems due to their flexibility. For instance, multiple output-specific layers can be created after a series of shared layers, allowing for specialized learning for each output. As a result, the model can handle each output's unique nuances and requirements. DNN can be expanded by adding additional neurons or layers as the number of targets (outputs) increases. This ensures that the network can model the increasing complexity as the number of outputs grows.

7.3.3 Developing the Proposed Solution Utilizing The Random Forest Classifier Model (RFC:)

The Random Forest classifier is a popular ensemble learning algorithm for classification and regression problems. During training, it constructs an array of decision trees and outputs the mean prediction for regression problems as individual trees or the mode of the classes as classification problems. RFC operates on the principles of decision trees, randomness, and ensemble learning, collectively contributing to its effectiveness in making predictions across various tasks [126].

1. **Building and training the RFC model:** In the proposed TBW-RAnk, the RandomForestClassifier model utilizes the ($n\_estimators$) parameter to determine the number of trees in the forest when training the model on labeled data for classification tasks. In this implementation, each classifier is configured to include 100 trees. Additionally, the (max_depth) parameter specifies the maximum depth of each tree. By setting it to None, there is no constraint on the maximum depth, enabling the trees to grow until all leaves are pure or contain a minimum number of samples. This flexibility in tree growth aids in capturing the complex patterns present in the data, potentially enhancing the model's predictive performance. The ($min\_samples\_split$) parameter is used to prevent overfitting by ensuring that splits that create noise are not made. Also, the ($min\_samples\_leaf$) parameter is utilized to help improve model generalization and ensure the model's detections are based on substantial data patterns. The ($random\_state$) parameter is used for reproducibility. The dataset is divided into the training and testing stages, where 80% of the data is allocated for training and the remaining 20% for testing. The model employs the RandomForestClassifier module from the scikit-learn library in Python. Table 7.5 shows the parameters used for building and training the model.

Parameter	*Description*	**Value**
n_estimators	*Number of trees in the forest*	100
max_depth	*The maximum depth of the tree*	20
min_samples_split	*Minimum number of samples required to split an internal node*	2
min_samples_leaf	*Minimum number of samples required to form a leaf node*	1
random_state	*Controls the randomness of the bootstrapping of the samples*	42

Table 7.5: Model building and training parameters for the RFC model

2. **Evaluation and validation using performance metrics and cross-validation:** Accuracy, precision, recall, and F1 score metrics were used as the performance metrics. They measure a model's success in accurately predicting outcomes based on the input data. Figure 7.5 illustrates the average performance metrics for all outputs. Appendix A.1 shows the performance metrics for each output. For cross-validation, the dataset was divided into training and testing sets. Then, the proposed model was trained on the training set and validated on the test set. These steps were repeated five times with different sets of training and testing.

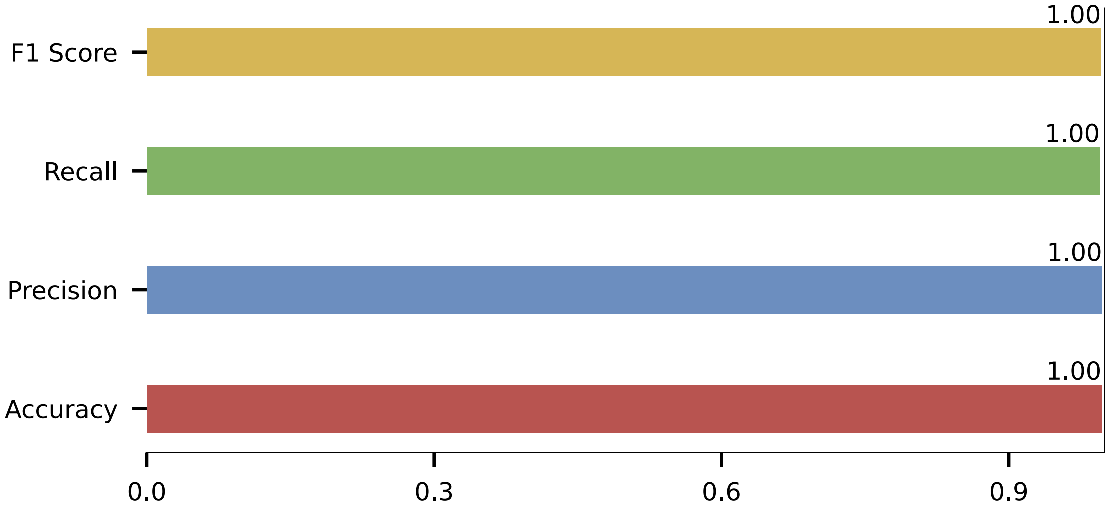


Figure 7.5: Average performance metrics of RFC

7.3.4 Developing the Proposed Solution Utilizing the Support Vector Classifier Model (SVC:)

SVC is one of the most commonly used supervised learning algorithms for classification and regression problems. It can efficiently handle n-dimensional space and non-linear relationships between features and target variables. It can determine the optimal planes that separate data points of different classes or predict the target variable with maximum margin, leading to robust and generalizable models [127].

1. **Building and training the SVC model:** Hyperparameter tuning was conducted for multiple SVC models, each corresponding to a different label in the proposed multi-output classification framework. Given its efficacy in capturing non-linear relationships in the data, the SVC models were configured with a radial basis function (RBF) kernel. The optimization process explored predefined hyperparameters with the regularization parameter C and the kernel coefficient $gamma$ to identify the combination that maximizes classification accuracy. The regularization parameters include three values for C (0.1, 1, 10) and five settings for $gamma$ ('scale,' 'auto,' 0.1, 1, 10), resulting in a comprehensive search across 15 configurations per model using the $GridSearchCV$. The regularization parameter C controls the trade-off between maximizing the margin between classes and minimizing classification errors, allowing the model's performance to be fine-tuned. The Python programming language is utilized for the experiment setup, leveraging the scikit-learn library for machine learning functionalities. To train and test the SVC model, the dataset is divided into 80% and 20% for training and testing, respectively. The best classifier parameters used for building and training the model are illustrated in Table 7.6.

Parameter	*Description*	**Values**
Regularization parameter (C)	*Controls the trade-off between smooth decision boundary and classifying training points correctly.*	10
Kernel	*Specifies the kernel type to be used in the algorithm, affecting the decision boundary's shape.*	RBF
Kernel coefficient $(gamma)$	*Determines the range of influence of a single training example.*	10

Table 7.6: Building and training parameters for the SVC model

2. **Evaluation and validation using performance metrics and cross-validation:** To measure the SVC model's performance in accurately predicting the BW solution rankings,

precision, recall, and F1 score metrics were employed. The average performance metrics for all outputs are shown in Figure 7.6. Appendix A.2 presents the performance metrics for each output. In addition, cross-validation was used to assess the performance of each parameter configuration. This approach facilitates the selection of the most effective hyperparameters and prevents overfitting by evaluating the model's performance across multiple data subsets.

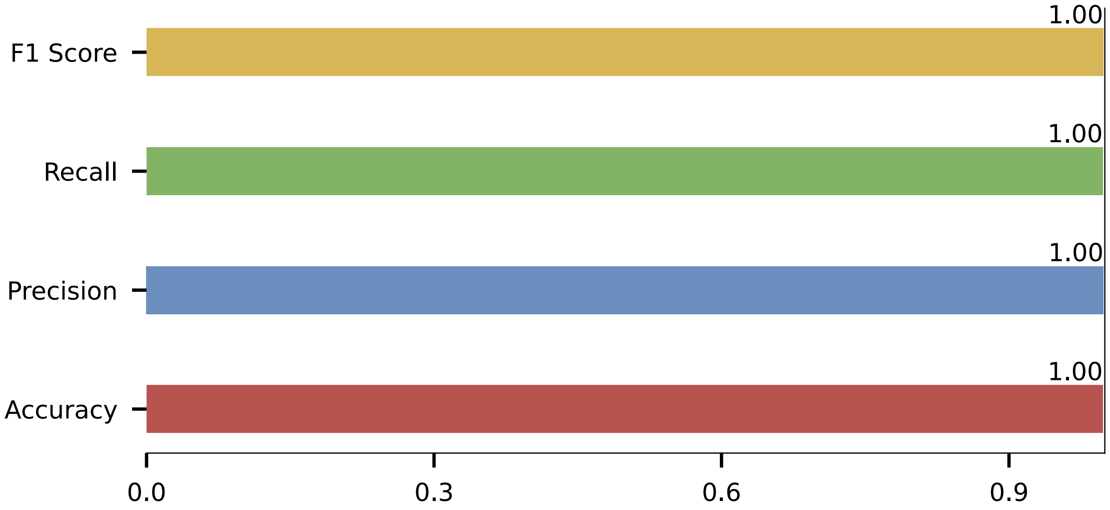
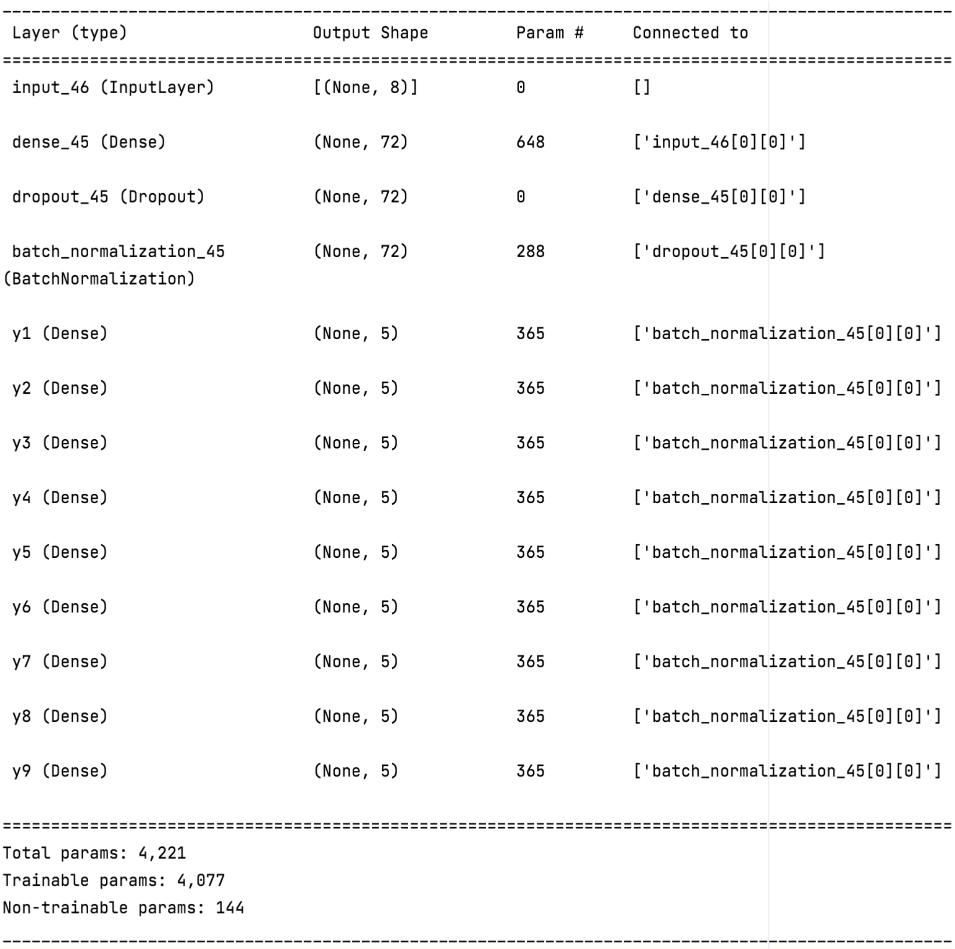


Figure 7.6: Average performance metrics of SVC

7.3.5 Developing the Proposed Solution Utilizing the Deep Neural Network Model (DNN:)

1. **Building and training the DNN model:** The DNN model consists of a dense layer with 72 neurons and a rectified linear unit (Relu) activation function. The Relu activation function allows the network to introduce non-linearity, enabling it to model complex relationships in the data. A dropout mechanism and batch normalization are employed to enhance the model's generalization capabilities. Dropout ensures that during training, a fraction (30% in our case) of the neurons are ”dropped” or turned off, promoting better distributed network learning and reducing over-reliance on particular neurons. Batch normalization normalizes the activation of the neurons, ensuring that the distribution remains consistent across batches, which can accelerate training and facilitate the learning process. The model is constructed with the Adam optimizer and categorical cross-entropy as loss functions. The Adam optimizer is well known for its adaptability to large datasets and complex architectures. The softmax activation, a categorical cross-entropy loss, is appropriate to ensure that the model can accurately predict the probability distribution over the categories. This architecture is distinguished by its ability to predict multiple outputs simultaneously. To identify categories effectively, the network branches out into a dense layer with a softmax activation function for each target column. Consequently, each output is given a set of learnable weights and can accurately predict categories. The dataset is partitioned into three sets to facilitate the evaluation and optimization of the proposed solution. Initially, 80% of the dataset is used for training, allowing the model to learn and refine its parameters based on the available data. 10% of the dataset is for validation within this training set. It is essential to fine-tune hyper parameters, monitor the model's performance during training, and protect against overfitting. Finally, the remaining 20% of the dataset is for testing the finalized model. This testing set objectively evaluates the model's performance on unseen data. Figure 7.7 shows the structure of the DNN model.

2. **Evaluation and validation using performance metrics and cross-validation:** The model was evaluated utilizing the Keras built-in `evaluate` function to assess its performance in terms of loss function and accuracy, as shown in Figure 7.8. The model has simultaneous multi-output layers and a multi-class nature. Thus, average metrics provide a comprehensive view of the model's performance across all outputs and are particularly insightful in multi-output scenarios. The loss function and accuracy metrics for the training and validation sets were calculated for every output and then averaged, providing



```
_____________________________________________________________________________________________
 Layer (type)                   Output Shape         Param #     Connected to
=============================================================================================
 input_46 (InputLayer)          [(None, 8)]          0           []

 dense_45 (Dense)               (None, 72)           648         ['input_46[0][0]']

 dropout_45 (Dropout)           (None, 72)           0           ['dense_45[0][0]']

 batch_normalization_45         (None, 72)           288         ['dropout_45[0][0]']
(BatchNormalization)

 y1 (Dense)                     (None, 5)            365         ['batch_normalization_45[0][0]']

 y2 (Dense)                     (None, 5)            365         ['batch_normalization_45[0][0]']

 y3 (Dense)                     (None, 5)            365         ['batch_normalization_45[0][0]']

 y4 (Dense)                     (None, 5)            365         ['batch_normalization_45[0][0]']

 y5 (Dense)                     (None, 5)            365         ['batch_normalization_45[0][0]']

 y6 (Dense)                     (None, 5)            365         ['batch_normalization_45[0][0]']

 y7 (Dense)                     (None, 5)            365         ['batch_normalization_45[0][0]']

 y8 (Dense)                     (None, 5)            365         ['batch_normalization_45[0][0]']

 y9 (Dense)                     (None, 5)            365         ['batch_normalization_45[0][0]']

=============================================================================================
Total params: 4,221
Trainable params: 4,077
Non-trainable params: 144
_____________________________________________________________________________________________
```

Figure 7.7: The structure of the DNN model

a comprehensive metric. For each output layer, which corresponds to a ranking criterion, categorical cross-entropy as the loss function L was used. Given that each output has five possible classes, the average categorical cross-entropy loss for an individual output layer k can be defined as:

$$L_k = -\frac{1}{N}\sum_{i=1}^{N}\sum_{j=1}^{5} y_{ij}\log(p_{ij}) \tag{7.4}$$

where:

- N represents the number of data points in the dataset
- y_{ij} denotes the true label for class j of output layer k.
- p_{ij} represents the predicted probability for class j of output layer k.

The average loss from all nine output layers and data points is calculated as follows:

$$L = \frac{1}{9}\sum_{k=1}^{9} L_k \tag{7.5}$$

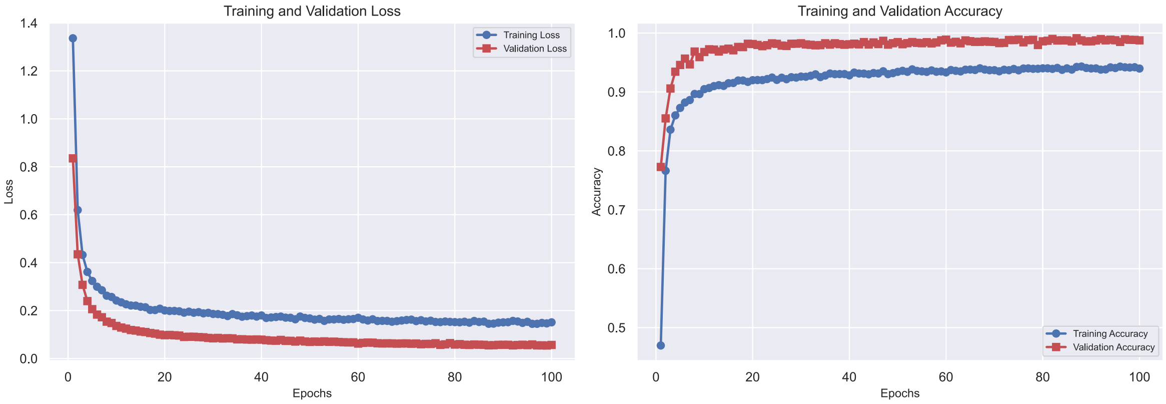


Figure 7.8: The average loss and accuracy of DNNs during training and validation

Moreover, to measure the performance of the DNN model, accuracy, precision, recall, and F1 score metrics were used. The performance metrics of the proposed DNN models are illustrated in Figure 7.9. Appendix A.3 presents the performance metrics for each output separately. K-fold cross-validation was used for each output on the training set and then evaluated on the test set to assess its performance.

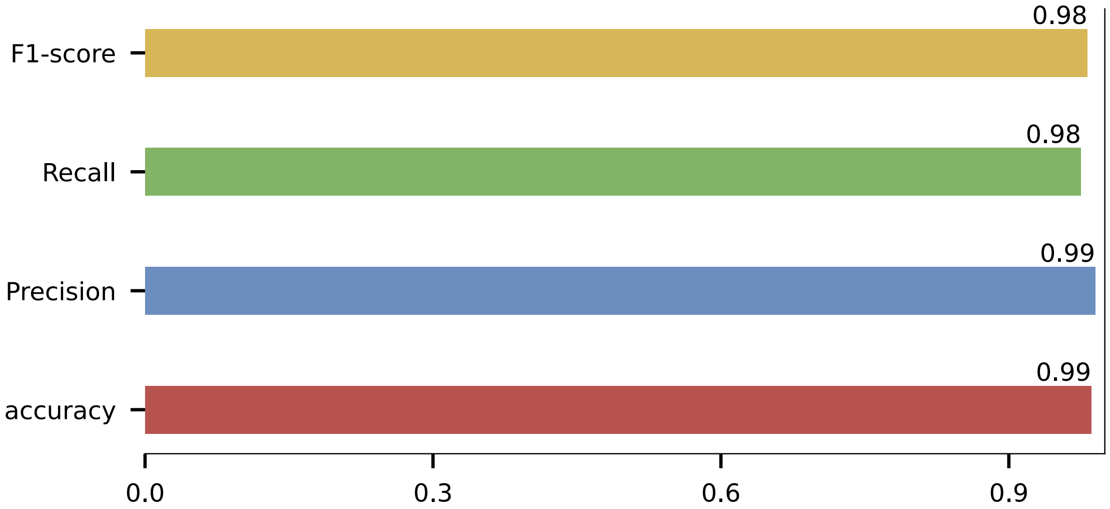


Figure 7.9: Average performance of DNN

7.4 Results and Discussion of the TBW-RAnk

This section discusses the outcomes of the proposed AI models, utilizing average cross-validation techniques to comprehensively assess their performance. Additionally, it examines the overall performance metrics, summarizing the average results across all outputs to provide a comprehensive overview of the model's effectiveness.

- **Comparison of the RFC, SVC and DNN models using average performance metrics:** Average performance metrics across multiple outputs are used in AI to provide a single summary statistic of a model's overall performance. The average of these metrics across all outputs can provide a general indication of the model's effectiveness on various tasks. As shown in Figures 7.5, 7.6 and 7.9, we used accuracy, precision, recall, and F1 score metrics to measure the performance of the RFC, SVC and DNN models.RFC and SVC achieved a perfect score of 1 (or 100%) for the accuracy matrix. This indicates that every prediction made by both models was correct. Regarding the precision matrix, the RFC and SVC models scored 1, meaning that every positive prediction made by the models was positive. In the recall matrix, the RFC and SVC models also scored 1, meaning they successfully identified all positive instances in the dataset without missing any. With precision and recall scoring 1, the F1 scores are 1, indicating a perfect balance between precision and recall. The results suggest that the RFC and SVC models ideally classified or predicted the general and personalized rankings of BW solutions. The DNN achieved an accuracy of 0.99, indicating that 99% of its predictions were correct. This is slightly lower than the perfect scores of RF and CVM but shows a high level of performance. As indicated by the precision score of 0.99, the DNN made very few false positive errors. At the same time, the recall of 0.98 suggests that the DNN can identify 98% of all positive instances, missing only a few. The F1 score of 0.98 is a harmonic mean of precision and recall, indicating a robust balance between the two. This suggests that the DNN has both high precision and high recall. While the DNN does not achieve perfect scores, it shows a very high level of performance across all metrics. The slight difference in recall (0.98) versus precision (0.99) suggests it is slightly more effective at identifying positive instances than avoiding false positives. Regardless, the overall balance is excellent, as shown by the F1 score.

- **Comparison of RFC, SVC and DNN models using cross-validation:** We systematically assessed the model's performance through k-fold cross-validation, executing the evaluation across various folds on five separate data subsets to ensure a thorough and reliable analysis. Table 7.7 shows the cross-validation results for the proposed RFC, SVC and

DNN models. These results provide a basis for comparing and selecting the best model from our proposed AI models. RFC and SVC have a high mean accuracy of 1.0, indicating they are highly effective at perfectly assessing the BW solution's trustworthiness. This accuracy suggests that RFC and SVC models can make reliable BW ranking predictions in most scenarios. DNN, on the other hand, has a mean accuracy of 0.99, which is lower than RFC and SVC. Although still high, it indicates that DNN may not perform as consistently as the other two models in accurately evaluating the trustworthiness of BW solutions. Regarding standard deviations, SVC has the lowest standard deviation (0.001), suggesting that its performance is highly consistent across different data sets. This consistency is crucial for maintaining reliability in various scenarios. In addition, RFC has a slightly higher standard deviation (0.002) than SVC, indicating higher variability in its accuracy, but it remains consistent overall. DNN shows the highest standard deviation (0.003), implying higher variability in accuracy that may affect its reliability, especially in complex BW solution evaluations. However, because of the minimal difference in performance results among models, training time is considered a decisive factor in selecting the optimal deployment model. RFC has a training time of 18 seconds, making it the fastest model to train of the three. This efficiency in training time is beneficial for scenarios requiring multi-output prediction. SVC takes longer to train than RFC, with a training time of 33 seconds. The increased training time is a trade-off for its high accuracy and low variability. DNN requires the longest training time, which is 1 minute and 35 seconds. This longer duration could be due to the complexity of neural networks and the computations involved. While it offers the benefit of handling non-linear data, the trade-off comes from increased computational resources and time. Overall, RFC and SVC stand out for their exceptional accuracy and low variability, with RF being more time-efficient and SVC showing slightly better consistency across different datasets, whereas DNN offers good accuracy, shows more variability and requires a significantly longer training time, which might limit its applicability in situations where rapid deployment or real-time predictions are necessary.

AI Model	**Mean Accuracy**	**Standard Deviations**	**Training Time**
RFC	1.0	0.002	18 seconds
SVC	1.0	0.001	33 seconds
DNN	0.99	0.003	1 minute, 35 seconds

Table 7.7: Comparison of the RFC, SVC and DNN models using cross-validation

7.5 Chapter Summary

- This chapter proposed the CCCI methodology for assessing the trustworthiness of BW solutions, utilizing wallet features as evaluation criteria. In addition, a trust-based ranking system (TBW-RAnk) for BW solutions was developed using RFC, SVC, and DNN models. The performance of each model was evaluated using accuracy, precision, recall, and F1 score metrics. The proposed models were compared using cross-validation to demonstrate their efficacy in accurately predicting the BW solution's ranking in a general and personalized manner. The results indicate that RFC offers a satisfactory balance between accuracy, efficiency, and consistency, which makes it an excellent choice for scenarios where multi-output predictions are needed.

- The next chapter (Chapter 8) presents the conclusion and suggests promising directions for future research.

CHAPTER

8 Conclusions and Future Work

8.1 Chapter Overview

This chapter concludes the thesis by summarizing the research results and suggests future research directions. This thesis integrates robust and adaptive security measures to enhance the security and trustworthiness of BW solutions. The proposed solution introduces a secure and reliable platform, leveraging 2FA and MFA, primarily improving access controls in BW solutions. Combining 2FA and MFA strengthens the security infrastructure of BW solutions by ensuring a multi-layered defence against potential threats. This approach not only safeguards access but also contributes to establishing a trustworthy environment. Additionally, the platform offers an AI-driven ranking system: a mechanism for accessing general and personalized rankings of BW solutions. Integrating AI models adds a dimension of intelligence to the platform, allowing it to generate comprehensive rankings tailored to individual BW user preferences. This advancement contributes significantly to the user experience in the BW community, providing valuable insights and aiding decision-making processes. The chapter is organized as follows: Section 8.2 outlines the problems that form the central emphasis of this thesis. Section 8.3 presents the significant contributions of the thesis. Lastly, Section 8.4 provides suggestions for future investigations, specifically exploring emerging security challenges in the BW landscape.

8.2 Problems Addressed in this Thesis

1. *Research Problem 1:* Integration of Hard and Soft Security Methods: Existing literature lacks an approach that effectively integrates hard and soft security methods to enhance the security of BW solutions. While various security measures exist, the absence of a comprehensive strategy combining robust physical (hard) and sophisticated logical (soft) security creates a vulnerability in the overall security framework.

2. *Research Problem 2:* Limited Use of Biometrics in Authentication: There is a noticeable gap in the literature regarding the use of biometrics to enhance authentication techniques for BW solutions, specifically using face recognition. Biometric authentication is a unique and secure method, yet the literature indicates limited exploration of its potential to strengthen the security layers of BW solutions.

3. *Research Problem 3:* Lack of Trust-based Assessment: Current research falls short in providing approaches that enable entities to conduct trust-based assessments on BW solutions to improve user adoption and acceptance. This gap hinders BW users and stakeholders from making informed decisions when choosing a BW solution that meets their requirements. The introduction of structured methodology and algorithms for establishing, evaluating, and managing trust among BW participants facilitates the decision-making process for selecting the best BW solution.

4. *Research Problem 4:* Intelligent Assessment and Ranking of BW solutions: There is a gap in the literature concerning intelligent assessment and ranking mechanisms for BW solutions. The lack of research on leveraging AI models for automated evaluation and ranking of BW solutions hinders the development of dynamic, adaptive, and context-aware assessment approaches.

8.3 Thesis Contributions

This thesis demonstrates that integrating hard and soft security mechanisms can improve BW security significantly, protecting them from various cyber attacks. The following are the contributions of this thesis:

8.3.1 Contribution 1: State-of-the-art SLR of the existing literature

We conducted a comprehensive systematic literature review (SLR) that focuses on BW security and trustworthiness. The SLR involved a rigorous academic exercise to collect, analyze, and synthesize existing research in BW security. This literature review provided a deeper understanding of the current security mechanisms employed in BWs, identifying the gaps, topics, and areas of consensus in recent research. This SLR covered many studies, ensuring a holistic view of the field. It categorized the existing work based on various security mechanisms and approaches proposed and implemented in BW systems. This categorization allowed for a clear and organized presentation of the current knowledge landscape, facilitating a better understanding of where the field stands and what areas require further exploration (see Chapter 2).

8.3.2 Contribution 2: Building a secure and trustworthy BW framework (STBWF)

The proposed framework is the cornerstone for developing secure, intelligent, and trustworthy BW solutions that integrate 2FA and MFA as a hard security measure and an AI-based ranking system as a soft security measure. It is built to facilitate the implementation and development of secure, intelligent, and trustworthy BW solutions. Also, it creates efficient and responsive BW solutions by introducing abstraction layers that provide a higher level of functionality. It allows for the integration of security and trustworthiness features seamlessly at a more abstract and intuitive level (see Chapter 5).

8.3.3 Contribution 3: Developing a BW website (BWW) with four authentication mechanisms

We developed and implemented a comprehensive system model for the BWW with four authentication mechanisms. This model provides a detailed overview of the various components in a wallet's architecture, effectively illustrating the relationship between cryptographic keys, blockchain networks, and user interfaces. This contribution includes creating a BWW that provides users with a secure platform for managing their cryptographic keys and digital assets. The innovative aspect of this system is the incorporation of a multi-modal authentication framework, allowing users to select from a variety of authentication options: Setting-1 (S1) Passwords Only, Setting-2 (S2) Passwords + Time-based One-Time Password (TOTP), Setting-3 (S3) Passwords + Face Recognition, and Setting-4 (S4) Passwords + TOTP + Face Recognition. This range of options allows for varied levels of security, serving different user preferences and risk tolerance (see Chapter 6).

8.3.4 Contribution 4: Developing a Trust-Based Ranking system (TBW-RAnk) using AI Models

We introduced a novel approach for ranking BW solutions according to the trustworthiness factors using RFC, SVC and DNN models. In this TBW-RAnk, BW solutions are assessed and ranked transparently based on several trusted and objective criteria. Ranking factors include MFA support, wallet age, support for multiple cryptocurrencies, currency control, user rating, and level of security. Consequently, BW users can make informed decisions, increasing their security within the blockchain ecosystem (see Chapter 7).

8.3.5 Contribution 5: Evaluation and validation of the proposed prototype

The proposed system is comprehensively evaluated using multiple approache, including a prototype demonstration. For hard security, the thesis extends beyond development to include a rigorous assessment of the four implemented authentication settings in the BBW. This evaluation is conducted through simulated attacks against BW accounts, aiming to quantify the effectiveness of each authentication setting. In addition, for soft security, the performance and accuracy of the TBW-RAnk are assessed based on accuracy, precision, recall, and F1 score (see Chapters 6 and 7).

8.4 Future Work

Several recommendations based on the findings of this thesis that may serve as inspiration for new research initiatives are as follows:

A. **Storing BW Solution Features in a Decentralized Manner:** While this thesis has introduced innovative advancements in designing and developing a secure, intelligent, and trustworthy BW solution, enhancing the storage and retrieval of BW solution features within the blockchain network offers several benefits and opportunities for further research. It includes investigating strategies to incorporate BW features directly into the blockchain ledger by leveraging smart contracts encapsulating essential information about BW solutions. Smart contracts automate the management process, enabling the blockchain community to determine feature updates or modifications using voting mechanisms, stakeholder participation, and other decentralized decision-making techniques.

B. **Leveraging Blockchain Technology for the Secure Storage of BW Users' Credentials:** An exciting prospect for future research involves utilizing blockchain technology as a secure and decentralized repository for storing BW users' sensitive credentials. Integrating user authentication credentials such as passwords and biometrics data directly into the blockchain ledger enhances security and transparency. For instance, it may include investigating mechanisms for fostering a paradigm shift in authentication techniques for BW owners, enabling the secure and user-centric management of the credentials of BW owners.

C. **Evaluating Additional Advanced Biometric Authentication Techniques:** The security and trustworthiness of BW solutions are becoming increasingly critical. An innovative method for MFA is required due to the growing sophistication of cyber threats. Exploring technologies beyond fingerprints and facial recognition, such as retina scans and heartbeat pattern identification, can offer BW users advanced security and convenience. These factors are inherently unique to each individual and provide effective methods for controlling access to BW solutions. In addition, behavioral biometrics can be analyzed to authenticate BW users using a continuous authentication system that can be created by analyzing patterns in typing, device interaction, and other behaviors. This method improves security by detecting anomalies in BW user behaviors to identify unauthorized access.

D. **Evaluating a Broad Spectrum of BW Solutions Threats:** While phishing attacks are a substantial concern, they are one aspect of numerous vulnerabilities. Future work should expand the focus to encompass more risks to ensure reliable BW solution security. The considerable threats encountered by BW solutions must be recognized and categorized using a systematic threat analysis. The threats may include the impacts of spyware, private key theft, ransomware, and cryptojacking, proposing detection, prevention, and recovery mechanisms.

E. **Advanced AI-Driven Trustworthiness Ranking for BW solutions:** Leveraging AI to rank BW solutions is a promising research direction. An essential part of future research involves conducting a feature importance analysis to identify which aspects most significantly influence the reliability of BW solutions. Determining the appropriate criteria for the trustworthiness of BW solutions is critical. This includes evaluating the robustness of security protocols, the frequency of updates, historical sensitive data breaches, the effectiveness of privacy measures, and adherence to legal and regulatory standards such as GDPR [128]. Additionally, establishing a real-time BW ranking solution can ensure that the rankings reflect the latest developments and provide BW users with current recommendations. This offers a novel mechanism for BW users to determine the most appropriate BW solutions that meet their requirements.

References

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system", *Decentralized Business Review*, p. 21 260, 2008. [Online]. Available: https://assets.pubpub.org/d8wct41f/31611263538139.pdf.

[2] P. K. Kaushal, A. Bagga, and R. Sobti, "Evolution of bitcoin and security risk in bitcoin wallets", in *International Conference on Computer, Communications and Electronics*, IEEE, 2017, pp. 172–177. DOI: 10.1109/COMPTELIX.2017.8003959.

[3] A. Phillip, J. S. Chan, and S. Peiris, "A new look at cryptocurrencies", *Economics Letters*, vol. 163, pp. 6–9, 2018. DOI: 10.1016/j.econlet.2017.11.020.

[4] K. Ranganathan, "Trustworthy pervasive computing: The hard security problems", in *IEEE Annual Conference on Pervasive Computing and Communications Workshops*, 2004, pp. 117–121. DOI: 10.1109/PERCOMW.2004.1276916.

[5] J. Lindley-French, "The revolution in security affairs: Hard and soft security dynamics in the 21st century", *European Security*, vol. 13, no. 1-2, pp. 1–15, 2004. DOI: 10.1080/09662830490484773.

[6] M. Nofer, P. Gomber, O. Hinz, and D. Schiereck, "Blockchain", *Business & Information Systems Engineering*, vol. 59, pp. 183–187, 2017. DOI: 10.1007/s12599-017-0467-3.

[7] Y. Li, G. Yang, W. Susilo, Y. Yu, M. H. Au, and D. Liu, "Traceable monero: Anonymous cryptocurrency with enhanced accountability", *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 2, pp. 679–691, 2021. DOI: 10.1109/TDSC.2019.2910058.

[8] A. Biryukov and S. Tikhomirov, "Security and privacy of mobile wallet users in bitcoin, dash, monero, and zcash", *Pervasive and Mobile Computing*, vol. 59, p. 101 030, 2019. DOI: 10.1016/j.pmcj.2019.101030.

[9] V. Dhillon, D. Metcalf, M. Hooper, V. Dhillon, D. Metcalf, and M. Hooper, "The hyperledger project", *Blockchain Enabled Applications: Understand the Blockchain Ecosystem and how to Make it Work for you*, pp. 139–149, 2017. DOI: 10.1007/978-1-4842-3081-7_10.

[10] J. Polge, J. Robert, and Y. Le Traon, "Permissioned blockchain frameworks in the industry: A comparison", *Ict Express*, vol. 7, no. 2, pp. 229–233, 2021. DOI: 10.1016/j.icte.2020.09.002.

[11] H. Abbas, M. Caprolu, and R. Di Pietro, "Analysis of polkadot: Architecture, internals, and contradictions", in *IEEE International Conference on Blockchain*, 2022, pp. 61–70. DOI: 10.1109/Blockchain55522.2022.00019.

[12] T. Koens and E. Poll, "Assessing interoperability solutions for distributed ledgers", *Pervasive and Mobile Computing*, vol. 59, p. 101 079, 2019. DOI: 10.1016/j.pmcj.2019.101079.

[13] Y. Chen and C. Bellavitis, "Blockchain disruption and decentralized finance: The rise of decentralized business models", *Journal of Business Venturing Insights*, vol. 13, e00151, 2020. DOI: 10.1016/j.jbvi.2019.e00151.

[14] F. Hofmann, S. Wurster, E. Ron, and M. Böhmecke-Schwafert, "The immutability concept of blockchains and benefits of early standardization", in *ITU Kaleidoscope: Challenges for a Data-Driven Society*, 2017, pp. 1–8. DOI: 10.23919/ITU-WT.2017.8247004.

[15] P. P. Momtaz, "Initial coin offerings", *Plos One*, vol. 15, no. 5, e0233018, 2020. DOI: 10.1371/journal.pone.0233018.

[16] B. Lashkari and P. Musilek, "A comprehensive review of blockchain consensus mechanisms", *IEEE Access*, vol. 9, pp. 43 620–43 652, 2021. DOI: 10.1109/ACCESS.2021.3065880.

[17] J. Xie, F. R. Yu, T. Huang, R. Xie, J. Liu, and Y. Liu, "A survey on the scalability of blockchain systems", *IEEE Network*, vol. 33, no. 5, pp. 166–173, 2019. DOI: 10.1109/MNET.001.1800290.

[18] Y. Wang, G. Gou, C. Liu, M. Cui, Z. Li, and G. Xiong, "Survey of security supervision on blockchain from the perspective of technology", *Journal of Information Security and Applications*, vol. 60, p. 102 859, 2021. DOI: 10.1016/j.jisa.2021.102859.

[19] G. Karame and S. Capkun, "Blockchain security and privacy", *IEEE Security and Privacy*, vol. 16, no. 4, pp. 11–12, 2018. DOI: 10.1109/MSP.2018.3111241.

[20] S. Taylor, S. H.-y. Kim, K. A. Zainol Ariffin, and S. N. H. Sheikh Abdullah, "A comprehensive forensic preservation methodology for crypto wallets", *Forensic Science International: Digital Investigation*, vol. 42-43, p. 301 477, 2022, ISSN: 2666-2817. DOI: 10.1016/j.fsidi.2022.301477. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2666281722001585.

[21] M. Lee and D. Jang, "A survey of blockchain security issues", *JP Journal of Heat and Mass Transfer*, vol. 2020, no. Special Is, pp. 29–35, 2020. DOI: 10.17654/HMSI120029.

[22] H. P. Singh, K. Stefanidis, and F. Kirstein, "A private key recovery scheme using partial knowledge", in *International Conference on New Technologies, Mobility and Security*, 2021, pp. 1–5. DOI: 10.1109/NTMS49979.2021.9432642.

[23] M. Aydar, S. C. Cetin, S. Ayvaz, and B. Aygun, "Private key encryption and recovery in blockchain", *ArXiv preprint arXiv:1907.04156*, 2019. DOI: 10.48550/arXiv.1907.04156.

[24] Sapna and D. Prashar, "Analysis on blockchain vulnerabilities & attacks on wallet", in *International Conference on Advances in Computing, Communication Control and Networking*, 2021, pp. 1515–1521. DOI: 10.1109/ICAC3N53548.2021.9725403.

[25] A. Andryukhin, "Phishing attacks and preventions in blockchain based projects", in *International Conference on Engineering Technologies and Computer Science*, 2019, pp. 15–19. DOI: 10.1109/EnT.2019.00008.

[26] S. Houy, P. Schmid, and A. Bartel, "Security aspects of cryptocurrency wallets—a systematic literature review", *ACM Computing Surveys*, vol. 56, no. 1, pp. 1–31, 2023. DOI: 10.1145/3596906.

[27] H. Albayati, S. K. Kim, and J. J. Rho, "A study on the use of cryptocurrency wallets from a user experience perspective", *Human Behavior and Emerging Technologies*, vol. 3, no. 5, pp. 720–738, 2021. DOI: 10.1002/hbe2.313.

[28] V. Marella, B. Upreti, J. Merikivi, and V. K. Tuunainen, "Understanding the creation of trust in cryptocurrencies: The case of bitcoin", *Electronic Markets*, vol. 30, no. 2, pp. 259–271, 2020. DOI: 10.1007/s12525-019-00392-5.

[29] M. Janssen, V. Weerakkody, E. Ismagilova, U. Sivarajah, and Z. Irani, "A framework for analysing blockchain technology adoption: Integrating institutional, market and technical factors", *International Journal of Information Management*, vol. 50, pp. 302–309, 2020. DOI: 10.1016/j.ijinfomgt.2019.08.012.

[30] A. Lazarenko and S. Avdoshin, “Financial risks of the blockchain industry: A survey of cyberattacks”, in *Proceedings of the Future Technologies Conference*, Springer, 2019, pp. 368–384. DOI: 10.1007/978-3-030-02683-7_26.

[31] A. J. Bidgoly, “Robustness verification of soft security systems”, *Journal of Information Security and Applications*, vol. 55, p. 102 632, 2020. DOI: 10.1016/j.jisa.2020.102632.

[32] M. Sain, O. Normurodov, C. Hong, and K. L. Hui, “A survey on the security in cyber physical system with multi-factor authentication”, in *International Conference on Advanced Communication Technology*, 2021, pp. 1–8. DOI: 10.23919/ICACT51234.2021.9370515.

[33] A. Asudeh, H. Jagadish, J. Stoyanovich, and G. Das, “Designing fair ranking schemes”, in *International Conference on Management of Data*, 2019, pp. 1259–1276. DOI: 10.1145/3299869.3300079.

[34] S. K. Dwivedi, R. Amin, and S. Vollala, “Blockchain based secured information sharing protocol in supply chain management system with key distribution mechanism”, *Journal of Information Security and Applications*, vol. 54, p. 102 554, 2020. DOI: 10.1016/j.jisa.2020.102554.

[35] S. Mollajafari and K. Bechkoum, “Blockchain technology and related security risks: Towards a seven-layer perspective and taxonomy”, *Sustainability*, vol. 15, no. 18, p. 13 401, 2023. DOI: 10.3390/su151813401.

[36] E. Zaghloul, T. Li, M. W. Mutka, and J. Ren, “Bitcoin and blockchain: Security and privacy”, *IEEE Internet of Things Journal*, vol. 7, no. 10, pp. 10 288–10 313, 2020. DOI: 10.1109/JIOT.2020.3004273.

[37] H. Zhao, Y. Zhang, Y. Peng, and R. Xu, “Lightweight backup and efficient recovery scheme for health blockchain keys”, in *IEEE International Symposium on Autonomous Decentralized System*, 2017, pp. 229–234. DOI: 10.1109/ISADS.2017.22.

[38] J. Leng, M. Zhou, J. L. Zhao, Y. Huang, and Y. Bian, “Blockchain security: A survey of techniques and research directions”, *IEEE Transactions on Services Computing*, vol. 15, no. 4, pp. 2490–2510, 2022. DOI: 10.1109/TSC.2020.3038641.

[39] S. Liu, L. Chen, H. Yu, S. Gao, and H. Fang, “BP-AKAA: Blockchain-enforced Privacy-preserving Authentication and Key Agreement and Access Control for IIoT”, *Journal of Information Security and Applications*, vol. 73, p. 103 443, 2023. DOI: 10.1016/j.jisa.2023.103443.

[40] D. Rushita, K. Sood, and U. S. Yadav, "Cryptocurrency and digital money in the new era", in *Digital Transformation, Strategic Resilience, Cyber Security and Risk Management*, vol. 111, Emerald Publishing Limited, 2023, pp. 179–190. DOI: 10.1108/S1569-37592023000111B013.

[41] A. Verma, P. Bhattacharya, U. Bodkhe, D. Saraswat, S. Tanwar, and K. Dev, "Fedrec: Trusted rank-based recommender scheme for service provisioning in federated cloud environment", *Digital Communications and Networks*, vol. 9, no. 1, pp. 33–46, 2023. DOI: 10.1016/j.dcan.2022.06.003.

[42] T. Yang, Z. Xu, Z. Wang, A. Tran, and Q. Ai, "Marginal-certainty-aware fair ranking algorithm", in *The ACM International Conference on Web Search and Data Mining*, 2023, pp. 24–32. DOI: 10.1145/3539597.3570474.

[43] A. Altman and M. Tennenholtz, "Ranking systems: The pagerank axioms", in *The 6th ACM Conference on Electronic Commerce*, 2005, pp. 1–8. DOI: 10.1145/1064009.1064010.

[44] K. Loewke, J. H. Cho, C. D. Brumar, *et al.*, "Characterization of an artificial intelligence model for ranking static images of blastocyst stage embryos", *Fertility and Sterility*, vol. 117, no. 3, pp. 528–535, 2022. DOI: 10.1016/j.fertnstert.2021.11.022.

[45] X. He, J. Lin, K. Li, and X. Chen, "A Novel Cryptocurrency Wallet Management Scheme Based on Decentralized Multi-Constrained Derangement", *IEEE Access*, vol. 7, pp. 185 250–185 263, 2019, ISSN: 2169-3536. DOI: 10.1109/ACCESS.2019.2961183.

[46] H. Rezaeighaleh and C. C. Zou, "New secure approach to backup cryptocurrency wallets", in *IEEE Global Communications Conference*, 2019, pp. 1–6. DOI: 10.1109/GLOBECOM38437.2019.9014007.

[47] F. Zhu, W. Chen, Y. Wang, *et al.*, "Trust your wallet: A new online wallet architecture for bitcoin", in *International Conference on Progress in Informatics and Computing*, 2017, pp. 307–311. DOI: 10.1109/PIC.2017.8359562.

[48] Y. Liu, R. Li, X. Liu, *et al.*, "An efficient method to enhance Bitcoin wallet security", in *IEEE International Conference on Anti-counterfeiting, Security, and Identification*, 2017, pp. 26–29. DOI: 10.1109/ICASID.2017.8285737.

[49] A. G. Khan, A. H. Zahid, M. Hussain, and U. Riaz, "Security Of Cryptocurrency Using Hardware Wallet And QR Code", in *International Conference on Innovative Computing*, 2019, pp. 1–10. DOI: 10.1109/ICIC48496.2019.8966739.

[50] H. Rezaeighaleh and C. C. Zou, “Multilayered Defense-in-Depth Architecture for Cryptocurrency Wallet”, *IEEE 6th International Conference on Computer and Communications*, pp. 2212–2217, 2020. DOI: 10.1109/ICCC51575.2020.9345013.

[51] I. Homoliak, D. Breitenbacher, O. Hujnak, P. Hartel, A. Binder, and P. Szalachowski, “SmartOTPs: An Air-Gapped 2-Factor Authentication for Smart-Contract Wallets”, 2018. [Online]. Available: http://arxiv.org/abs/1812.03598.

[52] P. Urien, “Innovative countermeasures to defeat cyber attacks against blockchain wallets”, in *Cyber Security in Networking Conference*, IEEE, 2021, pp. 49–54. DOI: 10.1109/CSNet52717.2021.9614649.

[53] E. Benli, I. Engin, C. Giousouf, M. A. Ulak, and Ş. Bahtiyar, “BioWallet: A Biometric Digital Wallet”, in *International Conference on Systems*, 2017, pp. 23–27. [Online]. Available: https://www.researchgate.net/publication/329373831_BioWallet_A_Biometric_Digital_Wallet.

[54] A. Albakri and C. Mokbel, “Convolutional neural network biometric cryptosystem for the protection of the blockchain’s private key”, *Procedia Computer Science*, vol. 160, pp. 235–240, 2019, ISSN: 18770509. DOI: 10.1016/j.procs.2019.09.462.

[55] A. Marcedone, R. Pass, and A. Shelat, *Minimizing Trust in Hardware Wallets with Two Factor Signatures*. 2019, vol. 11598 LNCS, pp. 407–425, ISBN: 9783030321000. DOI: 10.1007/978-3-030-32101-7_25.

[56] R. Gennaro, S. Goldfeder, and A. Narayanan, *Threshold-optimal DSA/ECDSA signatures and an application to Bitcoin wallet security*. 2016, vol. 9696, pp. 156–174, ISBN: 9783319395548. DOI: doi.org/10.1007/978-3-319-39555-5_9.

[57] D. Boneh, R. Gennaro, and S. Goldfeder, *Using Level-1 Homomorphic Encryption to Improve Threshold DSA Signatures for Bitcoin Wallet Security*. 2019, vol. 11368 LNCS, pp. 352–377, ISBN: 9783030252823. DOI: 10.1007/978-3-030-25283-0_19.

[58] T. Hu, X. Liu, W. Niu, K. Ding, Y. Wang, and X. Zhang, “Securing the Private Key in Your Blockchain Wallet: A Continuous Authentication Approach Based on Behavioral Biometric”, *Journal of Physics: Conference Series*, vol. 1631, no. 1, 2020, ISSN: 17426596. DOI: 10.1088/1742-6596/1631/1/012104.

[59] A. Thota, P. Upadhyay, S. Kulkarni, P. Selvam, and B. Viswanathan, “Software Wallet Based Secure Participation in Hyperledger Fabric Networks”, in *International Conference on Communication Systems and NETworks*, 2020, pp. 1–6, ISBN: 9781728131870. DOI: 10.1109/COMSNETS48256.2020.9027445.

[60] W. Dai, J. Deng, Q. Wang, C. Cui, D. Zou, and H. Jin, “SBLWT: A secure blockchain lightweight wallet based on trustzone”, *IEEE Access*, vol. 6, pp. 40 638–40 648, 2018, ISSN: 21693536. DOI: 10.1109/ACCESS.2018.2856864.

[61] M. Gentilal, P. Martins, and L. Sousa, “Trustzone-backed bitcoin wallet”, in *Proceedings of the Fourth Workshop on Cryptography and Security in Computing Systems*, ser. CS2 ’17, New York, NY, USA: Association for Computing Machinery, 2017, pp. 25–28, ISBN: 9781450348690. DOI: 10.1145/3031836.3031841.

[62] H. Wang, X. Li, J. Gao, and W. Li, “MOBT: A kleptographically-secure hierarchical-deterministic wallet for multiple offline Bitcoin transactions”, *Future Generation Computer Systems*, vol. 101, pp. 315–326, 2019. DOI: 10.1016/j.future.2019.04.055.

[63] P. Das, S. Faust, and J. Loss, “A formal treatment of deterministic wallets”, in *Proceedings of the ACM Conference on Computer and Communications Security*, 2019, pp. 651–668, ISBN: 9781450367479. DOI: 10.1145/3319535.3354236.

[64] A. Di Luzio, D. Francati, and G. Ateniese, “Arcula: A Secure Hierarchical Deterministic Wallet for Multi-asset Blockchains”, *ArXiv preprint arXiv:1906.05919*, 2019. [Online]. Available: https://arxiv.org/abs/1906.05919.

[65] T. S. Perry, “A bitcoin wallet for the masses: Square simplified credit-card transactions. now it wants to build cryptocurrency hardware”, *IEEE Spectrum*, vol. 59, no. 1, pp. 42–43, 2022. DOI: 10.1109/MSPEC.2022.9676357.

[66] P. Praitheeshan, Y. Xin, L. Pan, and R. Doss, *Attainable hacks on keystore files in ethereum wallets—A systematic analysis*. 2019, vol. 1113 CCIS, pp. 99–117, ISBN: 9783030343521. DOI: 10.1007/978-3-030-34353-8_7.

[67] T. Volety, S. Saini, T. McGhin, C. Liu, and K.-K. Choo, “Cracking Bitcoin wallets: I want what you have in the wallets”, *Future Generation Computer Systems*, vol. 91, pp. 136–143, 2019. DOI: 10.1016/j.future.2018.08.029.

[68] C.-I. Fan, Y.-F. Tseng, H.-P. Su, R.-H. Hsu, and H. Kikuchi, “Secure hierarchical Bitcoin wallet scheme against privilege escalation attacks”, *International Journal of Information Security*, pp. 1–11, 2019, ISSN: 1615-5270. DOI: 10.1007/s10207-019-00476-5.

[69] L. Wang, J. Gao, and X. Li, “Efficient Bitcoin Password-protected Wallet Scheme with Key-dependent Message Security.”, *IJ Network Security*, no. 5, pp. 774–784, 2019. [Online]. Available: http://ijns.jalaxy.com.tw/contents/ijns-v21-n5/ijns-2019-v21-n5-p774-784.pdf.

[70] A. Davenport and S. Shetty, "Air Gapped Wallet Schemes and Private Key Leakage in Permissioned Blockchain Platforms", in *IEEE INTERNATIONAL CONFERENCE ON BLOCKCHAIN*, 2019, pp. 541–545, ISBN: 978-1-7281-4693-5. DOI: 10.1109/Blockchain.2019.00004.

[71] W. Yin, Q. Wen, W. Li, H. Zhang, Z. Jin, and Ping, "An Anti-Quantum Transaction Authentication Approach in Blockchain", *IEEE ACCESS*, vol. 6, pp. 5393–5401, 2018, ISSN: 2169-3536. DOI: 10.1109/ACCESS.2017.2788411.

[72] M. Guri, "BeatCoin: Leaking Private Keys from Air-Gapped Cryptocurrency Wallets", in *IEEE International Conference on Internet of Things and IEEE Green Computing and Communications and IEEE Cyber, Physical and Social Computing and IEEE Smart Data*, 2018, pp. 1308–1316. DOI: 10.1109/Cybermatics_2018.2018.00227.

[73] A. Gkaniatsou, M. Arapinis, and A. Kiayias, "Low-Level Attacks in Bitcoin Wallets BT - Information Security", in *International Conference on Information Security*, P. Q. Nguyen and J. Zhou, Eds., Springer International Publishing, 2017, pp. 233–253, ISBN: 978-3-319-69659-1. DOI: 10.1007/978-3-319-69659-1_13.

[74] A. Dmitrienko, D. Noack, and M. Yung, "Secure wallet-assisted offline bitcoin payments with double-spender revocation", in *The ACM Asia Conference on Computer and Communications Security*, 2017, pp. 520–531, ISBN: 9781450349444. DOI: 10.1145/3052973.3052980.

[75] S. Chan, "Android-based Cryptocurrency Wallets : Attacks and Countermeasures", *IEEE International Conference on Blockchain*, pp. 9–16, 2020. DOI: 10.1109/Blockchain50366.2020.00010.

[76] G. Li and L. You, "A consortium blockchain wallet scheme based on dual-threshold key sharing", *Symmetry*, vol. 13, no. 8, p. 1444, 2021. DOI: 10.3390/sym13081444.

[77] A. Holmes and W. J. Buchanan, "A framework for live host-based bitcoin wallet forensics and triage", *Forensic Science International: Digital Investigation*, vol. 44, p. 301 486, 2023. DOI: 10.1016/j.fsidi.2022.301486.

[78] S. Sung, "A new key protocol design for cryptocurrency wallet", *ICT Express*, vol. 7, no. 3, pp. 316–321, 2021. DOI: 10.1016/j.icte.2021.08.002.

[79] M. Qi, Z. Xu, T. Jiao, S. Wen, Y. Xiang, and G. Nan, "A comparative study on the security of cryptocurrency wallets in android system", in *IEEE International Conference on Trust, Security and Privacy in Computing and Communications*, IEEE, 2022, pp. 399–406. DOI: 10.1109/TrustCom56396.2022.00062.

[80] H. Zhang, X. Zou, G. Xie, and Z. Li, “Blockchain multi-signature wallet system based on qr code communication”, in *Blockchain Technology and Application: 5th CCF China Blockchain Conference*, Springer, 2022, pp. 31–48. [Online]. Available: https://link.springer.com/chapter/10.1007/978-981-19-8877-6_3.

[81] N. Lehto, K. Halunen, O.-M. Latvala, A. Karinsalo, and J. Salonen, “Cryptovault-a secure hardware wallet for decentralized key management”, in *IEEE International Conference on Omni-Layer Intelligent Systems*, IEEE, 2021, pp. 1–4. DOI: 10.1109/COINS51742.2021.9524133.

[82] T. A. Lomazina, T. G. Surovtsova, and D. A. Ivanov, “Development of a cryptocurrency iot wallet with automatic authentication”, in *International Conference on Quality Management, Transport and Information Security, Information Technologies*, IEEE, 2021, pp. 318–323. DOI: 10.1109/ITQMIS53292.2021.9642727.

[83] Z. Jian, Q. Ran, and S. Liyan, “Securing blockchain wallets efficiently based on threshold ecdsa scheme without trusted center”, in *Asia-Pacific Conference on Communications Technology and Computer Science*, IEEE, 2021, pp. 47–51. DOI: 10.1109/ACCTCS52002.2021.00018.

[84] Y. Hu, S. Wang, G.-H. Tu, *et al.*, “Security threats from bitcoin wallet smartphone applications: Vulnerabilities, attacks, and countermeasures”, in *Proceedings of the Eleventh ACM Conference on Data and Application Security and Privacy*, 2021, pp. 89–100. DOI: 10.1145/3422337.3447832.

[85] W. Dai, Q. Wang, Z. Wang, X. Lin, D. Zou, and H. Jin, “Trustzone-based secure lightweight wallet for hyperledger fabric”, *Journal of Parallel and Distributed Computing*, vol. 149, pp. 66–75, 2021. DOI: 10.1016/j.jpdc.2020.11.001.

[86] W.-Y. Chiu, W. Meng, and W. Li, “Tpmwallet: Towards blockchain hardware wallet using trusted platform module in iot”, in *International Conference on Computing, Networking and Communications*, IEEE, 2023, pp. 336–342. DOI: 10.1109/ICNC57223.2023.10074126.

[87] D. Prashar *et al.*, “Analysis on blockchain vulnerabilities & attacks on wallet”, in *International Conference on Advances in Computing, Communication Control and Networking*, IEEE, 2021, pp. 1515–1521. DOI: 10.1109/ICAC3N53548.2021.9725403.

[88] M. Ferreira, S. Rodrigues, C. I. Reis, and M. Maximiano, “Blockchain: A tale of two applications”, *Applied Sciences*, vol. 8, no. 9, p. 1506, 2018. DOI: 10.3390/app8091506.

[89] A. Bosu, A. Iqbal, R. Shahriyar, and P. Chakraborty, "Understanding the motivations, challenges and needs of blockchain software developers: A survey", *Empirical Software Engineering*, vol. 24, no. 4, pp. 2636–2673, 2019. DOI: 10.1007/s10664-019-09708-7.

[90] L. Zhou, C. Ge, and C. Su, "A privacy preserving two-factor authentication protocol for the bitcoin spv nodes", *Science China Information Sciences*, vol. 63, pp. 1–15, 2020. DOI: 10.1007/s11432-019-9922-x.

[91] F. Sinigaglia, R. Carbone, G. Costa, and N. Zannone, "A survey on multi-factor authentication for online banking in the wild", *Computers & Security*, vol. 95, p. 101 745, 2020. DOI: 10.1016/j.cose.2020.101745.

[92] K. Dharavath, F. A. Talukdar, and R. H. Laskar, "Study on biometric authentication systems, challenges and future trends: A review", in *IEEE International Conference on Computational Intelligence and Computing Research*, 2013, pp. 1–7. DOI: 10.1109/ICCIC.2013.6724278.

[93] J.-H. Cho, K. Chan, and S. Adali, "A survey on trust modeling", *ACM Computing Surveys*, vol. 48, no. 2, pp. 1–40, 2015. DOI: 10.1109/ICCIC.2013.6724278.

[94] G. Ramos, L. Boratto, and M. Marras, "Reputation equity in ranking systems", in *The ACM International Conference on Information & Knowledge Management*, 2021, pp. 3378–3382. DOI: 10.1145/3459637.3482171.

[95] C. Kothari, *Research Methodology: Methods and Techniques*. New Age International (P) Limited, 2004, ISBN: 9788122415223. [Online]. Available: https://books.google.com.au/books?id=8c6gkbKi-F4C.

[96] K. Peffers, T. Tuunanen, M. A. Rothenberger, and S. Chatterjee, "A design science research methodology for information systems research", *Journal of Management Information Systems*, vol. 24, no. 3, pp. 45–77, 2007. DOI: 10.2753/MIS0742-1222240302.

[97] P. Doerfler, K. Thomas, M. Marincenko, *et al.*, "Evaluating login challenges as adefense against account takeover", in *The World Wide Web Conference*, 2019, pp. 372–382. [Online]. Available: https://dl.acm.org/doi/abs/10.1145/3308558.3313481.

[98] G. Soltana, M. Sabetzadeh, and L. C. Briand, "Synthetic data generation for statistical testing", in *IEEE/ACM International Conference on Automated Software Engineering*, 2017, pp. 872–882. DOI: 10.1109/ASE.2017.8115698.

[99] Y. Luo, H.-H. Tseng, S. Cui, L. Wei, R. K. Ten Haken, and I. El Naqa, "Balancing accuracy and interpretability of machine learning approaches for radiation treatment outcomes modeling", *BJR| Open*, vol. 1, no. 1, p. 20 190 021, 2019. DOI: 10.1259/bjro.20190021.

[100] E. J. Michaud, Z. Liu, and M. Tegmark, "Precision machine learning", *Entropy*, vol. 25, no. 1, p. 175, 2023. DOI: 10.3390/e25010175.

[101] A. Gupta, A. Anand, and Y. Hasija, "Recall-based machine learning approach for early detection of cervical cancer", in *International Conference for Convergence in Technology*, 2021, pp. 1–5. DOI: 10.1109/I2CT51068.2021.9418099.

[102] H. Huang, H. Xu, X. Wang, and W. Silamu, "Maximum f1-score discriminative training criterion for automatic mispronunciation detection", *IEEE/ACM Transactions on Audio, Speech, and Language Processing*, vol. 23, no. 4, pp. 787–797, 2015. DOI: 10.1109/TASLP.2015.2409733.

[103] D. Xu, Y. Shi, I. W. Tsang, Y.-S. Ong, C. Gong, and X. Shen, "Survey on multi-output learning", *IEEE Transactions on Neural Networks and Learning Systems*, vol. 31, no. 7, pp. 2409–2429, 2020. DOI: 10.1109/TNNLS.2019.2945133.

[104] S. Gowrishankar and A. Veena, *Introduction to Python programming*. CRC Press, 2018. [Online]. Available: https://www.google.com.au/books/edition/Introduction_to_Python_Programming/iIqADwAAQBAJ?hl=en&gbpv=1&dq=python+programming&pg=PP1&printsec=frontcover.

[105] M. Grinberg, *Flask web development: developing web applications with python.* " O'Reilly Media, Inc.", 2018. [Online]. Available: https://www.google.com.au/books/edition/Flask_Web_Development/cVlPDwAAQBAJ?hl=en&gbpv=1&dq=flask&pg=PT25&printsec=frontcover.

[106] S. Roy, A. Stavrou, B. L. Mark, K. Zeng, S. M. P D, and K. N. Khasawneh, "Characterization of aes implementations on microprocessor-based iot devices", in *IEEE Wireless Communications and Networking Conference*, 2022, pp. 55–60. DOI: 10.1109/WCNC51071.2022.9771975.

[107] A.-C. Careja and N. Tapus, "Digital identity using blockchain technology", *Procedia Computer Science*, vol. 221, pp. 1074–1082, 2023. DOI: 10.1016/j.procs.2023.08.090.

[108] A. Ghosh, M. Thakur, R. Praveen, and M. Saravanan, “Intelligent job navigation system for rural development”, in *IEEE International Conference on Communication Systems and Network Technologies*, 2021, pp. 892–897. DOI: 10.1109/CSNT51715.2021.9509671.

[109] Y.-C. Chiu, C.-Y. Tsai, M.-D. Ruan, G.-Y. Shen, and T.-T. Lee, “Mobilenet-ssdv2: An improved object detection model for embedded systems”, in *International Conference on System Science and Engineering*, 2020, pp. 1–5. DOI: 10.1109/ICSSE50014.2020.9219319.

[110] J. V. Dillon, I. Langmore, D. Tran, *et al.*, “Tensorflow distributions”, *ArXiv preprint arXiv:1711.10604*, 2017. DOI: 10.48550/arXiv.1711.10604.

[111] K. Krombholz, H. Hobel, M. Huber, and E. Weippl, “Advanced social engineering attacks”, *Journal of Information Security and Applications*, vol. 22, pp. 113–122, 2015. DOI: 10.1016/j.jisa.2014.09.005.

[112] S. Raj and N. K. Walia, “A study on metasploit framework: A pen-testing tool”, in *International Conference on Computational Performance Evaluation*, 2020, pp. 296–302. DOI: 10.1109/ComPE49325.2020.9200028.

[113] M. Kuperberg, “Blockchain-based identity management: A survey from the enterprise and ecosystem perspective”, *IEEE Transactions on Engineering Management*, vol. 67, no. 4, pp. 1008–1027, 2020. DOI: 10.1109/TEM.2019.2926471.

[114] H. Hick, M. Bajzek, and C. Faustmann, “Definition of a system model for model-based development”, *SN Applied Sciences*, vol. 1, pp. 1–15, 2019. DOI: 10.1007/s42452-019-1069-0.

[115] G. Morganti, E. Schiavone, and A. Bondavalli, “Risk assessment of blockchain technology”, in *2018 Eighth Latin-American Symposium on Dependable Computing*, 2018, pp. 87–96. DOI: 10.1109/LADC.2018.00019.

[116] M. N. Halgamuge, “Estimation of the success probability of a malicious attacker on blockchain-based edge network”, *Computer Networks*, vol. 219, p. 109 402, 2022. DOI: 10.1016/j.comnet.2022.109402.

[117] S. Aggarwal and N. Kumar, “Attacks on blockchain”, in *Advances in Computers*, vol. 121, Elsevier, 2021, pp. 399–410. DOI: 10.1016/bs.adcom.2020.08.020.

[118] Y. E. Oktian, S.-G. Lee, and H.-J. Lee, “Twochain: Leveraging blockchain and smart contract for two factor authentication”, in *International Seminar on Research of Information Technology and Intelligent Systems*, 2020, pp. 187–191. DOI: 10.1109/ISRITI51436.2020.9315514.

[119] G. Shemov, B. Garcia de Soto, and H. Alkhzaimi, “Blockchain applied to the construction supply chain: A case study with threat model”, *Frontiers of Engineering Management*, vol. 7, pp. 564–577, 2020. DOI: 10.1007/s42524-020-0129-x.

[120] O. Kramer and O. Kramer, “Scikit-learn”, *Machine Learning for Evolution Strategies*, pp. 45–53, 2016. DOI: 10.1007/978-3-319-33383-0_5.

[121] N. Ketkar and N. Ketkar, “Introduction to keras”, *Deep Learning with Python: A Hands-on Introduction*, pp. 97–111, 2017. DOI: 10.1007/978-1-4842-2766-4_7.

[122] H. Sekhon, C. Ennew, H. Kharouf, and J. Devlin, “Trustworthiness and trust: Influences and implications”, *Journal of Marketing Management*, vol. 30, no. 3-4, pp. 409–430, 2014. DOI: 10.1080/0267257X.2013.842609.

[123] A. Ben-Ner and F. Halldorsson, “Trusting and trustworthiness: What are they, how to measure them, and what affects them”, *Journal of Economic Psychology*, vol. 31, no. 1, pp. 64–79, 2010. DOI: 10.1016/j.joep.2009.10.001.

[124] E. Chang, F. Hussain, and T. Dillon, *Trust and reputation for service-oriented environments: technologies for building business intelligence and consumer confidence*. John Wiley & Sons, 2006. [Online]. Available: https://www.google.com.au/books/edition/Trust_and_Reputation_for_Service_Oriente/7PXZEWsIShsC?hl=en&gbpv=1&dq=Trust+and+Technologies+for+Building+Business+Intelligence+and.&pg=PR5&printsec=frontcover.

[125] J. C. Mendoza-Tello, H. Mora, F. A. Pujol-López, and M. D. Lytras, “Social commerce as a driver to enhance trust and intention to use cryptocurrencies for electronic payments”, *IEEE Access*, vol. 6, pp. 50 737–50 751, 2018. DOI: 10.1109/ACCESS.2018.2869359.

[126] A. Chaudhary, S. Kolhe, and R. Kamal, “An improved random forest classifier for multi-class classification”, *Information Processing in Agriculture*, vol. 3, no. 4, pp. 215–222, 2016. DOI: 10.1016/j.inpa.2016.08.002.

[127] A. Patle and D. S. Chouhan, “SVM kernel functions for classification”, in *International Conference on Advances in Technology and Engineering*, 2013, pp. 1–9. DOI: 10.1109/ICAdTE.2013.6524743.

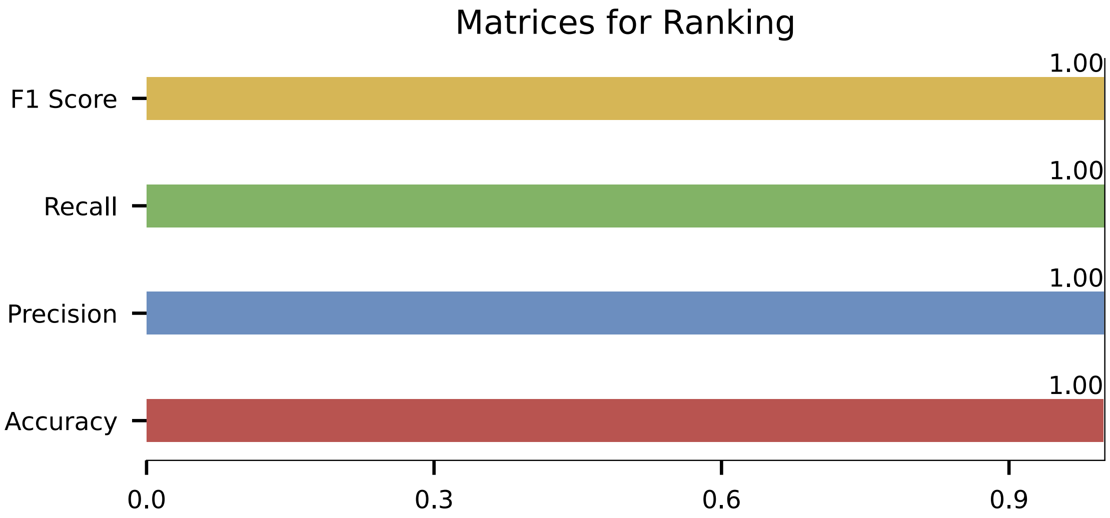
[128] A. B. Haque, A. K. M. N. Islam, S. Hyrynsalmi, B. Naqvi, and K. Smolander, "GDPR Compliant Blockchains–A Systematic Literature Review", *IEEE Access*, vol. 9, pp. 50 593–50 606, 2021. DOI: 10.1109/ACCESS.2021.3069877.

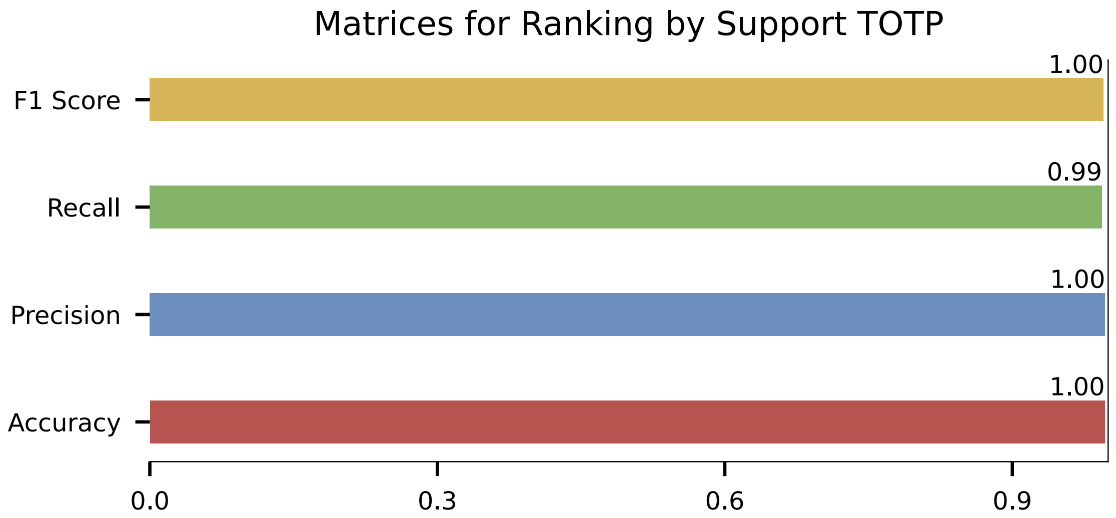
CHAPTER

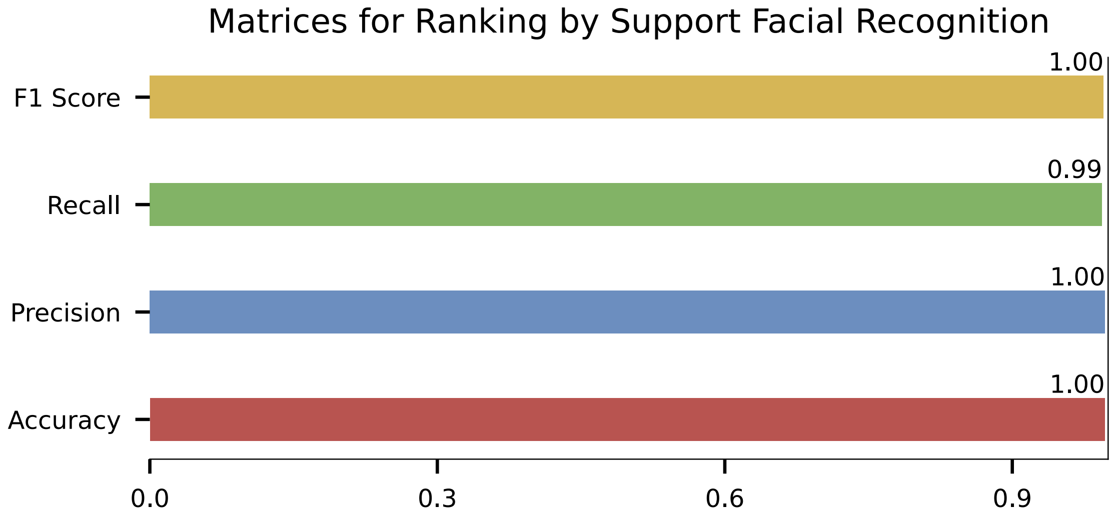
A Appendix

A.1 RFC model performance metrics

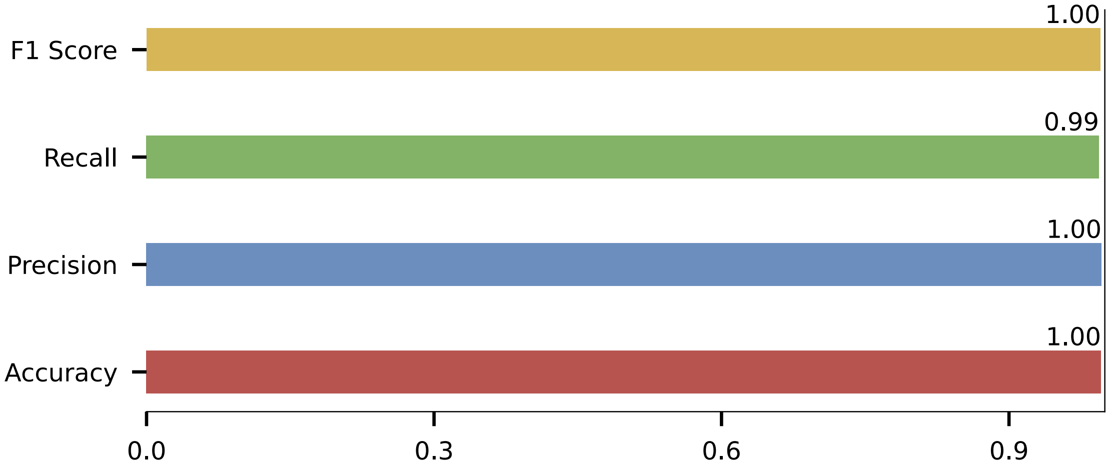
The performance metrics presented in this section correspond to each output label of the RFC model.



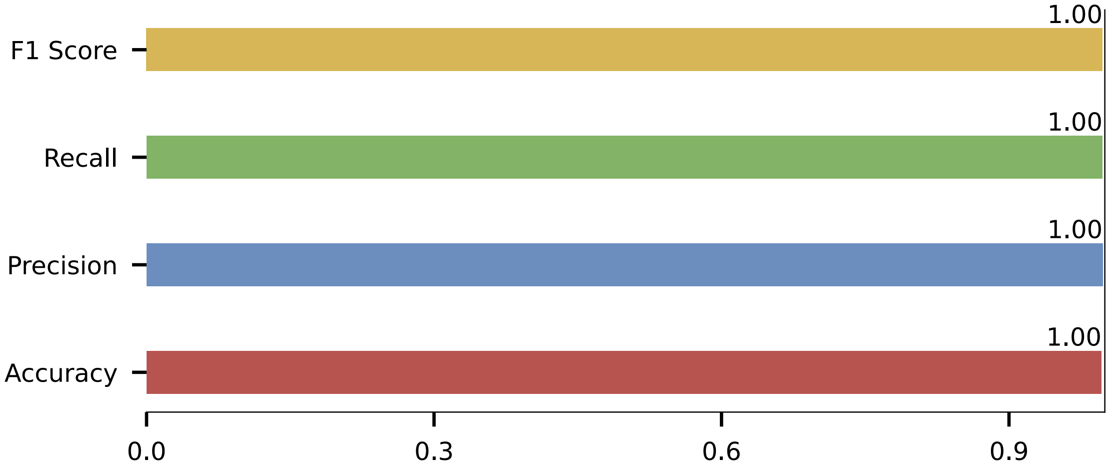

Matrices for Ranking by Support TOTP
F1 Score
Recall
Precision
Accuracy
1.00
0.99
1.00
1.00
0.0
0.3
0.6
0.9

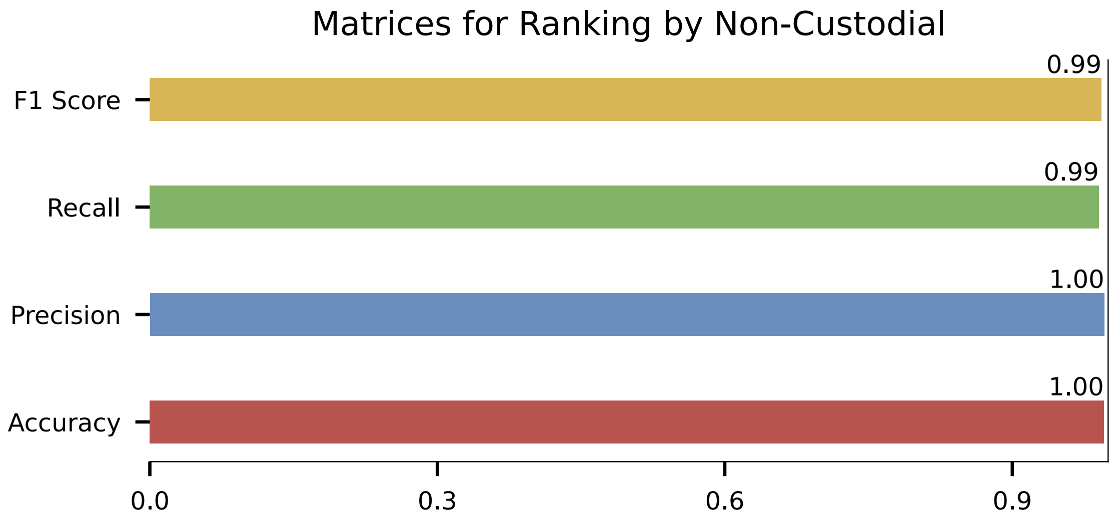

Matrices for Ranking by Support Facial Recognition
F1 Score
Recall
Precision
Accuracy
1.00
0.99
1.00
1.00
0.0
0.3
0.6
0.9

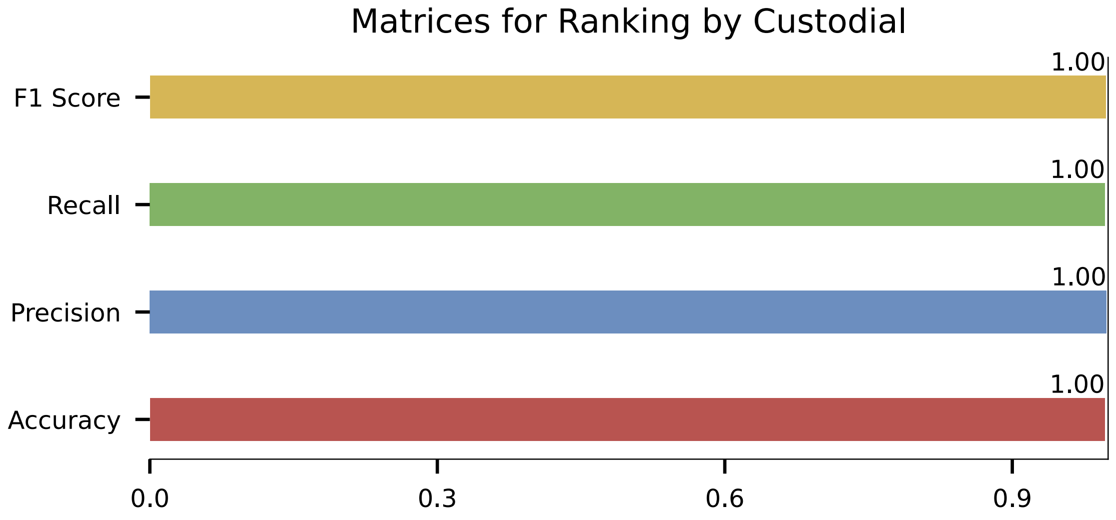
Matrices for Ranking by Multiple Cryptocurrencies

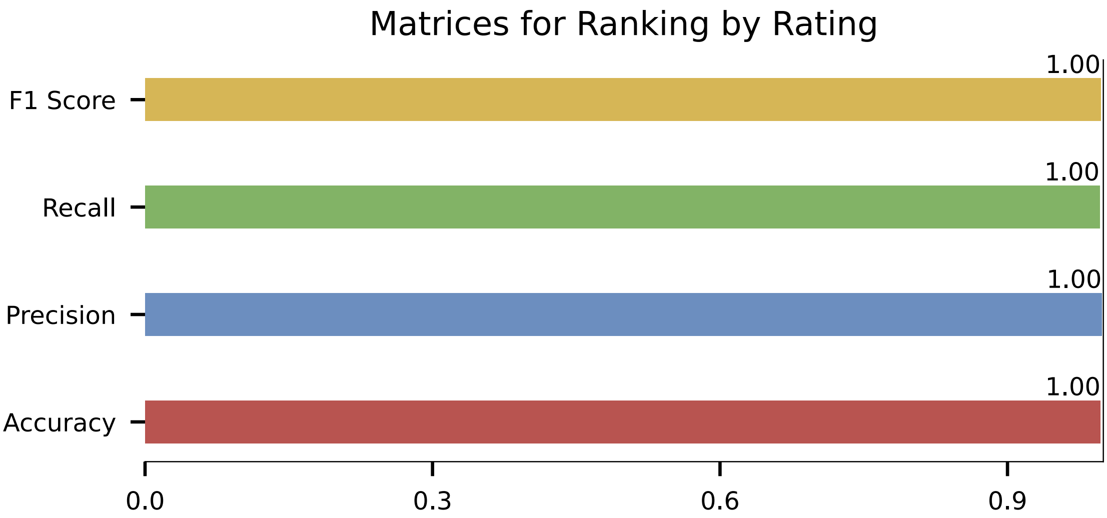


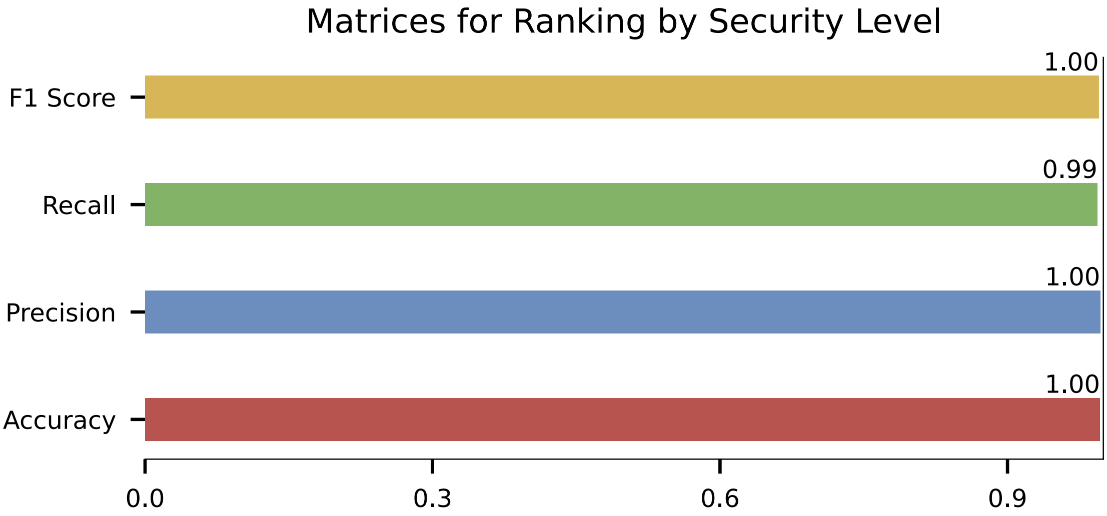
Matrices for Ranking by Wallet Age




Matrices for Ranking by Non-Custodial
F1 Score
Recall
Precision
Accuracy
0.99
0.99
1.00
1.00
0.0
0.3
0.6
0.9

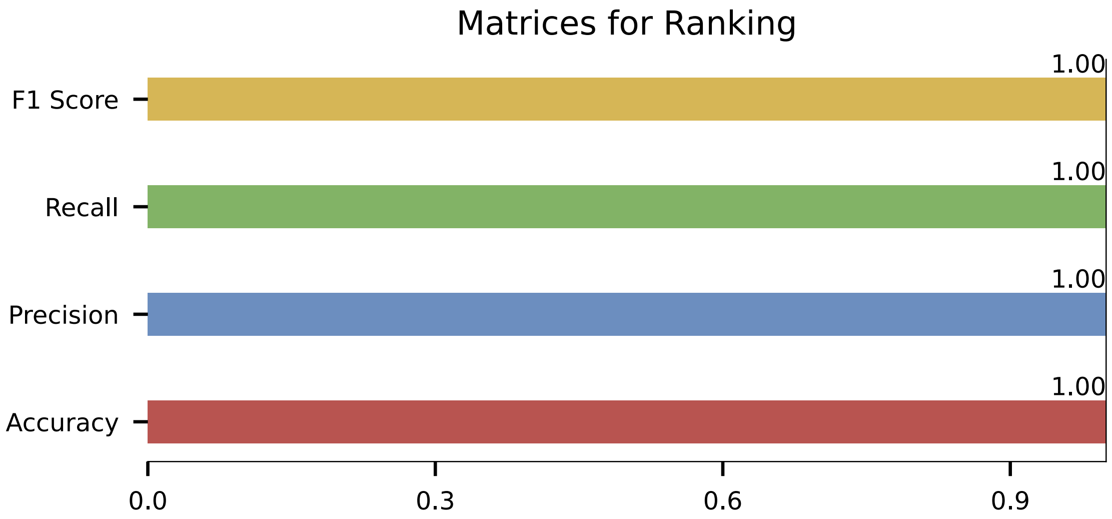

Matrices for Ranking by Custodial
F1 Score
Recall
Precision
Accuracy
1.00
1.00
1.00
1.00
0.0
0.3
0.6
0.9

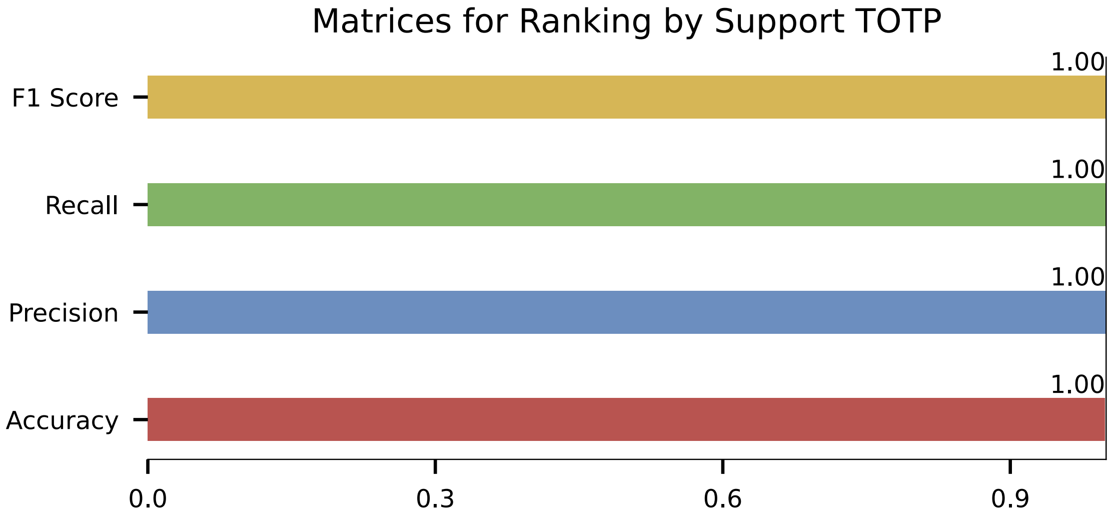

Matrices for Ranking by Rating
F1 Score
Recall
Precision
Accuracy
1.00
1.00
1.00
1.00
0.0
0.3
0.6
0.9

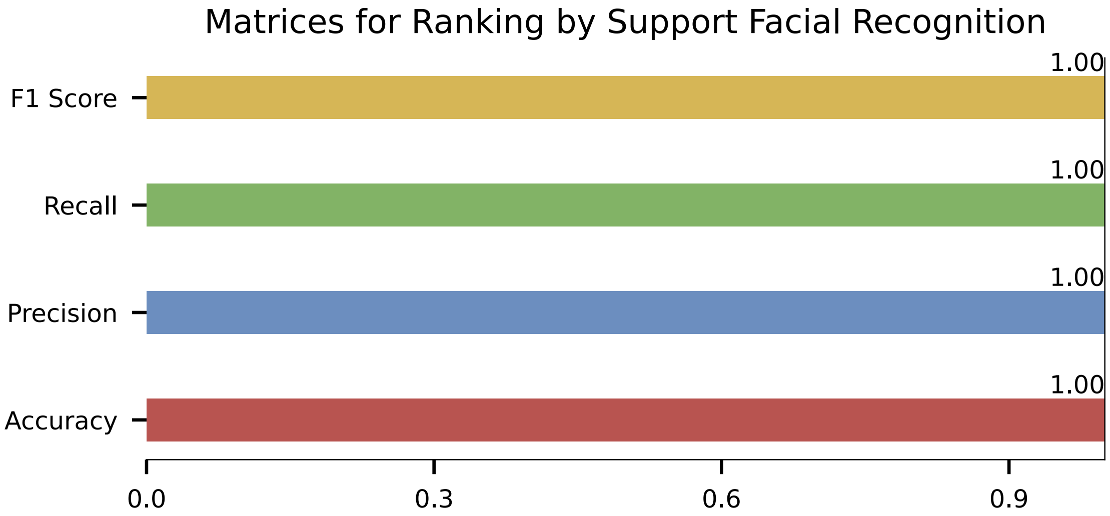

Matrices for Ranking by Security Level
F1 Score
Recall
Precision
Accuracy
1.00
0.99
1.00
1.00
0.0
0.3
0.6
0.9

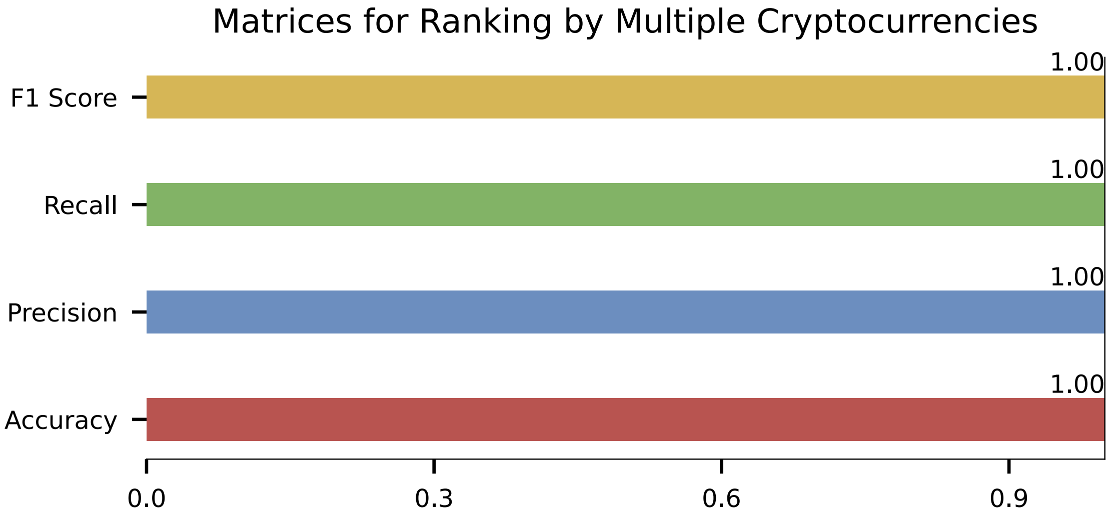
A.2 SVC model performance metrics

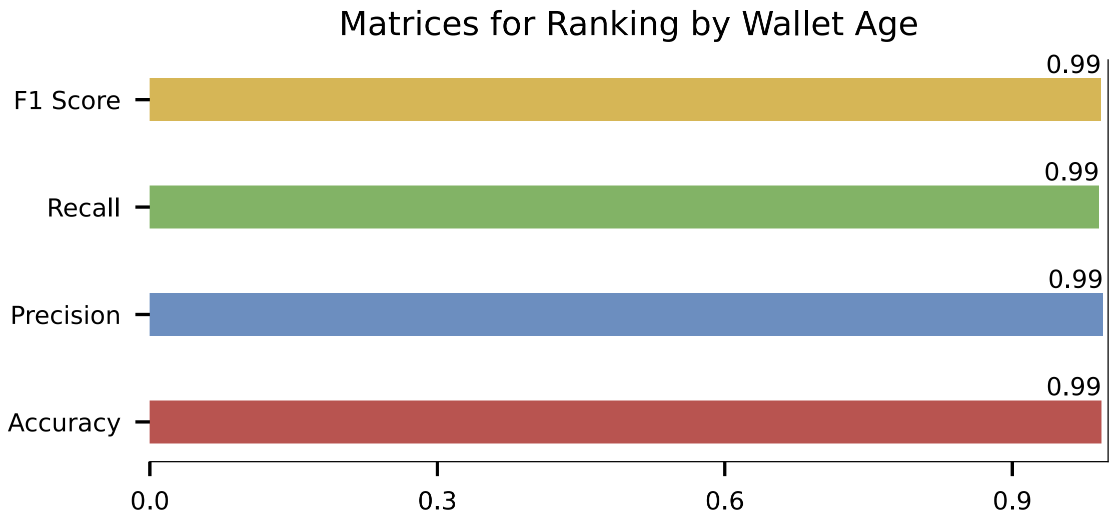
The following performance metrics relate to each output label in the SVC model.

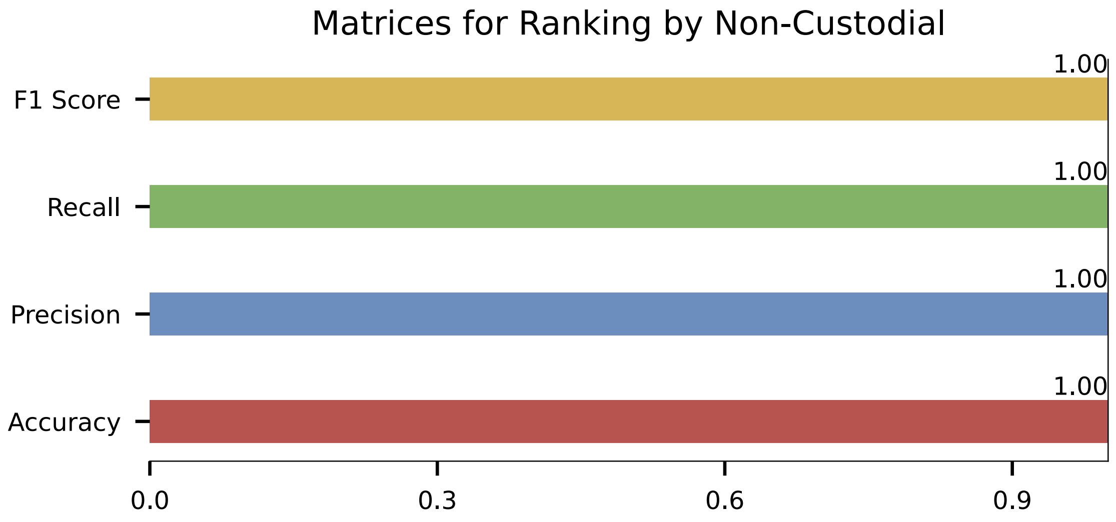


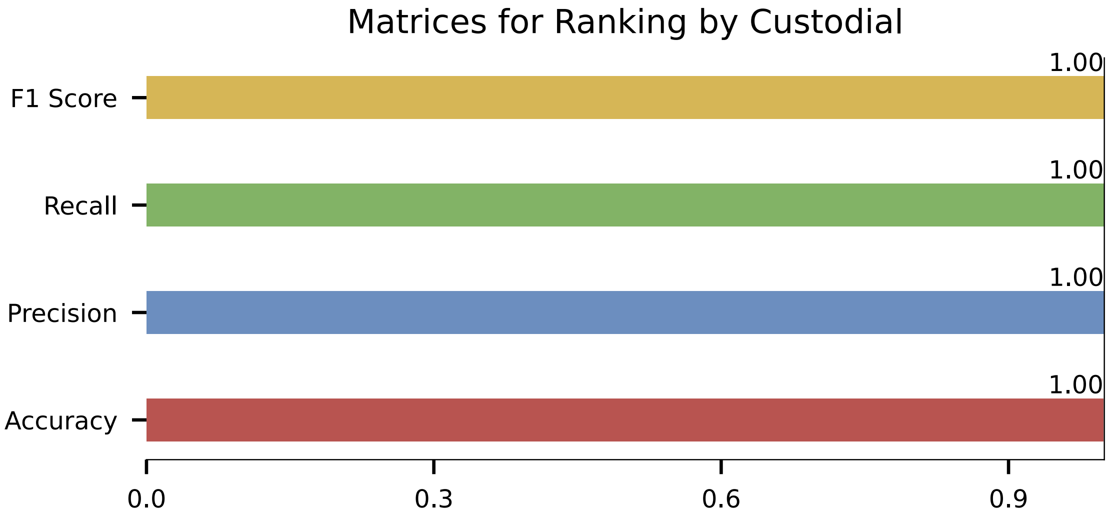


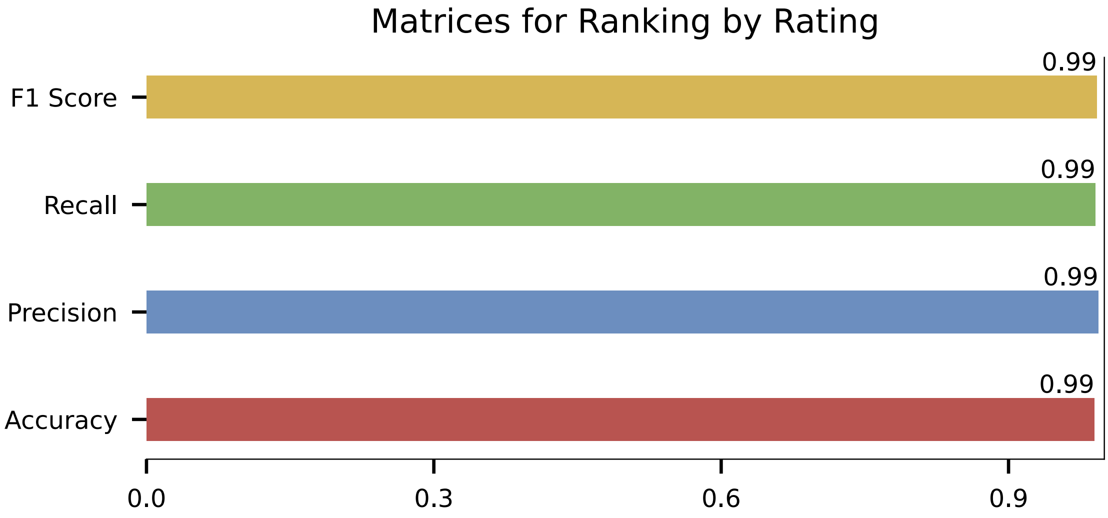

Matrices for Ranking by Support Facial Recognition
F1 Score
Recall
Precision
Accuracy
1.00
1.00
1.00
1.00
0.0
0.3
0.6
0.9

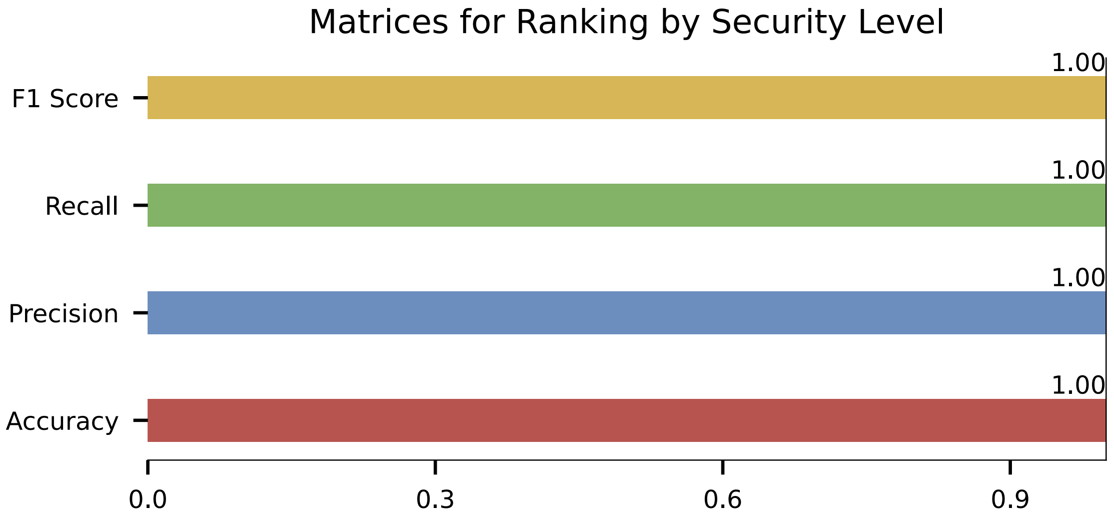

Matrices for Ranking by Multiple Cryptocurrencies
F1 Score
Recall
Precision
Accuracy
1.00
1.00
1.00
1.00
0.0
0.3
0.6
0.9


Matrices for Ranking by Wallet Age
F1 Score
Recall
Precision
Accuracy
0.99
0.99
0.99
0.99
0.0
0.3
0.6
0.9


Matrices for Ranking by Non-Custodial
F1 Score
Recall
Precision
Accuracy
1.00
1.00
1.00
1.00
0.0
0.3
0.6
0.9

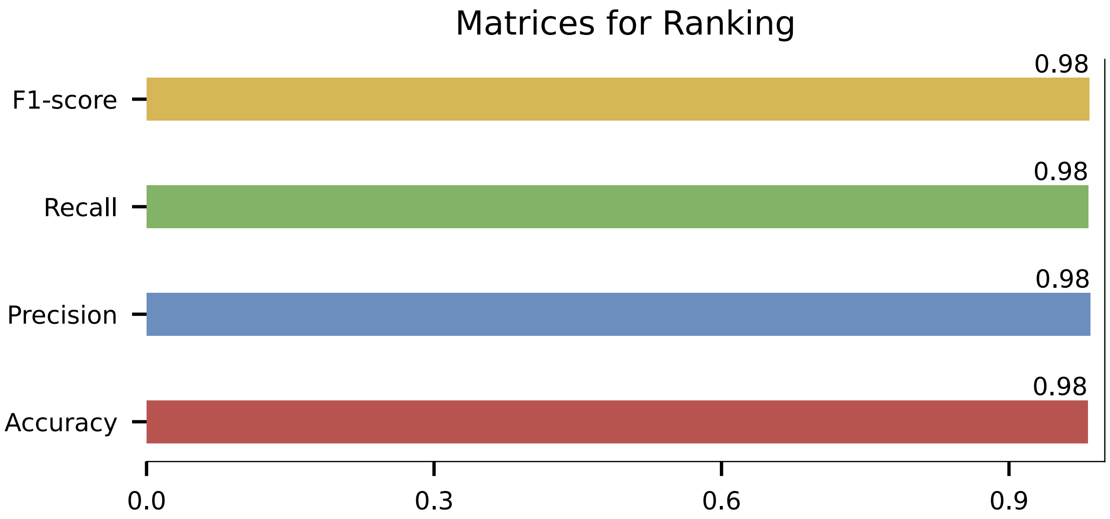

Matrices for Ranking by Custodial
F1 Score
Recall
Precision
Accuracy
1.00
1.00
1.00
1.00
0.0
0.3
0.6
0.9

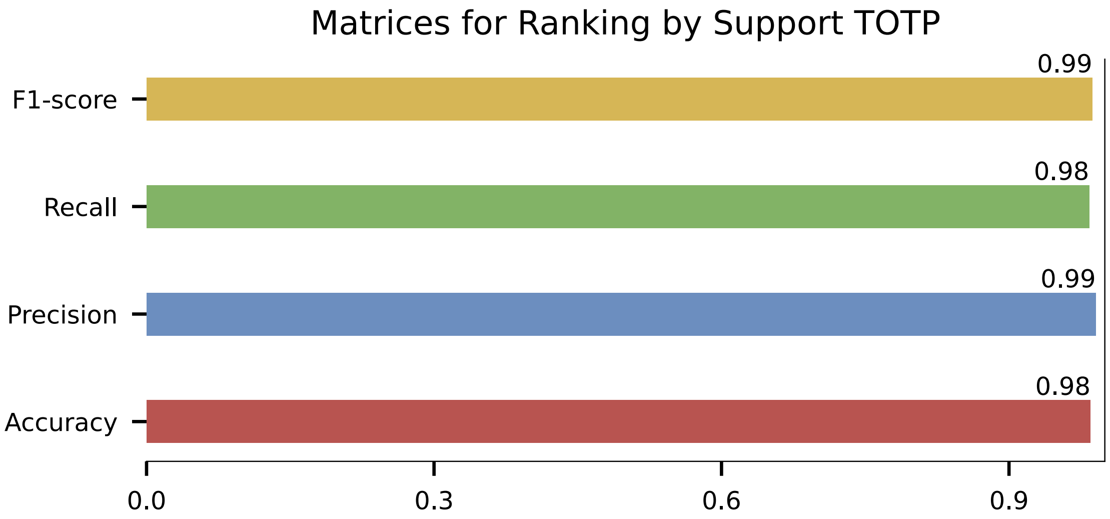

Matrices for Ranking by Rating
F1 Score
Recall
Precision
Accuracy
0.99
0.99
0.99
0.99
0.0
0.3
0.6
0.9

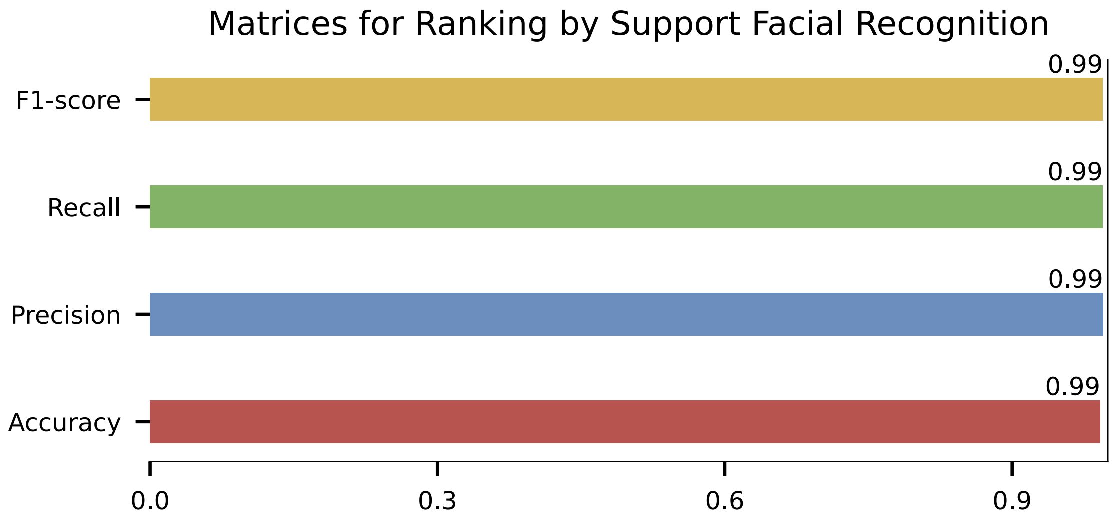

Matrices for Ranking by Security Level
F1 Score
Recall
Precision
Accuracy
1.00
1.00
1.00
1.00
0.0
0.3
0.6
0.9

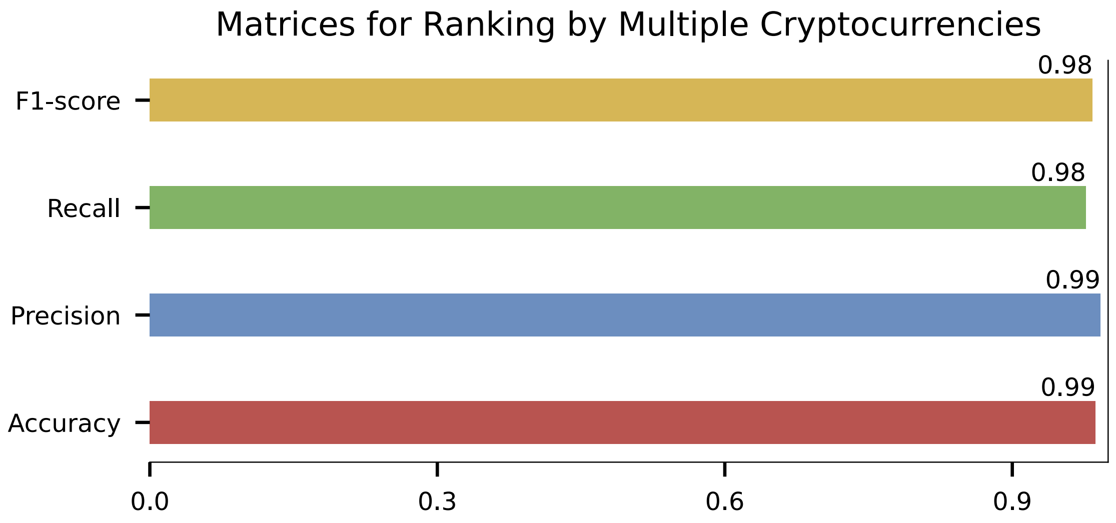
A.3 DNN model performance metrics

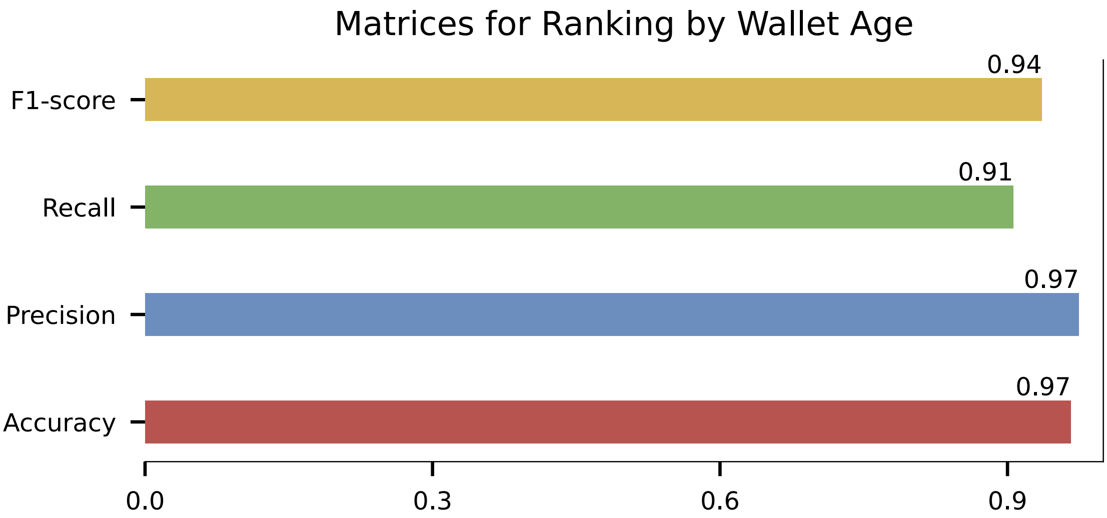
The DNN model performance metrics for each output label are shown in this section.

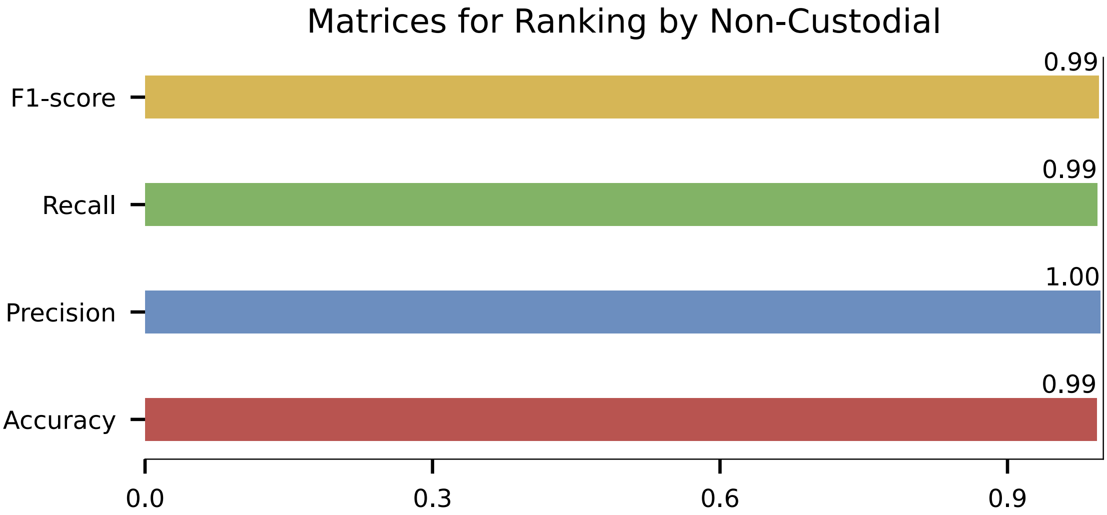


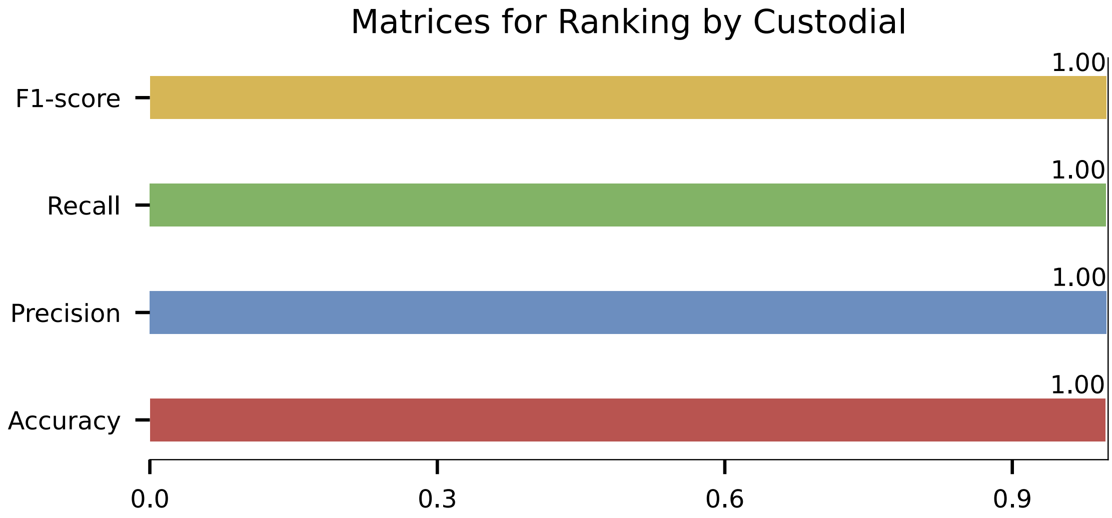


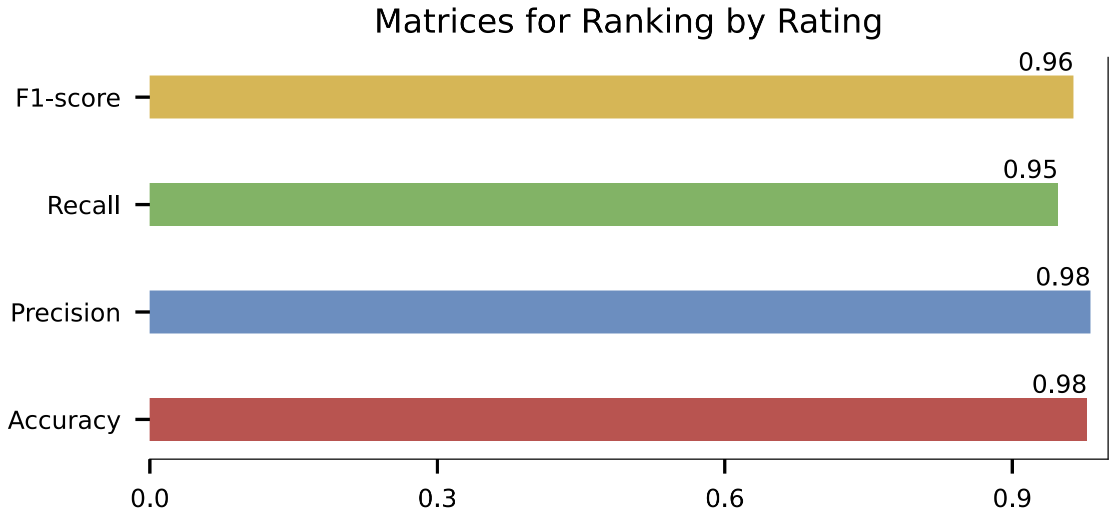

Matrices for Ranking by Support Facial Recognition
F1-score
Recall
Precision
Accuracy
0.99
0.99
0.99
0.99
0.0
0.3
0.6
0.9

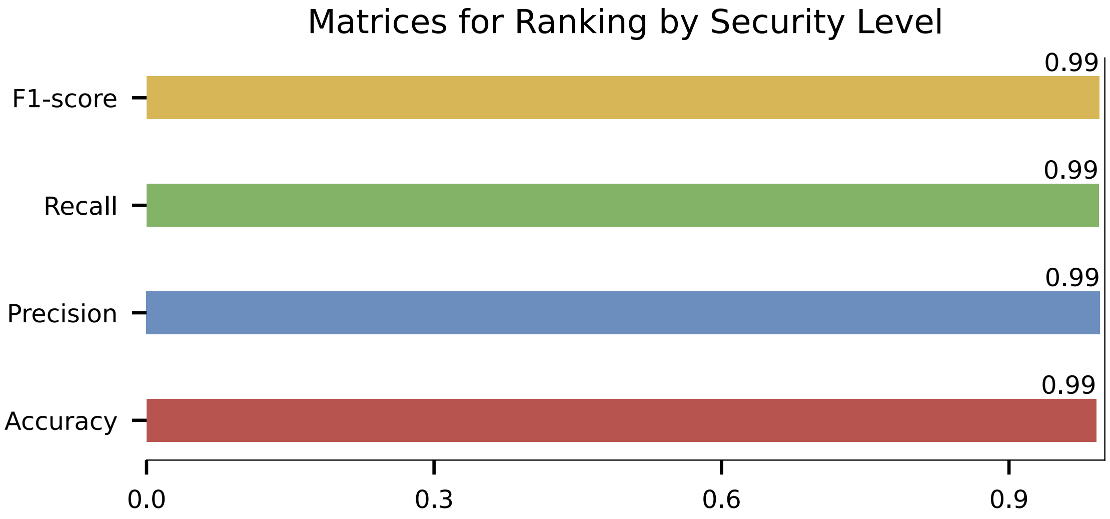

Matrices for Ranking by Multiple Cryptocurrencies
F1-score
Recall
Precision
Accuracy
0.98
0.98
0.99
0.99
0.0
0.3
0.6
0.9


Matrices for Ranking by Wallet Age
F1-score
0.94
Recall
0.91
Precision
0.97
Accuracy
0.97
0.0
0.3
0.6
0.9


Matrices for Ranking by Non-Custodial
F1-score
0.99
Recall
0.99
Precision
1.00
Accuracy
0.99
0.0
0.3
0.6
0.9


Matrices for Ranking by Custodial
F1-score
1.00
Recall
1.00
Precision
1.00
Accuracy
1.00
0.0
0.3
0.6
0.9


Matrices for Ranking by Rating
F1-score
0.96
Recall
0.95
Precision
0.98
Accuracy
0.98
0.0
0.3
0.6
0.9


Matrices for Ranking by Security Level
F1-score
Recall
Precision
Accuracy
0.99
0.99
0.99
0.99
0.0
0.3
0.6
0.9

A.4 The Codes Link

- The link to access the codes for the BWW and TBW-RAnk : https://github.com/MwAlmad/BWW_TBW-RAnk