APTISI Transactions on Technopreneurship (ATT)
Vol. 7, No. 2, July 2025, pp. 481−491
E-ISSN: 2656-8888 | P-ISSN: 2655-8807, DOI:10.34306

Enhancing Entrepreneurial Security in Cryptocurrency Wallets Using Cloud Technology

Sohel Rana[1], Rizal Mohd Nor[2*], Mohammad Enayet Hossain[3], Md Amiruzzaman[4]
[1,2]Department of Computer Science, International Islamic University Malaysia, Malaysia
[3]IIiBF, International Islamic University Malaysia, Malaysia
[4]Department of Computer Science, West Chester University, United States
[1]sohel4dev@gmail.com, [2]rizalmohdnor@iium.edu.my, [3]enayethossain26@gmail.com, [4]mamiruzzaman@wcupa.edu
***Corresponding Author**

Article Info

Article history:

Submission August 14, 2024
Revised December 6, 2024
Accepted June 24, 2025
Published July 19, 2025

Keywords:

Cryptocurrency Wallets
Cloud-based Security
Blockchain Technology
Cost Mitigation

ABSTRACT

The increasing adoption of cryptocurrency has underscored the critical need for robust security measures to protect digital assets stored in cryptocurrency wallets. Traditional security approaches have often proven inadequate in addressing the rapidly evolving threats in the digital landscape. In response, **cloud-based security solutions** have emerged as a promising method to enhance wallet protection, leveraging scalability, flexibility, and advanced security features. This study investigates the **security challenges** faced by cryptocurrency wallets and explores the potential of cloud-based solutions, focusing on multi-factor authentication, encryption protocols, real-time monitoring, and secure backup and recovery. The research assesses the **effectiveness** of these solutions in mitigating risks such as unauthorized access, data breaches, and digital asset theft. Findings reveal that cloud-based security solutions significantly improve protection by offering scalable, adaptable frameworks. However, challenges remain, including **privacy concerns, regulatory compliance**, and the **cost of implementation**. The research introduces a **cost-efficient approach** that integrates cloud-based technologies to optimize the total cost of ownership while maintaining robust security. This study also discusses the regulatory and privacy implications of cloud security in cryptocurrency ecosystems. In conclusion, this research provides **novel insights** into the integration of cloud-based security solutions, offering a comprehensive framework for safeguarding digital assets in cryptocurrency wallets. It contributes to the growing body of knowledge on the feasibility and impact of cloud technologies in enhancing the security of cryptocurrency systems.

DOI: https://doi.org/10.34306/att.v7i2.483

1. INTRODUCTION

The widespread adoption of cryptocurrency has led to a surge in the use of wallet applications for personal transactions [1]. As these wallets play a crucial role in managing cryptocurrency, they have become a prime target for malicious actors [2, 3]. The increasing variety and specifications of available wallets have made it challenging to select a secure and suitable option [4]. Furthermore, the lack of comprehensive understanding of the diverse vulnerabilities associated with these wallets exacerbates this issue [5]. It is essential to address this concern, as any vulnerability could result in the complete or partial loss of the tokens monetary value.

A blockchain functions as a distributed database, storing information in blocks that cryptography interconnects to form a chain. In simpler terms, each block serves as a container for encrypted data and comprises a block header and a block body [6]. Moreover, every block in the chain is associated with a timestamp that aids in determining the time of its addition. Blockchain blocks, once they reach their storage limit, connect to the most recent complete block to form a data chain [7]. Before inclusion in the blockchain, a block must undergo validation [8].

Blockchain technology was initially perceived as immutable and impervious to hacking [9]. This notion has persevered in both mainstream media and academic circles despite mounting evidence that blockchain, akin to traditional databases or data-sharing arrangements, is vulnerable to security breaches and cyberattacks [10]. In 2016, the Decentralized Autonomous Organization (DAO) Investments made the first significant blockchain breach [11]. Since 2011, cryptocurrency users have incurred collective losses exceeding $16 [12]. 7 billion, underscoring the paramount importance of maintaining a secure wallet [13]. This disconcerting figure accentuates the critical nature of the wallet security issue [14]. Wallet breaches and cyberattacks targeting exchanges significantly affect both individual users and communities relying on exchange services, exemplified by [15]. Gox hack that resulted in the misappropriation of nearly 850,000 cryptocurrencies [16].

During a recent incident, malevolent entities managed to abscond with a sum of USD 50 million from the Ethereum-based blockchain within a brief period [17]. We identified the root cause of the breach as the compromise of the blockchain consensus algorithms, which form the bedrock of the technology and require a predetermined proportion of network members (referred to as nodes) to validate data before its inclusion in the blockchain. The consensus mechanism of the DAO was dependent on a weighted system that bestowed greater decision-making authority upon investors with the highest stake. The perpetrator succeeded in siphoning cryptocurrency directly from the blockchain before other nodes could repudiate the unauthorized transfer as illegitimate [18].

Cryptocurrency transactions heavily rely on Hardware Security Modules (HSM) to safeguard their digital keys [19]. The HSM enables the offloading of cryptographic processes from the entire system, ensuring secure storage and facilitating the generation of key pairs [20]. However, a notable drawback is the necessity for regular algorithm updates and reconfigurations to meet evolving security standards [20]. Additionally, maintenance presents a challenge alongside the significant associated expenses [21].

The contributions of this paper are as follows:

- This study seeks to contribute to advancing sophisticated security solutions that improve the security and integrity of crypto transactions [22].
- By investigating distributed cloud-based options, the project aims to reduce the risks associated with distributed cost-effective solutions, such as single points of failure, mobility, and vulnerability to cyberattacks [23].
- This paper acknowledges that centralized methods have security concerns and limitations. It promotes a more robust and dispersed design for crypto wallet security by arguing for distributed solutions, which require a paradigm change that lessens reliance on distributed infrastructure.
- provide a thorough explanation of the subject of the security of cloud-based cryptocurrency wallets, this paper considers Amazon Web Services (AWS) as a cloud because AWS is the world most comprehensive and widely adopted cloud, offering over 200 fully featured services from data centers globally [24].

2. LITERATURE REVIEW

Cryptocurrency wallets, also referred to as crypto wallets, are essential tools for leveraging blockchain technology [25]. To participate in transactions on the blockchain platform, the possession of a crypto wallet is imperative [26]. Unlike traditional wallets designed to protect the physical currency, crypto-wallets store data for transactional purposes on the blockchain [27]. These wallets enable the establishment of an account by utilizing a pair of private and public keys, which are subsequently stored within the wallet software [28]. When initiating a transaction on the blockchain, the user must authorize the transfer of coins to the wallet address [29]. The coins can be spent by unlocking them within the wallet using the aforementioned keys [30]. It is important to note that there is no physical exchange of coins rather, the transfer of transactional data values occurs on the blockchain [31]. This characteristic renders cryptocurrency wallets more secure than traditional

currency exchanges [32]. The wallet address is denoted by an extensive string of characters produced through advanced cryptography techniques [33]. Figure 1 shows the Crypto Wallet model.

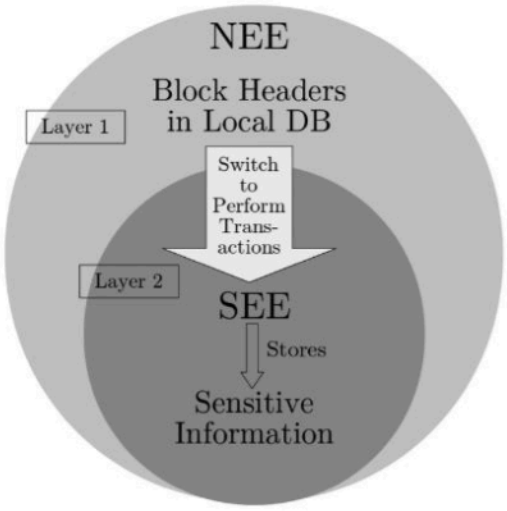

Figure 1. Crypto Wallet Model Based on TrustZone Scheme

Cryptocurrency systems utilize a blockchain database to store and maintain their state [34]. This state encompasses not only user data but also token balances [35]. Users append data structures, or transactions, to the blockchain to modify their data and initiate transactions involving their funds [36]. Users must provide proof of their identity to verify their authenticity as part of the transaction process [37].

2.1. Development of cryptocurrency wallets

The utilization of cryptocurrencies possesses the potential to significantly reshape the framework of our global monetary system, offering enticing attributes that could establish a secure and resilient environment for financial transactions [38]. While the existing system undoubtedly has scope for enhancement, some proponents assert that reinforcing its fundamental structure remains the sole essential measure [39]. Any duly authorized local intermediary can record a transaction in the distributed ledger and expedite it within the blockchain [40]. The Hot-Cold Hybrid Decentralized Exchange (HCH DEX) obviates the necessity for a centralized server system or common database to process transactions between two individual devices storing cryptocurrency wallet data [41]. Furthermore, a sleek smart card, considerably slimmer than current cards, could implement the proposed configuration [42]. E-Wallets and lightweight DLT nodes collaborate as local facilitators through a secure two-way authentication mechanism, permitting robust handshaking procedures [43]. It could be contended that this represents a foundational move towards an equitable economic structure capable of withstanding duplicitous and unethical practices across all strata [44].

Table 1. Evolution of the Crypto Wallet (Source: [17, 19]).

The First Ever Crypto Wallet	Satoshi Nakamoto designed the first cryptocurrency wallet for Bitcoin (BTC). Users had to download the entire Bitcoin blockchain history before using the wallet. Vitalik Buterin emphasized the need for the cryptocurrency wallet to be operational at all times by 2012 to keep up with the growing Bitcoin data.
The First Mobile BTC Wallet	In 2011, Electrum created the first Bitcoin wallet software for Android, aiming to simplify managing BTC on the go. Third-party wallet services have since emerged, offering alternative options with more user-friendly interfaces and extra capabilities to diversify the ecosystem of Bitcoin wallets.
Hardware Wallets	In 2014, the first Bitcoin cold wallets, made of hardware, entered the market. Trezor was one of the first hardware wallets.

Mult signature Cryptocurrency Wallets	A multi-signature cryptocurrency wallet requires multiple signatures to authorize a transaction. It involves multiple parties or private keys working together to verify and approve transactions, making it ideal for storing Bitcoin when more than one person or entity needs access. Examples include Armory, Guarda Wallet, and Linen Wallet.
Ethereum Wallet Enters the Scene	The wallet ecosystem for Ether (ETH) was introduced in 2016. An Ethereum wallet allows users to store and access digital assets developed in the Ethereum ecosystem. More than fifty Ethereum wallets, including Rabby Wallet and Portis, are available to consumers.
Token Wallets	The crypto sector has evolved over the years, leading to the development of wallets that can accommodate multiple currencies from various blockchains. Recently, Coinbase released a self-custody wallet for iOS, and Robinhood launched a Polygon-based wallet for Android and Windows.
The Crypto Wallets of 2023	In 2023, popular types of crypto wallets included hardware wallets, software wallets (or hot wallets), and paper wallets.

The emergence of cryptocurrency has presented unprecedented opportunities for the global monetary framework [45]. Throughout history, the practice of trading precious metals, such as gold and silver, has been one of humanity most enduring and reliable investment methods [46]. Nonetheless, the transition from tangible assets to paper and later digital currencies was driven by the limitations of physical mediums initially, the intrinsic link to real-world resources positioned these currencies as favorable options for trade [47, 48]. However, as the financial landscape evolved, inherent vulnerabilities surfaced, such as the potential for previously unavailable commodity trading [49]. While technology undoubtedly simplifies various processes, it also can endorse contentious activities and engender ethical dilemmas. Cryptocurrencies appear to amalgamate the favorable characteristics of digital currency with the principles underlying precious metal transactions. Analogous to precious metals, the value of cryptocurrencies is contingent on supply and demand dynamics, wherein the resources and exertion required for their acquisition profoundly impact their valuation [50, 51].

In 1983, David Chaum established e-Cash, an innovative platform that facilitated anonymous online money transactions (From Table 1). Although Chaum creation of Digicash in 1989 initially showed limited success, it was not until the mid-1990s that the project gained momentum. The eCash model fostered partnerships with several smaller financial institutions, including Deutsche Bank and Mark Twain Bank. The term ”cryptocurrency” was formally coined in 1998, the same year Digicash filed for bankruptcy. During this time, Wei Dai championed B-money, a concept emphasizing decentralization in cryptocurrency. The 2008 financial crisis disrupted the traditional financial sector, eroding faith in banks and conventional currencies. At that point, Bitcoin stood alone as the only recognized cryptocurrency. While Bitcoin is not the sole digital currency in existence, it has spearheaded the popularization of cryptocurrencies. Satoshi Nakamoto, an enigmatic figure, introduced Bitcoin, aiming to showcase the viability of alternative currencies that could facilitate global, decentralized transactions independent of traditional financial institutions. Although initially met with skepticism, Nakamoto vision appears to have stood the test of time.

2.2. Overview of cloud computing

Cloud computing, which began in the 1960s for mainframe computers, has evolved into an interconnected system of computer networks. It combines various computing, software, and storage resources to create a shared virtual resource pool for customers. This technology improves service utilization and reduces costs. However, despite its effective management, cloud computing presents vulnerabilities, including IT risks related to storage and potential asset loss. Security concerns over sensitive technological assets contribute to assessing monetary risks, and risk management involves identifying, assessing, and controlling these threats. As the cloud computing model expands, companies are increasingly transitioning to it.

According to the National Institute of Standards and Technology (NIST), Cloud Computing is a model that enables the convenient provisioning and access of a shared pool of configurable computing resources including applications, storage, networks, and servers. This model allows users to access these resources from anywhere at any time with minimal involvement from the service provider. The key merits of cloud computing

are its availability, scalability, and management, along with qualities such as affordability, accessibility, multi-tenancy, stability, flexibility, and on-demand service. This comprehensive overview serves as an essential reference for understanding the fundamental and distinctive aspects of cloud computing.

2.3. Cloud-based crypto security

The implementation of security systems enforces policies through security services. Elastica Q2 2015 and the CSA examine cloud application security engineering, which provides control, visibility, and remediation. The ISO emphasizes data security in technological solutions, particularly cloud computing. Outsourcing data and software to the cloud shifts control to the service provider, making trust dependent on their execution methodology. There are five types of security attacks:

- Memory and storage
- Operating system
- Software layer
- Network layer
- Blockchain protocol

Each category has further subdivisions into attacker models based on assumptions and conditions in the literature, with distinct objectives or common purposes.

3. PROTOTYPE DESIGN

The Cryptocurrency wallet involves integrating various blockchain-specific components essential for its core functionalities. This encompasses provisioning and managing blockchain nodes, implementing robust private key management systems, developing efficient transaction handling modules, and navigating intricate blockchain data architectures. The complexity of these components necessitates advanced security protocols and meticulous infrastructure management.

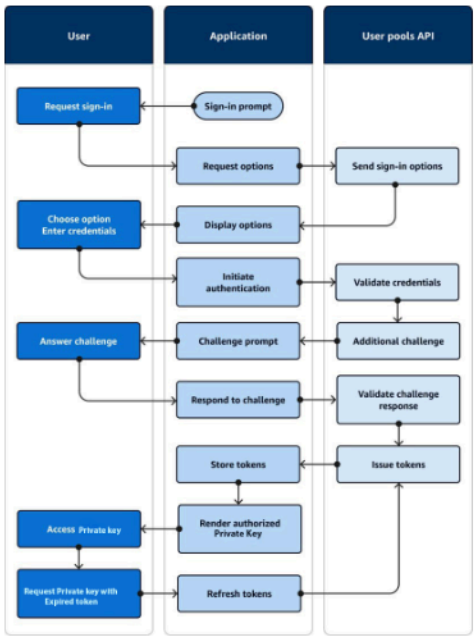

Figure 2. Procedure to User Log in to Our Crypto Wallet

Figure 2 depicts a typical situation in which a user logs into an application. The sample application offers the user many sign-in alternatives. They choose one by inputting their credentials, supplying an extra authentication factor, and logging in.

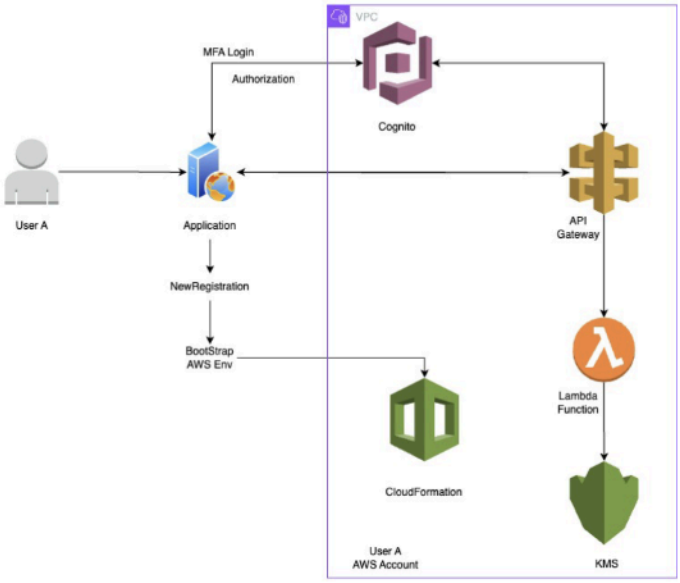

Figure 3. Cloud-Based Model for the Cryptocurrency Wallet

As Blockchain technology and cryptocurrencies gain popularity, the need for secure devices that facilitate operations in reliable cryptocurrency wallets has become more critical. A digital wallet that stores, manages, and grants access to one cryptocurrency assets over the Internet is known as a cloud-based cryptocurrency wallet (Show on Figure 3). A cloud-based crypto wallet stores its currency on a distant server. Nowadays, many companies provide cloud computing services, such as AWS, GCP, and Microsoft. Any device with an internet connection, including smartphones, tablets, and PCs, can access it. This makes it possible for users to manage their cryptocurrency holdings from any location without the need for any special hardware or software installation. For new users or those who want quick and straightforward access to their money, cloud-based wallets are a beneficial option because they emphasize user experience and accessibility. Cloud-based wallets often include security features with Multi-Factor Authentication (MFA), such as biometric logins, Two-Factor Authentication (2FA), and other forms of identification verification to prevent illegal access. Most online wallets include a way to back up and restore money in the event that the user loses their private key. This backup and recovery feature may employ mnemonic phrases or encrypted keys. While user data remains safe, this makes account recovery easy. Figure 3 illustrates the proposed Cloud-Based Model for the Cryptocurrency Wallet. This model stores private data in the cloud without compromising security. It saves a lot of costs compared to HSM, where the user should be verified through the AWS Cognito with multifactor authentication. Using the AWS lambda function, the security key will be retrieved from KMS.

3.1. Key Components of Secure Private Key

- Cognito serves as an identity platform designed for both web and mobile applications. It functions as a user directory, an authentication server, and an authorization service for OAuth 2.0 access tokens and credentials. Establish a user pool when you need to authenticate and permit users to access your application or API. User pools act as a directory that allows for both self-service and administrator-managed user creation, management, and authentication. Your user pool can operate as a standalone directory and OIDC Identity Provider (IdP), as well as an intermediary Service Provider (SP) for external workforce and customer identity providers. You can implement Single Sign-On (SSO) within your application for your organization workforce identities using SAML 2.0 and OIDC IdPs through user pools. Additionally, you can provide SSO capabilities in your app for your organization customer identities via the public OAuth 2.0 identity providers such as Amazon, Google, Apple, and Facebook.

- The API Gateway functions as the primary entry point for facilitating communication between the front-end and back-end systems. It is responsible for managing and routing API requests, enforcing security policies, and executing load balancing to accommodate high levels of user traffic. The API Gateway is

crucial for ensuring seamless interactions and enabling secure and efficient data flow. Figure 4 illustrates the API Gateway.

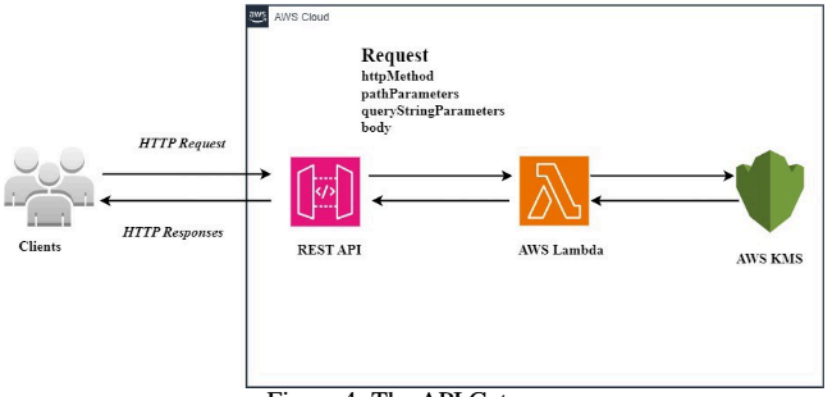

Figure 4. The API Gateway

- Lambda Functions AWS Lambda function constitutes a segment of code that executes in response to specific events and is autonomously managed by AWS Lambda. AWS Lambda serves as a serverless computing service, enabling users to run code without the necessity of managing or provisioning servers. It empowers users to execute code without the burdens of server provisioning or management, developing workload-aware cluster scaling mechanics, maintaining event integrations, or overseeing runtimes. By integrating AWS Lambda with other AWS services, developers are capable of constructing sophisticated web applications that automatically scale according to demand and operate in a highly available configuration across multiple data centers. This integration requires no administrative effort for scalability, backups, or redundancy in various data centers.

4. MANAGERIAL IMPLICATIONS

The findings of this study present several managerial implications for organizations adopting cloud-based security solutions, particularly in the context of cryptocurrency wallets.

4.1. Enhanced Security Measures

Managers should prioritize integrating advanced cloud-based security solutions, such as multi-factor authentication, real-time monitoring, and encryption protocols, to safeguard sensitive data in cryptocurrency wallets. This will help mitigate the risk of cyber-attacks and breaches, which can significantly impact financial stability.

4.2. Cost-Efficient Security Solutions

Cloud-based security solutions offer scalability and flexibility, which can reduce operational costs compared to traditional security models like HSM. Managers should consider the financial benefits of adopting cloud computing services, ensuring they balance security needs with cost-effective strategies.

4.3. Trust and Vendor Management

Since cloud-based services transfer control to the service provider, it is critical for managers to carefully evaluate and choose reliable cloud vendors. Ensuring that cloud providers meet security and compliance standards will help mitigate risks associated with data breaches and privacy concerns.

4.4. Ongoing Training and Awareness

As cloud computing continues to evolve, it is essential for organizations to invest in ongoing training for their staff. Employees should be educated on potential risks, secure practices for managing digital assets, and the use of cloud-based systems to reduce human error and ensure robust security.

4.5. Regulatory and Compliance Considerations

With the integration of cloud-based security solutions, managers must stay informed of evolving regulatory requirements in their region or industry. Ensuring compliance with data protection laws and cybersecurity regulations will protect organizations from legal liabilities and reputational damage.

4.6. Scalability and Future-Proofing

Managers should recognize the scalability of cloud-based security solutions, which can grow alongside the organization needs. This adaptability is particularly important in rapidly evolving sectors like cryptocurrency, where emerging threats require flexible and upgradable security measures.

5. CONCLUSION

This research reveals a significant gap between available security measures and their practical application in cryptocurrency wallets. The study proposes a cloud-based solution for enhancing wallet security through multi-factor authentication, encryption protocols, and other cloud technologies. By addressing vulnerabilities such as data breaches and unauthorized access, the proposed security model offers robust protection for digital assets. Despite its promising potential, scalability challenges, such as the limited key storage capacity of HSM, need to be resolved to enhance the overall effectiveness of the security solutions.

Future studies should explore scalable solutions to overcome the limitations of HSMs, particularly in key management. For example, developing a master key using HSM technology to encrypt sensitive wallet information like Ethereum seed phrases could be an area for deeper investigation. Further research could also focus on integrating more advanced technologies such as machine learning or FPGA designs to improve wallet security and address evolving cybersecurity threats. Additionally, there is a need for studies examining the regulatory implications of using cloud-based solutions for wallet security, especially in relation to data privacy and compliance with global standards.

The findings of this research have significant managerial implications for organizations in the cryptocurrency space. First, integrating cloud-based security solutions can offer a cost-effective way to safeguard user wallets while mitigating the risk of cyber-attacks. Managers should prioritize vendor trust and compliance when selecting cloud service providers to ensure robust security measures. Additionally, user education and awareness play a critical role in enhancing security at the individual level, as users must understand the security features of the exchanges they use. Lastly, the adoption of the proposed security model can help organizations optimize their security infrastructure and minimize exposure to digital threats, fostering greater trust and stability in the cryptocurrency ecosystem.

6. DECLARATIONS

6.1. About Authors

Sohel Rana (SR) https://orcid.org/0009-0003-1099-9276

Rizal Mohd Nor (MN) https://orcid.org/0000-0002-8994-2234

Mohammad Enayet Hossain (EH) https://orcid.org/0000-0001-6499-0566

Md Amiruzzaman (MA) https://orcid.org/0000-0002-2292-5798

6.2. Author Contributions

Conceptualization: MN; Methodology: SR; Software: SR; Validation: SR and MN; Formal Analysis: SR and MN; Investigation: SR; Resources: SR; Data Curation: SR; Writing Original Draft Preparation: SR, MN and EH; Writing Review and Editing: EH and MA; Visualization: SR; All authors, SR, MN, EH, and MA, have read and agreed to the published version of the manuscript.

6.3. Data Availability Statement

The data presented in this study are available on request from the corresponding author.

6.4. Funding

The authors received no financial support for the research, authorship, and/or publication of this article.

6.5. Declaration of Conflicting Interest

The authors declare that they have no conflicts of interest, known competing financial interests, or personal relationships that could have influenced the work reported in this paper.

REFERENCES

[1] 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.

[2] S. Geetha, R. Naveenkumaran, K. Selvaraju, C. Kishore, and A. N. Rathish, "Blockchain based mechanism for cloud security," in *2023 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS)*. IEEE, 2023, pp. 1287–1295.

[3] V. T. Truong, L. Le, and D. Niyato, "Blockchain meets metaverse and digital asset management: A comprehensive survey," *Ieee Access*, vol. 11, pp. 26 258–26 288, 2023.

[4] R. Indumathi, P. Mathivanan, D. Mohanapriya, and M. Sangeetha, "Quantum ai, cybersecurity, and their impact on bitcoin, cryptocurrency, and blockchain-based financial systems," in *Quantum AI and its Applications in Blockchain Technology*. IGI Global Scientific Publishing, 2025, pp. 75–110.

[5] S. Singh, A. S. Hosen, and B. Yoon, "Blockchain security attacks, challenges, and solutions for the future distributed iot network," *Ieee Access*, vol. 9, pp. 13 938–13 959, 2021.

[6] 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.

[7] A. Nuche, O. Sy, and J. C. Rodriguez, "Optimizing efficiency through sustainable strategies: The role of management and monitoring in achieving goals," *APTISI Transactions on Management*, vol. 8, no. 2, pp. 167–174, 2024.

[8] I. Eyal, "On cryptocurrency wallet design," in *3rd International Conference on Blockchain Economics, Security and Protocols (Tokenomics 2021)*. Schloss-Dagstuhl-Leibniz Zentrum für Informatik, 2022.

[9] A. A. Mohammed, A. M. S. Rahma, and H. B. Abdul Wahab, "Transformative innovations in digital currency and e-wallet systems: A comprehensive exploration of security, scalability, and adoption," in *AIP Conference Proceedings*, vol. 3207, no. 1. AIP Publishing, 2024.

[10] Kaspersky.com, "What is Cryptocurrency and How Does it Work?" https://www.kaspersky.com/resource-center/definitions/what-is-cryptocurrency, 2024, online; accessed 15 December 2024.

[11] T. Fareed, "A systemic review of payment technologies with a special focus on digital wallets," *Financial Technologies and DeFi: A Revisit to the Digital Finance Revolution*, pp. 89–97, 2023.

[12] V. Raja *et al.*, "Exploring challenges and solutions in cloud computing: A review of data security and privacy concerns," *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, vol. 4, no. 1, pp. 121–144, 2024.

[13] D. S. S. Wuisan, R. A. Sunardjo, Q. Aini, N. A. Yusuf, and U. Rahardja, "Integrating artificial intelligence in human resource management: A smartpls approach for entrepreneurial success," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 5, no. 3, pp. 334–345, 2023.

[14] J. Prakash, "Cryptocurrency a digital wallet: Pro's and con's," *Int. J. Multidiscip. Educ. Res*, vol. 11, no. 9, pp. 65–68, 2022.

[15] K. Mavrou, S. Symeonidou, and M. Tsakiri, "Once inclusive always inclusive (?): experiences of cypriot teachers and parents of children with disabilities on the use of technology and collaboration before and during the covid-19 pandemic," *International Journal of Inclusive Education*, pp. 1–17, 2024.

[16] A. T. Olutimehin, "The synergistic role of machine learning, deep learning, and reinforcement learning in strengthening cyber security measures for crypto currency platforms," *Deep Learning, and Reinforcement Learning in Strengthening Cyber Security Measures for Crypto Currency Platforms (February 11, 2025)*, 2025.

[17] I. Mavrou, "The Evolution of Crypto Wallets: Exploring The History and Future of Secure Storage," https://www.techopedia.com/the-evolution-of-crypto-wallets-exploring-the-history-and-future-of-secure-storage, 2023, online; accessed 15 December 2024.

[18] I. Maria *et al.*, "Unlocking success: Human resource management for startupreneur," *Startupreneur Business Digital (SABDA Journal)*, vol. 3, no. 1, pp. 89–97, 2024.

[19] Crypto Fundamentals, MEXC Creators, "The History and Evolution of Crypto Wallets," https://blog.

mexc.com/the-history-and-evolution-of-crypto-wallets-creator-obed/, 2024, online; accessed 15 December 2024.

[20] 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.

[21] I. Homoliak and M. Perešíni, "Sok: Cryptocurrency wallets–a security review and classification based on authentication factors," in *2024 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*. IEEE, 2024, pp. 1–8.

[22] Kementerian Pendidikan, Kebudayaan, Riset, dan Teknologi, "Kemendikbudristek pastikan keamanan data pendidikan indonesia," 2023, accessed: 2025-06-30. [Online]. Available: https://www.kemendikdasmen.go.id/berita/4932-kemendikbudristek-pastikan-keamanan-data-pendidikan-indonesia

[23] N. M. Shivale, P. Mahalle, G. M. Bhandari, S. Patil, U. Gaikwad, S. Thaware, S. Tamboli, S. Pawale, and V. D. Sonawane, "Detailed review on enabling secure and seamless crypto wallet: A blockchain solution," *Cureus Journals*, vol. 2, no. 1, 2025.

[24] J. Limdrian, M. N. M. Thorif, R. Fredyan, and M. A. Ibrahim, "Exploring security in cryptocurrency: Challenges, solutions, and implications–a systematic literature review," in *2024 International Conference on ICT for Smart Society (ICISS)*. IEEE, 2024, pp. 1–9.

[25] P. Weichbroth, K. Wereszko, H. Anacka, and J. Kowal, "Security of cryptocurrencies: A view on the state-of-the-art research and current developments," *Sensors*, vol. 23, no. 6, p. 3155, 2023.

[26] H. M. Varghese, D. A. Nagoree, N. Jayapandian *et al.*, "Cryptocurrency security and privacy issues: A research perspective," in *2021 6th International Conference on Communication and Electronics Systems (ICCES)*. IEEE, 2021, pp. 902–907.

[27] N. A. VA and D. Bindhu, "The swoc factors influencing cryptocurrency wallets: A comprehensive study of their strengths, weaknesses, opportunities, and challenges," *HR Connect*, vol. 1, no. 6, pp. 39–46, 2024.

[28] T. Navamani, "A review on cryptocurrencies security," *Journal of Applied Security Research*, vol. 18, no. 1, pp. 49–69, 2023.

[29] O. Hämäläinen, "Analyzing usability issues in self-custody cryptocurrency wallets with jakob nielsen's 10 usability heuristics," *Aalto University School of Business*, 2023.

[30] S. Bhujel and Y. Rahulamathavan, "A survey: Security, transparency, and scalability issues of nft's and its marketplaces," *Sensors*, vol. 22, no. 22, p. 8833, 2022.

[31] J. Velani and D. S. Patel, "A review: Fraud prospects in cryptocurrency investment," *International Journal of Innovative Science and Modern Engineering*, vol. 11, no. 6, pp. 1–4, 2023.

[32] A. Vaidya, "Emerging technologies and cyber security," *India Banking and Finance Report*, vol. 145, 2023.

[33] S. I. Al-Hawary, J. R. N. Alvarez, A. Ali, A. K. Tripathi, U. Rahardja, I. H. Al-Kharsan, R. M. Romero-Parra, H. A. Marhoon, V. John, and W. Hussian, "Multiobjective optimization of a hybrid electricity generation system based on waste energy of internal combustion engine and solar system for sustainable environment," *Chemosphere*, vol. 336, p. 139269, 2023.

[34] P. Golait, D. S. Tomar, R. Pateriya, and Y. K. Sharma, "Blockchain security and challenges: A review," in *2023 IEEE 2nd International Conference on Industrial Electronics: Developments & Applications (ICIDeA)*. IEEE, 2023, pp. 140–145.

[35] R. Raheja, P. C. Pathak, and S. A. Ansar, "Major security risks and its alleviating techniques: Blockchain web application perspectives," in *2024 7th International Conference on Contemporary Computing and Informatics (IC3I)*, vol. 7. IEEE, 2024, pp. 572–577.

[36] V. Rattanawiboonsom and N. Khan, "Blockchain technology in mobile payments: A systematic review of security enhancements in mobile commerce." *International Journal of Interactive Mobile Technologies*, vol. 18, no. 21, 2024.

[37] A. A. Almamoori and W. S. Bhaya, "Survey on cryptocurrency security attacks and detection mechanisms," *Bulletin of Electrical Engineering and Informatics*, vol. 12, no. 6, pp. 3638–3646, 2023.

[38] Z. Liu and X. Li, "Sok: Security analysis of blockchain-based cryptocurrency," *arXiv preprint arXiv:2503.22156*, 2025.

[39] V. P. Dangcalan, J. D. V. Barbadillo, G. E. Bueno, C. S. Santiago Jr, and Z. J. R. Centeno, "Decentralized finance (defi) wallets: A review of its efficiency, usability," in *Innovations in Information and Decision Sciences: Proceedings of the 12th International Conference on Frontiers in Intelligent Computing: Theory and Applications (FICTA 2024)*, vol. 422. Springer Nature, 2025, p. 237.

[40] Kementerian Pendidikan, Kebudayaan, Riset, dan Teknologi, "Kajian budaya politik dan keamanan siber mahasiswa indonesia," 2023, accessed: 2025-06-30. [Online]. Available: https://www.kemendikdasmen.go.id/berita/3836-kajian-budaya-politik-dan-keamanan-siber-mahasiswa-indonesia

[41] M. Buhler, "Enhancing multi-signature cryptocurrency wallets with risk-based authentication," *PRISM Repository*, 2025.

[42] S. Lestari, S. Watini, and D. E. Rose, "Impact of self-efficacy and work discipline on employee performance in sociopreneur initiatives," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 6, no. 2, pp. 270–284, 2024.

[43] S. Prabanand and M. Thanabal, "Advanced financial security system using smart contract in private ethereum consortium blockchain with hybrid optimization strategy," *Scientific Reports*, vol. 15, no. 1, p. 6764, 2025.

[44] K. K. Singamaneni, A. K. Budati, S. Islam, R. Kolandaisamy, and G. Muhammad, "A novel hybrid quantum-crypto standard to enhance security and resilience in 6g enabled iot networks," *IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing*, 2025.

[45] V. Walunj, V. Rajaraman, J. Dutta, and A. Sharma, "Integrating crypto-based payment systems for data marketplaces: Enhancing efficiency, security, and user autonomy," in *International Conference on Information Systems Security*. Springer, 2025, pp. 443–452.

[46] M. M. Shabir, K. Zhang, B. Reulet, and G. Gagnon, "Qaas: hybrid cryptocurrency wallet-as-a-service based on quantum rng," *Cluster Computing*, vol. 28, no. 3, p. 180, 2025.

[47] D. E. Rose, J. Van Der Merwe, and J. Jones, "Digital marketing strategy in enhancing brand awareness and profitability of e-commerce companies," *APTISI Transactions on Management*, vol. 8, no. 2, pp. 160–166, 2024.

[48] J. Rosa-Bilbao, J. Boubeta-Puig, J. Lagares-Galán, and M. Vella, "Leveraging complex event processing for monitoring and automatically detecting anomalies in ethereum-based blockchain networks," *Computer Standards & Interfaces*, vol. 91, p. 103882, 2025.

[49] V. V. Krasinsky, A. N. Norkina, P. Y. Leonov, and V. M. Sushkov, "Cryptocurrency monitoring tools in financial investigations," in *Biologically Inspired Cognitive Architectures Meeting*. Springer, 2024, pp. 200–205.

[50] V. Salunkhe and S. Rajkumar, "Protection of electronic health records (ehrs) on the ethereum blockchain: Identifying and preventing active threats to smart contracts." *KSII Transactions on Internet & Information Systems*, vol. 19, no. 1, 2025.

[51] T. S. Goh, D. Jonas, B. Tjahjono, V. Agarwal, and M. Abbas, "Impact of ai on air quality monitoring systems: A structural equation modeling approach using utaut," *Sundara Advanced Research on Artificial Intelligence*, vol. 1, no. 1, pp. 9–19, 2025.