ASIAN JOURNAL OF ELECTRICAL AND ELECTRONIC ENGINEERING
Vol. 4 No. 2 2024
E-ISSN: 2785-8189

Blockchain Based Email Security to Mitigate Phishing Attack

Othman O. Khalifa[1,2*], Tengku Hanis Sofea Binti Tengku Nor Effendy[1], Muhammed Zaharadeen Ahmed[1], Elmahdi A. El-Khazmi[3] and Abdelrahim Nasser Esgiar[4]

[1]*Deptment of Electrical and Computer Engineering, Faculty of Engineering, International Islamic University Malaysia, Malaysia*
[2]*Libyan Center for Engineering Research and Information Technology, Bani Walid, Libya*
[3]*College Of Electronic Technology, Bani Walid, Libya*
[4]*Department of Electrical and Electronic Engineering, Sirte University, Libya*

*Corresponding author: ookhalifa@gmail.com

(Received: 13 December 2024; Accepted: 18 December 2024)

Abstract— Due to the rapid development of research in blockchain technology and cryptocurrencies, all sectors of an economy rely on their security essentials to mitigate various patterns of attack on the Internet. The smart contract is a transaction protocol that strengthens, verifies, and automatically enforces agreements after negotiation between multiple untrustworthy blockchain parties. Despite the positive aspects of smart contracts, issues of security risks, weaknesses, and legal challenges continue to undermine their implementation. This paper proposes an enhanced email verification system using blockchain-enabled smart contracts. In this framework, blockchain email enables swift verification of all emails being transmitted by introducing a challenging framework that prevents an internet attacker or cybercriminal from altering the authentication process. An acknowledgement email will be transmitted to the sender upon successful delivery, and the receiver can automatically receive the email with unique credentials. The findings reveal that the proposed system significantly mitigates phishing attacks by ensuring email authenticity and transaction integrity through blockchain hashing techniques, thereby enhancing email security in both online and offline environments.

Keywords: *Blockchain, Smart Contract, Email Security, Phishing Attack, Authentication, Decentralized System.*

1. INTRODUCTION

Nowadays, customers are provided with numerous internet and social platforms to access businesses of all sorts using technology. However, all these applications have not silenced the use of email applications in all aspects of human digital communications. Based on Cisco 2020 statistics [1], up to 300 billion emails are sent and received every 24 hours. Therefore, its significance makes hackers naturally attract hackers. The average worker sends and receives several emails daily. This transmission traffic stimulates cybercriminals to send phishing emails [2].

In corporate, educational, and political institutions, email applications are among the most susceptible communication channels whereby security issues such as password theft and man-in-the-middle assaults to spear-phishing and invoicing fraud can occur easily. Email can be used to transmit viruses to a susceptible end device. This especially occurs in the challenges of ransomware. This challenge risks a company from leaking confidential information and profit losses in billions and trillions from customers. The conventional email application is vulnerable due to its plain text nature of message transmission. Users can easily translate, duplicate, or alter the message [3].

Phishing activity is a form of online cybercrime. It enables online criminals to send deceptive messages to users to steal vital information. Phishing is a social engineering technique that persuades a user as an attack target to generate vital information. This information can be emailing addresses, usernames, passwords, biodata or users' financial information [4]. Phishing attacks can be in the form of e-mail, VOIP, SMS, instant messaging, social media, and even multiplayer gaming. Some of the major categories

DOI: https://doi.org/10.69955/ajoeee.2024.v4i2.73

2. LITERATURE REVIEW

In this paper, an analysis is conducted on email security and phishing attacks using their online security operational criteria.

2.1. Email Security and Phishing Attacks

The Electronic mail application (email) is a highly significant and formal means of digital communication. Most people that use the internet in corporate, educational, business sports etc. use email to exchange information. Email is a soft target for cyber criminals when conducting criminal activities like spoofing and phishing. With the large use of email communication, uploading attachments is being misused and can lead to the transmission of malware to some target devices. The email communications on the internet are not fully secured as they are being transmitted from source to destination. Some messages can be blocked and intercepted to avoid successful delivery to an intended destination [5] [6]. This allows an unauthorized recipient to access and read the message, which can be exposed to the public.

The conventional email protocol system has some obvious challenges. Therefore, [7] analyzed the issues below ass a critical challenge that require research enhancement.

i. Username and password-based authentication is considered weak. This is because the attacker can guess this information using a dictionary attack and break the authentication technique.
ii. Mailboxes and email messages security for mail servers depends on operating system (OS) security. The lack of a better OS security policy can enable the attacker to obtain access to the mailboxes and email messages.
iii. Emails are delivered by users with limited security knowledge and their configuration parameters. This enables cybercriminal access and alters email messages.

Based on research in [8][9][10], the following security criteria can enhance email security.

i. *Confidentiality*: Confident data ensures user privacy for email communication.
ii. *Integrity*: this ensures an effective policy of protection against attacks such as spam, phishing, malware etc.
iii. *Authentication*: This verification process is used to identify a user.
iv. *Non-repudiation*: this defines the sender's non-denial such that the email is not disowned by its sender even with a low-security mechanism.

Phishing is frequently used as a straightforward approach for most cyber criminals. They steal user data through fraudulent means, such as passwords, credit card number information, user login information, etc. They compose a false email to random users requesting such information. Figure 1. Shows the phishing activities by years.

Fig. 1: Phishing Websites Detected by Years (https://www.statista.com/statistics/266155/number-of-phishing-domain-names-worldwide/)

However, phishing activity is not limited to emails only but extends to Voice Over IP (VOIP), Short Message Service (SMS), instant messaging, social media, and website advertisements [11]. A complete process of phishing attack is presented in Figure 2.

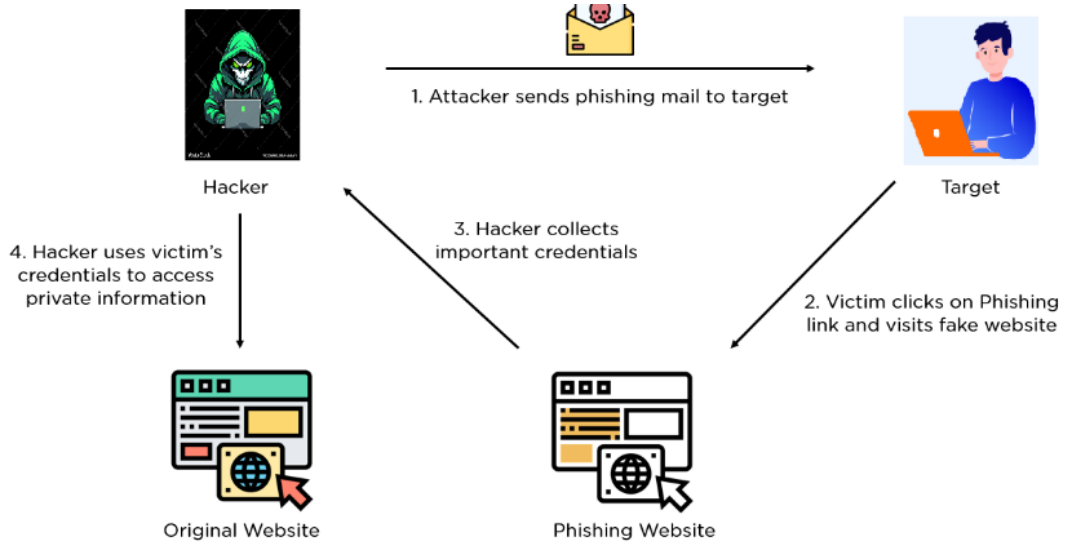

Fig. 2: Phishing attack diagram [2]

3. RELATED WORK

This paper reviewed the related studies on email security and phishing using blockchain technology. In [12], a blockchain-based ledger service is proposed such that a public key for all email addresses transmitted can be viewed and retrieved. This can lead the attacker to generate a compressed Bitcoin address. Therefore, a Bitcoin address for a transmitting user is sent as an email. This will then be kept as a record on the attacker server using time and size information. The transmitter's private key was signed based on the number of recipients who authorized the online transaction.

The. Mashtalyar *et al.* conducted research on spam message identification using blockchain [13]. All the emails transmitted using this approach will contain a wallet account address. However, the process of transmitting and receiving email protocol is unchanged.

Another researcher, Abroshan et al., integrates the Ethereum blockchain to link email addresses to an online wallet account to prevent hackers from transmitting spam messages [14] s. At the transmitter's end, the mail server verifies the availability of cryptocurrency funds to process a query. When funds are available, the crypto server enables email acknowledgement for the recipient's wallet. This process triggers mining onto the blockchain, and another email gets transmitted to the intended receiver with the transaction receipt. At the receiver's end, the mail server checks matching cryptocurrency if it is credited into the receiver's wallet account. If confirmed, an email is sent to the recipient. if otherwise, the email is considered spam and will be sent to the receiver's spam folder.

4. METHODOLOGY

The proposed solution is to develop a software plugin that any email service provider can use. This functions by installing it on a PC and linking the application through the browser. This can detect whether a received email is phishing after checking the email's header, subject line, and domain name. These criteria are pre-defined and stored in the system's database. Therefore, only users with registered credentials and who have no database records will be recognized as authenticated users within the company. Then, the system will notify the user whether it is safe to click an email or delete it. This solution is presented in a flowchart, as shown in Figure 3.
The flowchart of the figure above depicts the verification process of using blockchain between the sender/ transmitter and receiver ends.

The following procedure is executed at the sender's end.

i. Blockchain is used to enable email provider parties to connect the extension through verification.

ii. After acknowledgement of email delivery, the sender, receiver, message hash, and data are transmitted to the blockchain system.
iii. The blockchain server nodes immediately complete the verification process, and the data is written into a block.
iv. Transaction ID gets transmitted to the email provider as an acknowledgement.
v. transaction ID information gets recorded in the email header field. Hence, the message is delivered to the intended destination.

The following procedures are executed at the receiver's end.

i. The email provider that connects the blockchain extension receives the mail.
ii. Blockchain transaction ID gets deleted from the header field and transmitted to the blockchain API service. This process generates information such that all email IDs, sender, and hash value gets compared with the receiving mail.
iii. When information matches, it confirms to the system framework that there is no email forgery.
iv. Due to a lack of infrastructure at the client end, the customer business continues with additional email security.

Table 1. Summary of Related Works

Author	Contribution	Results	Limitations
[1]	The paper assesses Ethereum Blockchain based on internet attacks to prevent phishing and spam attacks	• The paper achieves successful security on both the transmitter-receiver using the blockchain wallet account • The paper achieves successful acknowledgement after email information validation for the cryptocurrency account	• The paper was not able to detect an email at the receiver if it is spam or a normal email message • The paper noted identifying losing a crypto payment at the sender end when an email is moved to the spam folder by the receiver
[2]	The paper implements a multi-channel graph classification (MCGC) framework to detect Phishing	• The paper enhanced the transaction pattern graph for each user • The paper conducted graph classification to detect phishing attacks.	• The paper identifies the high complexity of graph analysis on large-scale data
[3]	The paper implements a Deep Neural Network That can detect phishing attacks on the internet	• The paper achieves High accuracy in detecting phishing attack	• The paper was limited to depend highly on the setting of different learning parameters
[4]	The paper conducts a Machine Learning approach to detecting cybercrime	• The paper achieves real-time data for phishing attacks using legitimate website classes • The paper exploits various classifiers for detecting phishing with high accuracy and robust output	• The paper has not exploited the technique of Ensemble learning techniques. • The paper identifies Feature reduction as a parameter not exploited to Lower performance for phishing using comparison with extra tree base classifier technique.

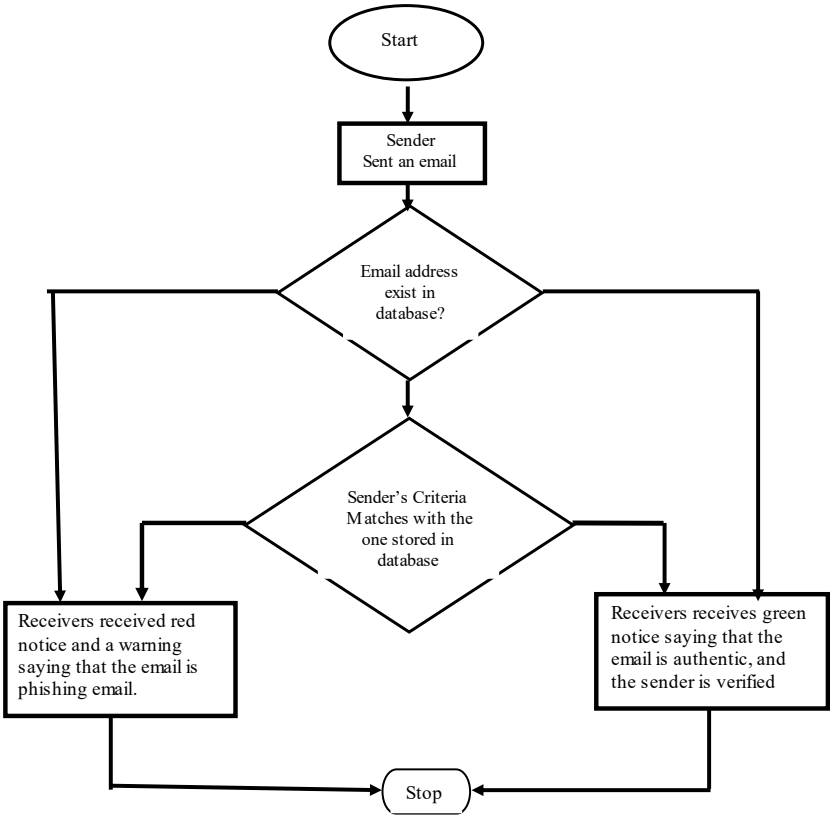

Fig. 3: Proposed Flowchart of the Email Security System

The process of reading the proposed abstraction level and program development is presented in a flowchart, as shown in Figure 4.

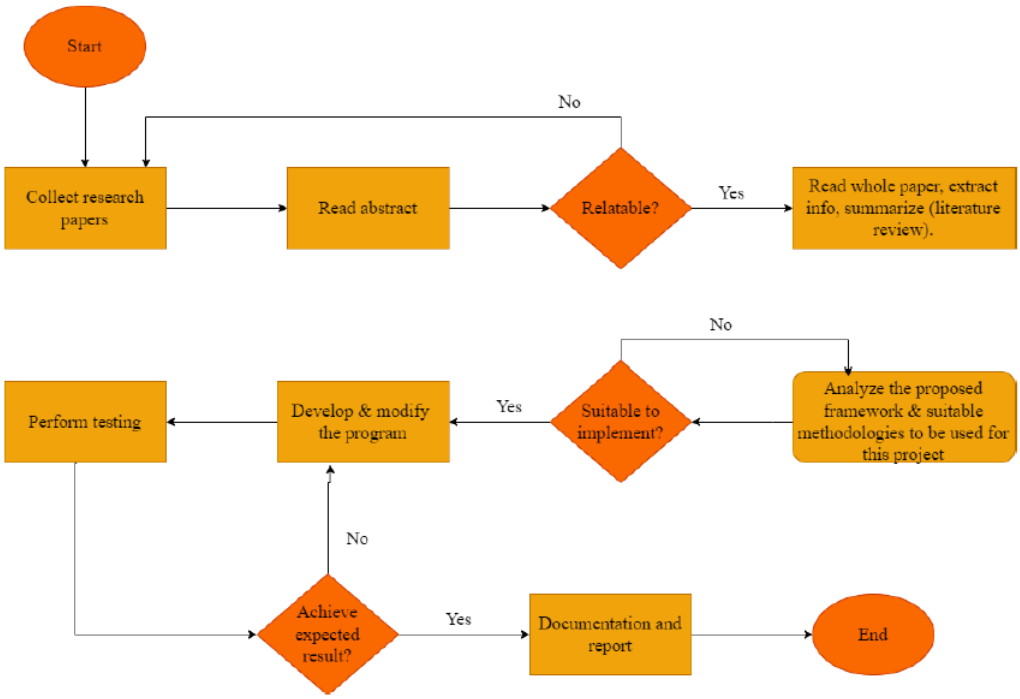

Fig. 4: Initial flowchart of proposed solution

The Conventional approach of verification does not support blockchain-based verification. Email records like

sender, recipients, and timestamp are hashed and preserved by any company that intends to secure its email gateways using the proposed blockchain framework in this paper. This, however, can compromise their privacy. Meanwhile, the email may not be spoofed because any entity in reception will require validation using blockchain service.

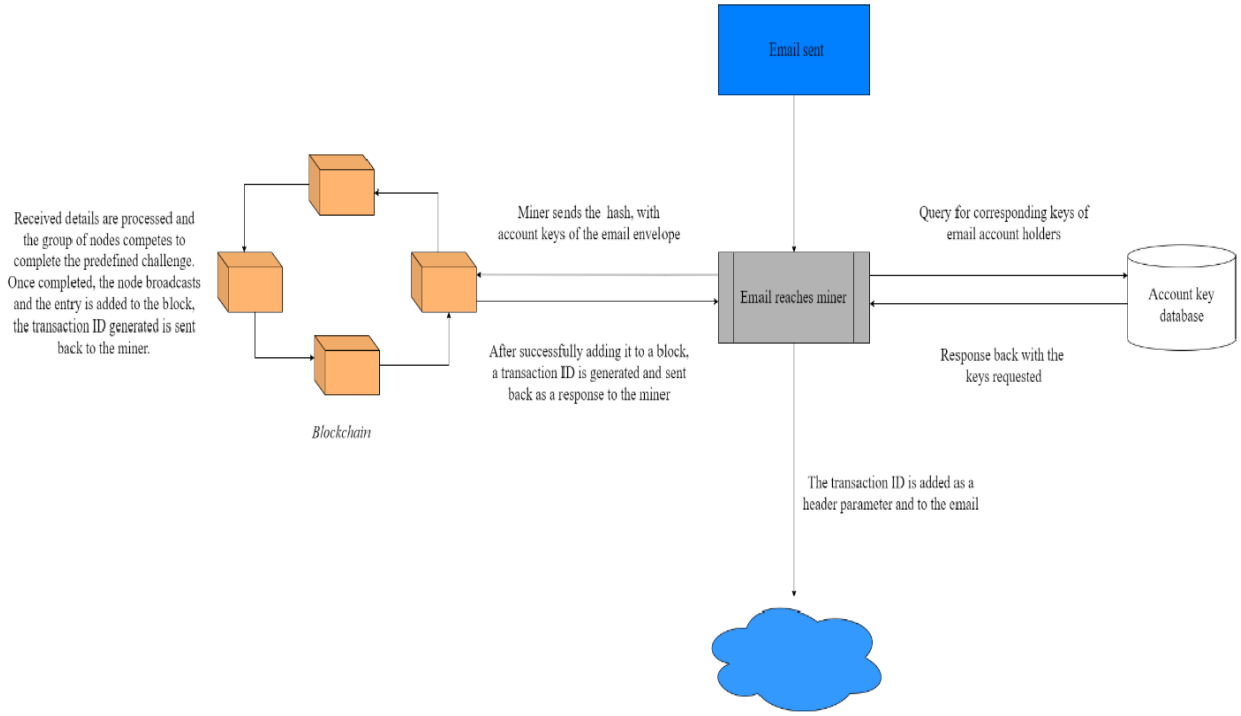

Fig. 5: Email Verification Process at Sender

At the sender's end, figure 5 above presents the process of email verification using blockchain technology.

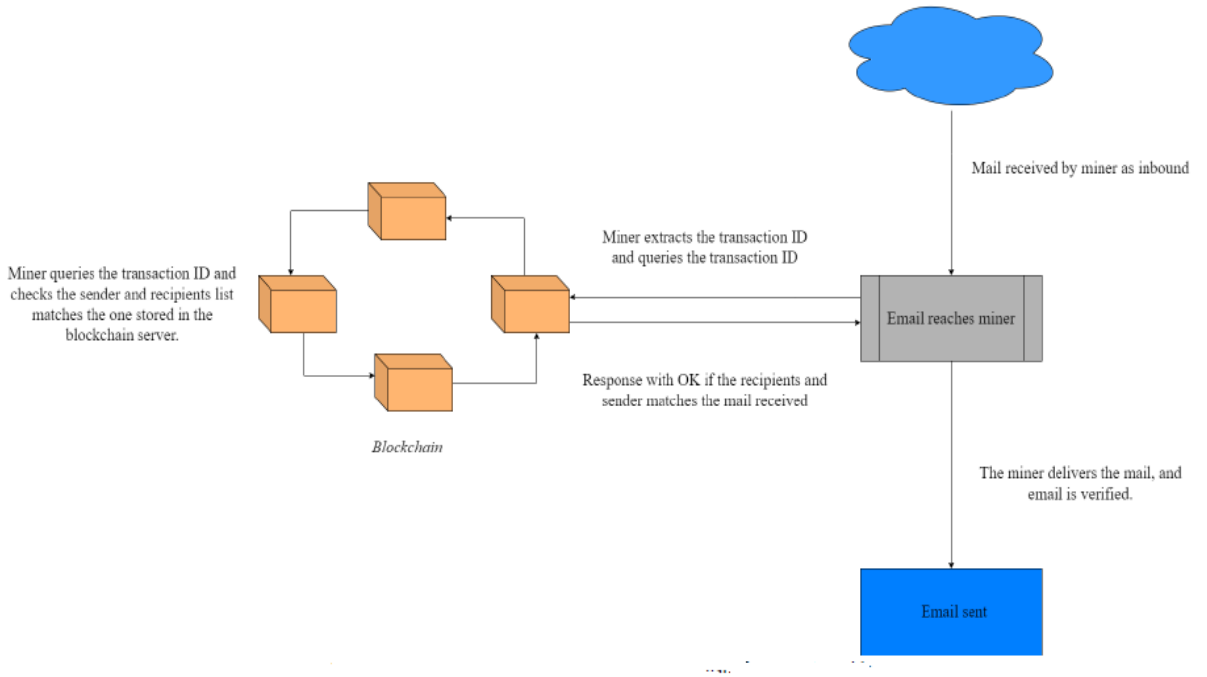

Fig. 6: Email Verification Process at Receiver

Figure 6 above presents the email verification process using blockchain technology at the receiver's end. This paper uses a local blockchain known as 'LBRY' by transmitting an email initiate, a transaction for the blockchain containing metadata. The blockchain stores the email metadata and encrypted data only accessed by the transmitter and receiver. All the blocks are indexed using hash value, where a new block carries the hash value of a previous block. This technique can ensure a steady exchange of resources for the transaction, as presented in the result section.

5. RESULTS

This section presents the simulation results on the local host and the internet for the blockchain email application to mitigate the impact of phishing attacks and enhance email security.

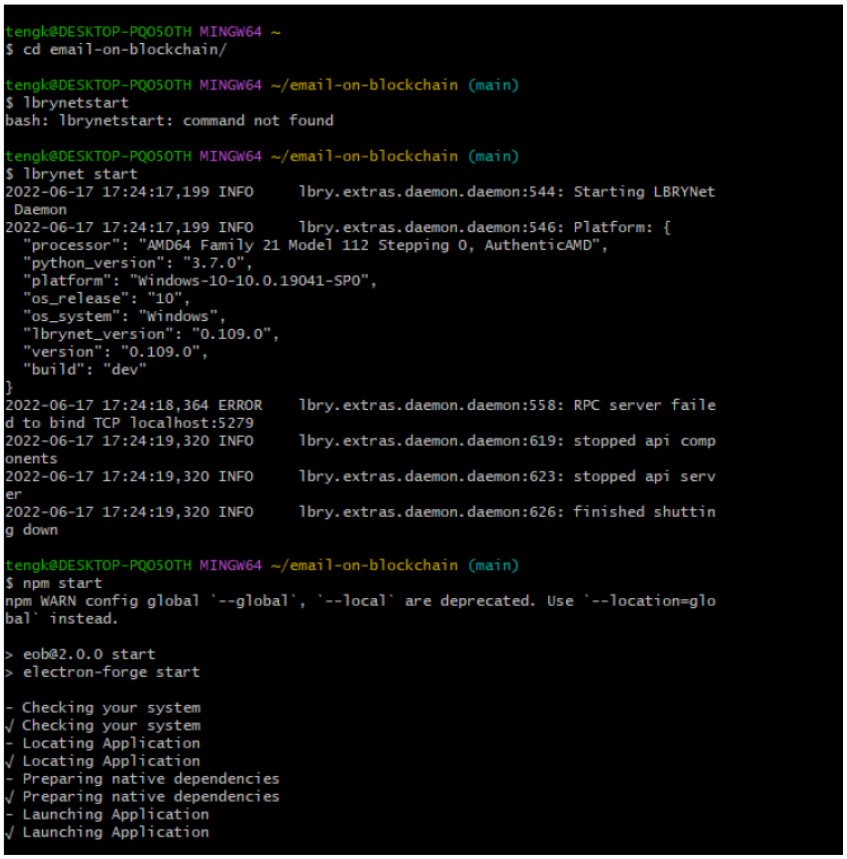

Fig. 7: Local host result of command prompt

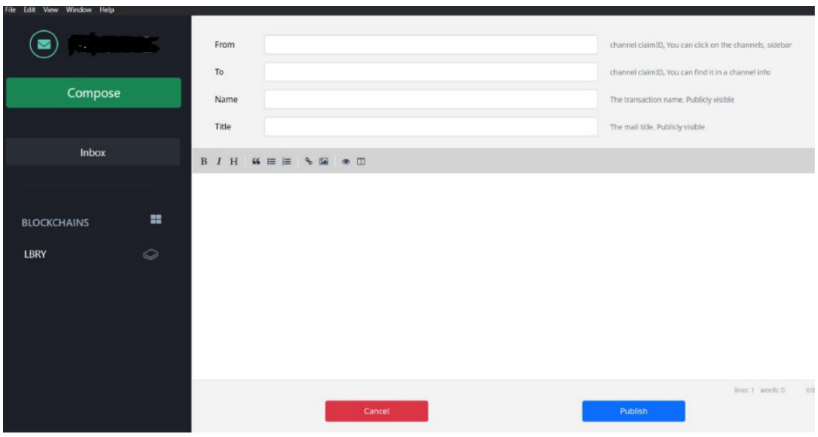

Fig. 8: Interface of Blockchain Email System

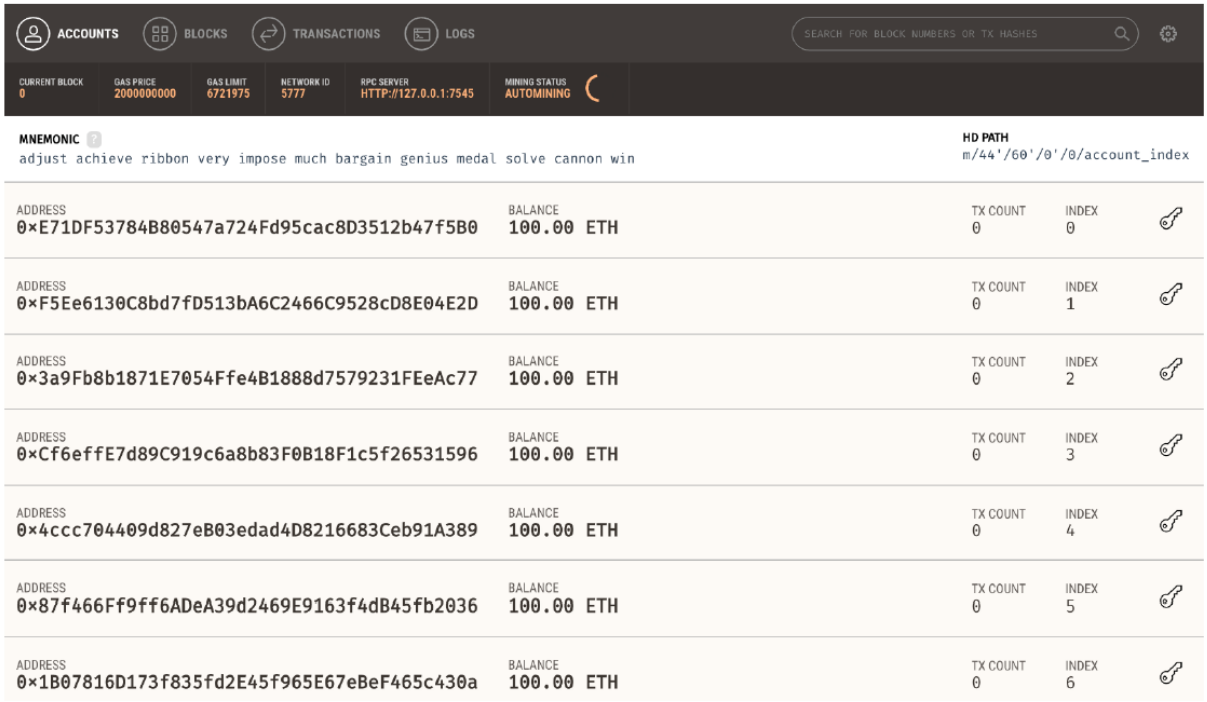

Fig. 9: Blockchain Transactions

Based on Figure 7 above, the end device implements the blockchain transaction in a local host. Therefore, the emailed application can be deployed and implemented both online and on a local host using a Windows command prompt. In addition, the research also conducts analysis both online and offline. The online blockchain email interface is presented in Figure 8.

Based on Figure 9, the online Transactions conducted are being hashed using the local personal blockchain. Therefore, records show that marketers using email are among the major beneficiaries of Blockchain email.

6. COMPARISON AGAINST EXISTING EMAIL SECURITY FRAMEWORKS

Traditional email security systems rely on TLS, SSL, and password-based authentication. While these approaches provide convenience and encryption in transit, they are subject to phishing, spoofing, and password assaults due to inadequate verification procedures and reliance on human factors (Alhassan et al., 2020). The proposed blockchain-based approach addresses these restrictions by decentralizing email verification via immutable metadata storage, assuring integrity and validity prior to transmission.

Table 2. Comparison of the proposed system with existing email security frameworks

Framework	Processing Time	Scalability	Recourse Consumption
Traditional Email Security	Low processing time but vulnerable to phishing and spoofing	Highly scalable but lacks advanced verification mechanisms	Minimal resource consumption but relies on weak security models.
PKI and S/MIME	Moderate processing time due to cryptographic operations.	Limited scalability due to complex key management processes.	High resource consumption for key exchange and verification.
Proposed System	Optimized processing time with lightweight hash verification.	Highly scalable due to decentralized design without cryptocurrency reliance.	Low resource consumption as no complex cryptographic management is required.

Furthermore, PKI and S/MIME use cryptographic key pairs to encrypt and digitally sign emails, assuring privacy and sender legitimacy. However, relying on central Certificate Authorities (CAs) introduces single points of failure, and key management is complicated and vulnerable to MITM attacks (Rathi & Kumar, 2021). The proposed method removes CAs by verifying using a decentralized blockchain ledger, decreasing complexity and

improving security.

To evaluate the effectiveness of the proposed blockchain-based email security system, a comparison is conducted against traditional email security frameworks and PKI-based solutions. The comparison focuses on processing time, scalability, and resource consumption, as shown in Table 2.

However, the proposed system's primary merits are its anti-phishing mechanism, deterministic verification of email authenticity, and seamless interaction with existing email protocols. By integrating blockchain's immutability and decentralization, the system tackles the constraints of conventional frameworks, PKI-based solutions, AI systems, and existing blockchain implementations.

This comparison shows that the proposed blockchain-based email security system improves processing speed, scalability, and resource usage while addressing the constraints of current email security frameworks.

7. CONCLUSION

The fundamental characteristics of Blockchain are its privacy and security features. These features are implemented in new authentication models, connection upgrades, security enhancements, and the adoption of encryption standards. Blockchain enhancements become beneficial in lessening the impact of spam, phishing, and data theft, supporting an improved email protocol. Additionally, the blockchain technology mode of operation is decentralized. This decentralization guarantees the highest level of protection for emails. In peer-to-peer communications, security is ensured, offering the highest levels of data protection, personal information security, and password security for email protocols.

This paper reviewed related works to highlight email security issues based on security requirements and parameter assessments. It also investigated and identified the most effective approaches for detecting phishing attacks in electronic mail protocols. In this work, the proposed approach improves email security by hashing email information and preserving it permanently on a decentralized blockchain ledger. This provides tamper-proof verification of email authenticity before transmission, overcoming the constraints of conventional, PKI-based, AI-driven, and current blockchain systems. Key characteristics include proactive phishing avoidance, deterministic verification, and easy interaction with current email protocols, resulting in a scalable and effective solution.

REFERENCES

[1] H. S. Al-Julandani and K. Al-Harthy, "Integrate Blockchain with Cloud Based Architecture to Prevent Phishing Attack," in 2022 10th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), Noida, India, 2022, pp. 1-6. https://doi.org/10.1109/ICRITO56286.2022.9964982

[2] B. Samuel and V. T. Somasundaran, "Prevention of Man-in-the-Middle Attacks using Blockchain VPN," unpublished.

[3] A. Alabdulatif, I. Khalil, and M. S. Rahman, "Security of Blockchain and AI-Empowered Smart Healthcare: Application-Based Analysis," Applied Sciences, vol. 12, no. 21, p. 11039, 2022. https://doi.org/10.3390/app122111039

[4] A. Chakraborty, A. Biswas, and A. K. Khan, "Artificial Intelligence for Cybersecurity: Threats, Attacks and Mitigation," arXiv preprint arXiv:2209.13454, 2022. https://doi.org/10.1007/978-3-031-12419-8_1

[5] A. Pillai, A. V. Ramachandran, and V. Saraswat, "Design Considerations for Protection of Blockchain based Digital Identity Ecosystem," Journal of Information Assurance & Security, vol. 17, no. 3, pp. 171-180, 2022.

[6] G. R. Permana, T. E. Trowbridge, and B. Sherborne, "Ransomware Mitigation: An Analytical Investigation into the Effects and Trends of Ransomware Attacks on Global Business," unpublished, 2022. https://doi.org/10.31234/osf.io/ayc2d

[7] M. S. Kumar, S. Vimal, N. Z. Jhanjhi, S. S. Dhanabalan, and H. A. Alhumyani, "Blockchain based peer to peer communication in autonomous drone operation," Energy Reports, vol. 7, pp. 7925-7939, 2021. https://doi.org/10.1016/j.egyr.2021.08.073

[8] D. Piedrahita, J. Bermejo, and F. Machío, "A Secure Email Solution Based on Blockchain," in International Congress on Blockchain and Applications, Springer, Cham, 2021, pp. 355-358. https://doi.org/10.1007/978-3-030-86162-9_36

[9] M. M. Salama, "Using Blockchain Technology to Prevent Spoofing Attack in IoT Environment," International Journal of Computer Science and Network Security (IJCSNS), vol. 21, no. 3, pp. 51-58, 2021. https://doi.org/10.1201/9781003337393-8

[10] A. Pillai, A. V. Ramachandran, and V. Saraswat, "Design Considerations for Protection of Blockchain based Digital Identity Ecosystem," Journal of Information Assurance & Security, vol. 17, no. 3, pp. 171-180, 2022.

[11] A. Bhardwaj, F. Al-Turjman, V. Sapra, M. Kumar, and T. Stephan, "Privacy-aware detection framework to mitigate new-age phishing attacks," Computers & Electrical Engineering, vol. 96, p. 107546, 2021. https://doi.org/10.1016/j.compeleceng.2021.107546

[12] H. Abroshan, J. Devos, G. Poels, and E. Laermans, "Phishing happens beyond technology: the effects of human behaviors and demographics on each step of a phishing process," IEEE Access, vol. 9, pp. 44928-44949, 2021. https://doi.org/10.1109/ACCESS.2021.3066383

[13] N. Mashtalyar, U. N. Ntaganzwa, T. Santos, S. Hakak, and S. Ray, "Social engineering attacks: Recent advances and challenges," in International Conference on Human-Computer Interaction, Springer, Cham, 2021, pp. 417-431. https://doi.org/10.1007/978-3-030-77392-2_27

[14] H. Abroshan, J. Devos, G. Poels, and E. Laermans, "Phishing happens beyond technology: the effects of human behaviors and demographics on each step of a phishing process," IEEE Access, vol. 9, pp. 44928-44949, 2021. https://doi.org/10.1109/ACCESS.2021.3066383