The Evolution of Email Encryption: From PGP to Modern Standards

Edward Danso Ansong
Dept of Computer Science
University of Ghana

Simon Bonsu Osei
Dept of Computer Science
University of Ghana

Gloria Agyapong
Dept of Computer Science
University of Ghana

ABSTRACT
Email encryption has evolved from early methods like PGP and S/MIME to modern standards such as End-to-End Encryption (E2EE) and Transport Layer Security (TLS). This paper reveals persistent usability issues, particularly among novice users, and highlight the demand for automated and user-friendly encryption solutions. PGP uses a decentralized model, while S/MIME relies on Certificate Authorities. Today, services like ProtonMail use E2EE to protect content, and TLS secures email during transmission. Despite advancements, challenges remain, innovative solutions, including blockchain-based key management and AI-enhanced cryptography, are proposed to address these challenges and promote broader adoption. By integrating automation, intuitive design, and educational initiatives, email encryption can become more accessible, fostering secure communication across diverse user groups.

General Terms
Secure/Multipurpose Internet Mail Extensions (S/MIME), Pretty Good Privacy (PGP), End-to-End Encryption (E2EE), Transport Layer Security (TLS).

Keywords
Encryption keys, Quantum-resistant encryption, Blockchain key management, Cyber threats, Artificial intelligence in encryption.

1. INTRODUCTION
Email encryption is vital for securing the confidentiality and integrity of messages over potentially insecure networks [1]. It ensures that sensitive data, such as financial, personal, and business information, is protected from unauthorized access. As email became a key communication method, the need for robust encryption grew due to increased risks from cyberattacks and data breaches [2]. The evolution of email encryption began with early methods like Secure/Multipurpose Internet Mail decentralized trust model combining digital signatures with symmetric and asymmetric encryption [4]. In contrast, S/MIME, which emerged shortly after PGP, uses a hierarchical certificate authority (CA) model, integrating well with email clients but presenting different trust and security challenges [5, 6]. As cyber threats evolved, so did the importance of email encryption. The increasing volume of sensitive information and the potential consequences of breaches underscored the need for robust encryption methods, making it essential for both security and regulatory compliance [7].

2. RELATED WORKS
The evolution of email encryption has led to the development of robust standards designed to protect user privacy and data security. However, these modern standards face numerous challenges and limitations that have sparked extensive research and debate. This section reviews the existing literature on these challenges, the methodologies developed to address them, and the comparative effectiveness of these approaches.

2.1 Modern Standards in Email Encryption and their Implementation
In the evolving landscape of digital communication, modern standards in email encryption have become essential for ensuring the privacy and security of email content.

2.1.1 End-to-End Encryption
One of the most prominent advancements in this domain is End-to-End Encryption (E2EE), which has been increasingly adopted by privacy-focused email services like ProtonMail and TutanotaEmails are encrypted on the sender's device and are only decryptable by the receiver thanks to E2EE. This procedure ensures that not even email service providers, who lack the decryption keys, may view the contents of the mails. In order to encrypt an email, a pair of cryptographic keys must normally be created: a public key for encryption and a private key for decryption. This method of encryption is particularly valued for its ability to provide a high level of security and privacy, especially in scenarios where sensitive information is being exchanged [8, 9]. For instance, ProtonMail uses the recipient's public key to automatically encrypt emails as soon as they are composed, thereby implementing E2EE. After receiving the email, the recipient decrypts and reads the message using their private key. This method guards against any breaches within the email service provider itself in addition to external threats to the content. Similarly, Tutanota offers a fully encrypted mailbox, where even the subject lines and attachments are protected. Tutanota further enhances privacy by integrating encryption into its contact forms and calendar features, extending E2EE beyond standard email communication. These services have gained popularity due to their strong privacy policies and user-friendly interfaces, making advanced encryption accessible to a broader audience [10, 11]. The implementation of E2EE in these services exemplifies the growing demand for robust privacy solutions in a world where digital communications are frequently targeted by cyber threats [10].

2.1.2 Transport Layer Security
The TLS protocol is made up of header which contains the message content, the message data, validation and a footer. A transport protocol and standard should form the foundation of the TLS Record Protocol [34].

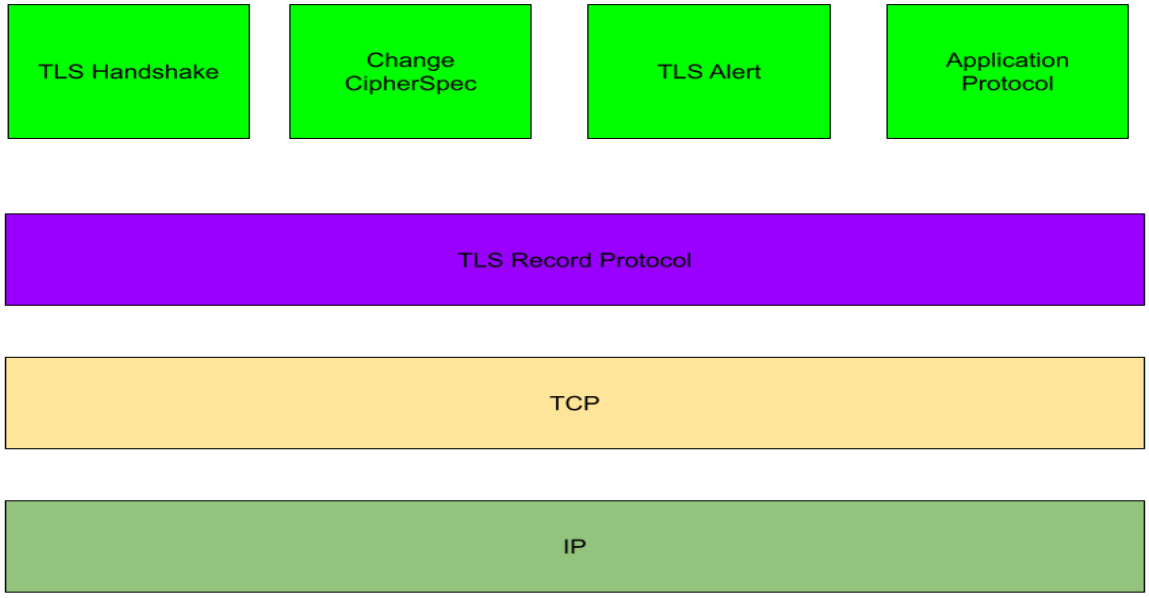

Figure 1: Framework for Transport Layer Security Record Protocol

Transport Layer Security (TLS) is another critical component in the modern email encryption framework, playing a key role in securing email during transmission. To prevent email from being intercepted while it is in transit, TLS encrypts the communication link between the email servers of the sender and the recipient. A description is what is found in fig 1. By using TLS, data is protected against easy reading and manipulation even in the event of interceptions [12]. STARTTLS, an extension of the Simple Mail Transfer Protocol (SMTP) that allows email servers to convert a plaintext connection to an encrypted one using TLS and is a popular way that TLS is implemented in email systems. STARTTLS is widely supported by most modern email servers and clients, providing a basic level of security for email transmission. However, while TLS and STARTTLS significantly reduce the risk of interception during transit, they do not offer end-to-end encryption, meaning that emails could still be accessed by service providers or compromised if the servers are breached [13, 14].

2.1.3 Quantum Computing

Email encryption will encounter significant difficulties in the future as technology develops, especially with the introduction of quantum computing. Conventional encryption schemes, which are based on challenging mathematical issues that are challenging for classical computers to answer, may be broken by quantum computers. As a result of this impending danger, encryption techniques that are resistant to quantum computers' processing capability have been developed [15]. The goal of this field's current research is to develop cryptography methods that withstand quantum attacks. Two intriguing methods that have demonstrated resistance to attempts at quantum decryption are lattice-based encryption and hash-based cryptography [16]. The integration of quantum-resistant encryption into email services is still in its early stages, but it is an essential area of research as we prepare for a future where quantum computing could potentially compromise existing encryption methods [17].

3. Methodology

To analyze the evolution of email encryption technologies, this study employed a mixed-methods approach that combines qualitative and quantitative research methods. The methodology aimed to comprehensively assess the progression of email encryption standards, their effectiveness, usability challenges, and adoption barriers. Below are the steps taken during the research process:

A thorough literature review was conducted to gather and synthesize existing research on email encryption methods, including Pretty Good Privacy (PGP), Secure/Multipurpose Internet Mail Extensions (S/MIME), End-to-End Encryption (E2EE), and Transport Layer Security (TLS). Key trends and gaps in the literature were identified to establish a foundation for analysis. Based on insights from the literature, criteria were established to evaluate the selected encryption methods. The evaluation focused on factors such as security effectiveness, usability, and adoption barriers.

3.1 Structured Interviews on Email Encryption

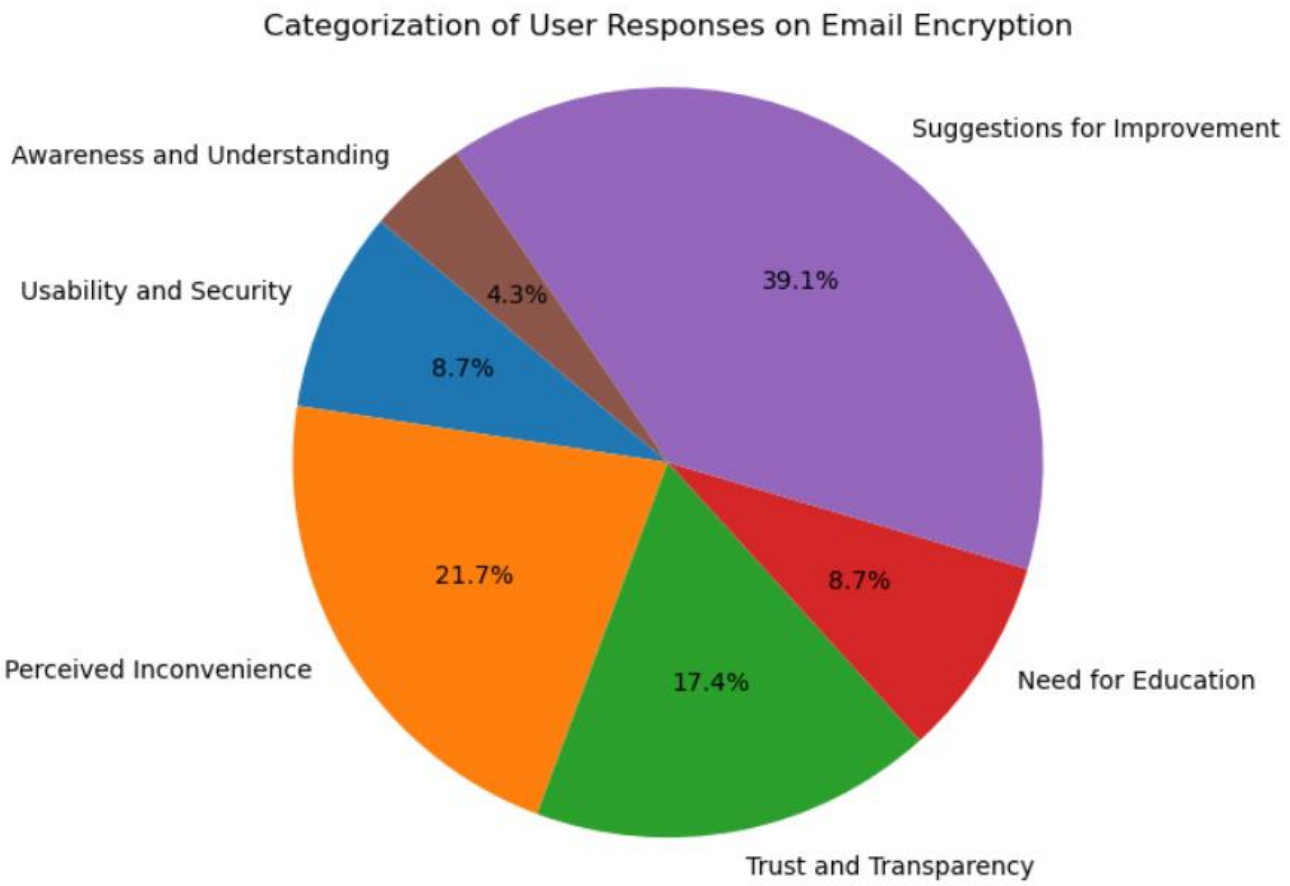

Figure 2: User Response on Email Encryption

Semi-structured interviews were conducted with a total of 30 participants categorized into three groups: novice users (Group A), intermediate users (Group B), and advanced users (Group C). The participants were selected to represent diverse demographics, including varying levels of technical expertise, age groups, and professional backgrounds. Focus group discussions provided additional qualitative insights into user perceptions, challenges, and suggestions regarding email encryption.

3.2 Thematic Analysis

Thematic analysis was conducted on the qualitative data collected from interviews and focus group discussions regarding user perceptions of email encryption. This analysis aimed to identify common trends and patterns that emerged from participants' experiences, challenges, and suggestions related to email encryption and blockchain key management. The thematic analysis revealed critical insights into user perceptions of email encryption, highlighting the importance of awareness, usability, trust, and improvement with regards to email encryption.

3.3 Coding Framework for Categorizing Responses in User Experiences and Challenges with Email Encryption

To analyze the qualitative data collected from interviews and focus group discussions, a coding framework programmed in python is employed. This framework categorizes responses into specific codes, allowing for the identification of patterns and insights regarding user experiences and challenges with email encryption.

3.3.1 Coding Process Overview

Familiarization: Read through the data to understand the content and context.

Initial Coding: Generate initial codes based on recurring themes and concepts.

Focused Coding: Refine and group initial codes into broader categories.

Thematic Analysis: Identify overarching themes from the categorized codes.

Table 1: Thematic Coding Categories and Codes

Category	Code	Description
Suggestions for Improvement	Integrating, Blockchain, One-Click	Advocacy for more intuitive and user-friendly encryption interfaces.
Awareness and understanding	Awareness	Recognition of email encryption and its importance.
Usability Challenges	Complicated, Overwhelmed	Difficulty in navigating encryption tools and processes.

Perceived Inconvenience	Time, Takes too long	Concerns about the time required to encrypt emails.
Trust and Transparency	Trust, Resources	Doubts about the privacy practices of email service providers.
Need for Education	Educational	Suggestions for workshops, tutorials, and resources to improve understanding.

3.4 Security And Usability Trade-Off

One of the primary challenges in modern email encryption is the trade-off between security and usability. Strong encryption mechanisms, such as End-to-End Encryption (E2EE), offer high levels of security but often come at the cost of user convenience. For instance, users must manage cryptographic keys, which can be a complex and error prone process. Papers such as those by [18] have extensively discussed this usability challenge, coining the term "Johnny can't encrypt" to describe the difficulty that average users face in effectively using encryption tools. More recent studies continue to highlight this issue, pointing out that while security has improved, usability remains a significant barrier to widespread adoption [19, 20].

3.5 Barriers to Email Encryption Adoption

Another significant challenge is the widespread adoption of email encryption technologies. Despite the availability of sophisticated encryption tools, their adoption remains limited due to factors such as lack of user education, complexity of setup, and inconsistent support across different email clients and platforms. Research by [21] highlights that many users are either unaware of the need for encryption or find it too difficult to implement. Moreover, regulatory and legal barriers, particularly in regions with stringent government surveillance policies, further complicate the adoption of encryption technologies. Studies by [22, 23] discussed how government regulations, such as the UK's Investigatory Powers Act, pose challenges to the widespread adoption of encryption by creating potential conflicts between privacy and legal compliance.

3.6 Enhancing Usability in Email Encryption

Researchers have proposed various methodologies to address the usability challenges of email encryption. One approach focuses on improving the user interface (UI) and experience (UX) of encryption tools to make them more intuitive. For instance, [24] developed simplified key management systems and integrated them seamlessly into email clients, reducing the cognitive load on users. Their studies demonstrate that with better design, the perceived complexity of encryption can be significantly reduced, leading to higher adoption rates. Another approach involves leveraging existing platforms, such as webmail services, to integrate encryption in a way that is invisible to the user, thereby eliminating the need for users to manage encryption keys manually [25].

3.7 Comparative Analysis

A comparative analysis of modern encryption methods was conducted using the established criteria. Quantitative measures and qualitative insights were combined to assess the effectiveness, usability, and adoption of these methods. Blockchain and AI integration were explored as potential solutions to address existing challenges in email encryption.

3.8 Blockchain for Decentralized Email Encryption

Technological innovations have increasingly been directed at overcoming the inherent limitations of modern email encryption, particularly in the areas of key distribution and verification. One of the most promising solutions to these challenges is the integration of blockchain technology, which has been proposed as a means to decentralize key management and verification processes [26]. Traditional email encryption systems rely heavily on Certificate Authorities (CAs) to issue and validate digital certificates, which are used to establish trust between communicating parties. However, this centralized approach introduces several vulnerabilities, including the risk of CA compromise, certificate forgery, and the possibility of single points of failure [27, 28].

3.9 Blockchain as an Alternative to Traditional Certification Authorities

Research by [26] delves into the potential of blockchain technology to address these issues by providing a decentralized alternative to traditional CAs. In a blockchain-based system, encryption keys and certificates can be distributed and verified across a network of nodes, eliminating the need for a central authority. This decentralized approach inherently enhances security by making it significantly more difficult for attackers to compromise the entire system. Even if one or more nodes in the blockchain network are compromised, the integrity of the overall key management process remains intact, as the system relies on consensus among multiple nodes to validate transactions.

3.10 AI-Enhanced Cryptography

Artificial Intelligence (AI) has also been employed to enhance encryption methods by automating key management processes and detecting vulnerabilities in real-time. A study by [29] demonstrates how AI-driven cryptographic analysis tools can identify weaknesses in encryption protocols, leading to more secure implementations.

3.11 Legal and Ethical Challenges in Email Encryption

Legal and ethical considerations surrounding email encryption are also a critical area of research. The tension between maintaining user privacy and complying with government regulations has led to significant debate and legal challenges. [30] argue that legal mandates requiring backdoors in encryption systems undermine the security of all users, creating vulnerabilities that can be exploited by malicious actors. Conversely, studies by [23] discuss the ethical implications of denying law enforcement access to encrypted communications, particularly in cases involving national security. This ongoing debate underscores the complexity of balancing security, privacy, and legal obligations in the design and implementation of email encryption technologies.

4. ANALYSIS

4.1 Results from Focus Group Discussions on Email Encryption

Participants in Group C expressed a strong understanding of encryption methods, particularly E2EE and TLS but expressed a desire for more information on how these technologies protect their data. However, many end-users reported limited knowledge about how these technologies work, with several

stating they only understood the basic concept of encryption. Participants across all groups recognized the term "encryption" but had varying levels of understanding. Novice users often associated encryption with security but could not explain how it worked or its importance. Email service providers noted that while they implement encryption, many users do not actively engage with or understand its importance.

With regards to usability challenges it shows end-users frequently cited the complexity of managing cryptographic keys as a significant barrier to using encryption tools effectively. Many users expressed that the perceived inconvenience of using encryption tools was a major barrier and also to remember passwords and manage keys. The additional steps required to encrypt emails were seen as time-consuming, particularly for users who send a high volume of emails daily. Participants emphasized the need for seamless integration of encryption features into existing email platforms to reduce friction in the user experience.

Participants voiced concerns about trusting email service providers with their data. Many expressed skepticisms about whether providers genuinely prioritize user privacy or if they might comply with government surveillance requests. They indicated a preference for email services that explicitly offer E2EE, as they felt this provided an additional layer of security and privacy.

The identified themes underscore the need for email service providers to address usability challenges and automate encryption to foster greater adoption of encryption technologies. By focusing on user-centric design and transparent communication, providers can better meet the needs of diverse user groups and promote secure email practices.

4.2 Drawing Insights

Higher frequency indicates that many participants find encryption tools and cryptographic key management processes difficult to use and time consuming therefore the necessity for simplifying user interfaces and automating encryption tasks to enhance accessibility and ease of use. Suggestions for improvement emerged as a dominant theme (from Fig 2), with 39.1% of responses advocating for solutions like blockchain-based key management systems to streamline encryption processes. Automated systems were viewed as critical for addressing usability barriers and boosting adoption.

The findings revealed a significant gap with 4.3% in awareness and understanding of email encryption among novice and intermediate users. For example, Staidorf Consult in their response during a discussion session stated, they noted that while they implement encryption, many users do not actively engage with or understand it importance, as a result there is a pressing need to organize training sessions for users. Participants emphasized the need for structured educational initiatives, including workshops and tutorials, to bridge this knowledge gap and promote informed usage of encryption tools. Perceived Inconvenience comprises 23% of responses suggesting users perceive email encryption as an obstacle due to the technical knowledge to be able to encrypt each email.

Trust and Transparency accounts for 17.4%, participants expressed skepticism about the privacy practices of email service providers, with a preference for those offering explicit End-to-End Encryption (E2EE). Building trust through transparency and robust privacy is essential for fostering user confidence in encryption solutions. Usability and Security with an 8.7% shows that the advanced users pointed out the critical need to balance strong security measures with user-friendly designs. While robust encryption methods are vital, they should not compromise the overall user experience, as this deters widespread adoption.

These categories underscore the importance of addressing these challenges through a multi-faceted approach. By integrating intuitive design, automation, and educational programs, while ensuring transparency and robust privacy protections, email encryption technologies can achieve broader adoption and usability across diverse user groups.

5. COMPARATIVE ANALYSIS OF MODERN EMAIL ENCRYPTION METHODS AND TECHNOLOGIES

Several studies have compared the effectiveness of different methodologies and technologies in overcoming the challenges associated with modern email encryption. For instance, [24] found that their simplified key management system significantly improved user adoption and satisfaction compared to traditional methods. Users were able to successfully encrypt and decrypt emails with minimal training, suggesting that usability enhancements can have a profound impact on the effectiveness of encryption technologies. Similarly, [25] demonstrated that integrating encryption seamlessly into webmail services led to higher usage rates, as users were not required to take additional steps to secure their communications. Recently in terms of technological innovations, technological innovations have significantly impacted the landscape of encryption systems, particularly in key management. One of the most promising advancements is the integration of blockchain technology, which offers a decentralized approach to key management. Unlike traditional systems that rely on centralized authorities to manage encryption keys, blockchain-based solutions distribute this responsibility across a network of nodes. This decentralization inherently enhances the security of the system by reducing the risk of key compromise through single points of failure. As noted by [26], blockchain can ensure greater transparency and auditability in key management processes, which is crucial for maintaining trust in encryption systems, a description is what is found in fig 3 used by [35]. [35] Designed a blockchain based management key to solve the issue of lack of confidence between the sites in the absence of trust anchors.

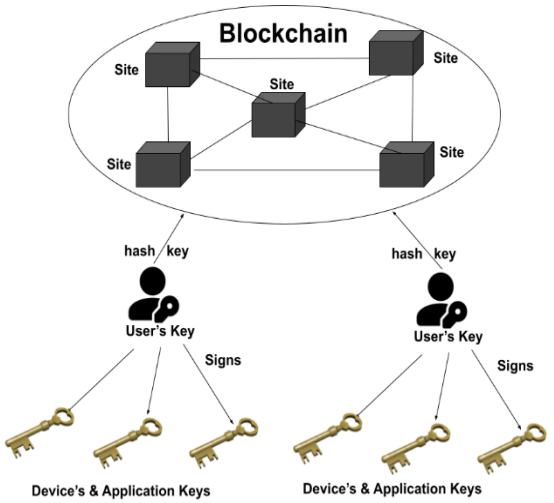

Figure 3: Blockchain Based Management Key

Despite these advantages, blockchain-based key management systems are still in their early stages of development. Scalability remains a significant challenge; as the number of participants in the blockchain network increases, so does the complexity and resource demand of maintaining the system [31, 32]. This can lead to performance bottlenecks, which need to be addressed before blockchain can be widely adopted in high-demand environments. Additionally, while blockchain offers robust security, the reliance on consensus mechanisms can introduce latency, which might be problematic for real-time applications [33]. Therefore, ongoing research is essential to overcome these hurdles and fully realize the potential of blockchain in enhancing encryption security.

Another area of innovation in encryption systems is the application of artificial intelligence (AI). AI-driven approaches have demonstrated substantial potential in automating the identification and mitigation of vulnerabilities within encryption protocols. For instance, [14] highlight how automated analysis tools, powered by AI, can perform comprehensive security assessments of encryption implementations much faster than traditional manual methods. These tools can simulate a wide range of attack scenarios, identify potential weaknesses, and even suggest or implement fixes, thereby enhancing the overall security posture of the system. This automation not only accelerates the development process but also reduces the likelihood of human error, which is a common source of vulnerabilities.

Moreover, AI can contribute to the continuous improvement of encryption systems by learning from previous security incidents and evolving threats. Machine learning models can analyze vast amounts of data to predict and counteract new forms of attacks, ensuring that encryption protocols remain resilient over time. However, the integration of AI into encryption systems also introduces new challenges, such as the need for robust training data and the risk of adversarial attacks against the AI models themselves [29]. As with blockchain, further research is needed to optimize AI-driven solutions and ensure their reliability in real-world applications.

The related works reviewed in this section highlight the significant challenges faced by modern email encryption standards and the innovative methodologies developed to address these issues. While considerable progress has been made in improving usability, adoption, and security, ongoing research is needed to address emerging threats, particularly in the context of quantum computing and evolving legal landscapes.

6. CONCLUSION

In conclusion, the evolution of email encryption from early methods like PGP and S/MIME to modern standards such as End-to-End Encryption (E2EE) and Transport Layer Security (TLS) highlights significant progress in safeguarding digital communications. While these advancements have greatly enhanced email security, challenges such as balancing security with usability, overcoming adoption barriers, and addressing legal and regulatory issues remain. Recent research emphasizes the need for improved usability in encryption tools, the potential of technological innovations like blockchain and AI, and the importance of developing quantum-resistant algorithms to future-proof email security. Case studies and comparative analyses of different methodologies underscore the practical impacts and ongoing challenges in the field. As email continues to be a vital communication tool, ongoing efforts to address these challenges and integrate new technologies will be crucial in ensuring robust and user-friendly email encryption.

7. ACKNOWLEDGMENTS

Special thanks to the experts who have contributed in discussions towards the writing of this paper.

8. REFERENCES

[1] Sangeetha, V., Rokhade, K. S., & Vijayalakshmi, N. B. (2024, January). Email Protection in the Digital Age: Evaluating Symmetric Cryptographic Algorithms. In 2024 International Conference on Intelligent and Innovative Technologies in Computing, Electrical and Electronics (IITCEE) (pp. 1-6). IEEE.

[2] Zhang, L. (2013). Provably secure certificateless one-way and two-party authenticated key agreement protocol. In Information Security and Cryptology–ICISC 2012: 15th International Conference, Seoul, Korea, November 28-30, 2012, Revised Selected Papers 15 (pp. 217-230). Springer Berlin Heidelberg.

[3] Housley, R. (2022). Evolution of Email Security Standards. IEEE Communications Magazine, 60(11), 6-9.

[4] Stransky, C., Wiese, O., Roth, V., Acar, Y., & Fahl, S. (2022, May). 27 years and 81 million opportunities later: Investigating the use of Email encryption for an entire university. In 2022 IEEE Symposium on Security and Privacy (SP) (pp. 860-875). IEEE.

[5] Sannella, M. J. 1994 Constraint Satisfaction and Debugging for Interactive User Interfaces. Doctoral Thesis. UMI Order Number: UMI Order No. GAX95-09398., University of Washington. S/MIME with multiple e-mail address certificates: A usability study.

[6] Astorga, J., Barcelo, M., Urbieta, A., & Jacob, E. (2022). Revisiting the feasibility of public key cryptography in light of iiot communications. Sensors, 22(7), 2561.

[7] Akimova, O., Zhydovska, N., Kuchmiiova, T., Kozitska, N., & Buriak, I. (2024). Cyber Protection of Financial Data in Accounting: Implementation and Use of Cryptographic Techniques. Economic Affairs, 69(2), 1041-1052.

[8] Escobar, F. A., Canard, S., Laguillaumie, F., & Phan, D. H. (2024). Computational Differential Privacy for Encrypted Databases Supporting Linear Queries. Cryptology ePrint Archive.

[9] Bertino, E. (2016, June). Data security and privacy: Concepts, approaches, and research directions. In 2016 IEEE 40th annual computer software and applications conference (COMPSAC) (Vol. 1, pp. 400-407). IEEE.

[10] Prabhune, S., & Sharma, S. (2021, December). End-to-end encryption for chat app with dynamic encryption key. In 2021 3rd International Conference on Advances in Computing, Communication Control and Networking (ICAC3N) (pp. 1361-1366). IEEE.

[11] Velagala, N., Maglaras, L., Ayres, N., Moschoyiannis, S., & Tassiulas, L. (2022, June). Enhancing Privacy of Online Chat Apps Utilising Secure Node End-to-End Encryption (SNE2EE). In 2022 IEEE Symposium on Computers and Communications (ISCC) (pp. 1-3). IEEE.

[12] Patel, N. D., & Singh, A. (2023). Security Issues, Attacks and Countermeasures in Layered IoT Ecosystem. International Journal of Next-Generation Computing, 14(2).

[13] Galu, T. S., Adeyelu, A. A., & Otor, S. U. An Improved

Deffie Hellman Scheme for Mitigating an Eavesdropping Attack on a Network.

[14] de Carné de Carnavalet, X., & van Oorschot, P. C. (2023). A Survey and Analysis of TLS Interception Mechanisms and Motivations: Exploring how end-to-end TLS is made "end-to-me" for web traffic. ACM Computing Surveys, 55(13s), 1-40.

[15] Mosca, M. (2018). Cybersecurity in an era with quantum computers: Will we be ready?. IEEE Security & Privacy, 16(5), 38-41.

[16] Kumar, M., & Pattnaik, P. (2020, September). Post quantum cryptography (pqc)-an overview. In 2020 IEEE High Performance Extreme Computing Conference (HPEC) (pp. 1-9). IEEE.

[17] Döberl, C., Eibner, W., Gärtner, S., Kos, M., Kutschera, F., & Ramacher, S. (2023, August). Quantum-resistant end-to-end secure messaging and email communication. In Proceedings of the 18th International Conference on Availability, Reliability and Security (pp. 1-8).

[18] Mayer, P., Poddebniak, D., Fischer, K., Brinkmann, M., Somorovsky, J., Sasse, A., ... & Volkamer, M. (2022). " I {don't} know why I check this..."-Investigating Expert Users' Strategies to Detect Email Signature Spoofing Attacks. In Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022) (pp. 77-96).

[19] Di Nocera, F., Tempestini, G., & Orsini, M. (2023). Usable Security: A Systematic Literature Review. Information, 14(12), 641.

[20] Islam, M. (2023). A Practical Framework for Storing and Searching Encrypted Data on Cloud Storage. arXiv preprint arXiv:2306.03547.

[21] Starren, N., Schraffenberger, H., & Jacobs, B. (2022). Johnny can Encrypt? A Usability Study of IRMAseal.

[22] Rivest, R. (2016). Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications.

[23] Jarvis, C. (2020). Crypto wars: the fight for privacy in the digital age: A political history of digital encryption. CRC Press.

[24] Ruoti, S., Andersen, J., Dickinson, L., Heidbrink, S., Monson, T., O'neill, M., ... & Seamons, K. (2019). A usability study of four secure email tools using paired participants. ACM Transactions on Privacy and Security (TOPS), 22(2), 1-33.

[25] Koh, J. S., Bellovin, S. M., & Nieh, J. (2019, March). Why Joanie can encrypt: Easy email encryption with easy key management. In Proceedings of the Fourteenth EuroSys Conference 2019 (pp. 1-16).

[26] Guo, H., & Yu, X. (2022). A survey on blockchain technology and its security. Blockchain: research and applications, 3(2), 100067.

[27] Halder, R., Das Roy, D., & Shin, D. (2024). A Blockchain-Based Decentralized Public Key Infrastructure Using the Web of Trust. Journal of Cybersecurity and Privacy, 4(2), 196-222.

[28] Saju, S., Sabu, I. R., & Mary Anita, E. A. (2023, September). Certificate Generation and Validation Using Blockchain. In Congress on Intelligent Systems (pp. 275-282). Singapore: Springer Nature Singapore.

[29] Garcia, J. L. C., Udechukwu, I. P., Ibrahim, I. B., Chukwu, I. J., Dağ, H., Dimitrova, V., & Mollakuqe, E. (2024, June). Securing AI Systems: A Comprehensive Overview of Cryptographic Techniques for Enhanced Confidentiality and Integrity. In 2024 13th Mediterranean Conference on Embedded Computing (MECO) (pp. 1-8). IEEE.

[30] Bhandari, V., Bailey, R., & Rahman, F. (2021). Backdoors to Encryption: Analysing an Intermediary's Duty to Provide "Technical Assistance".

[31] Springer, J., & Haindl, P. (2024). Blockchain-based PKI within a Corporate Organization: Advantages and Challenges. arXiv preprint arXiv:2407.04536.

[32] Deng, Y., & Tang, H. (2024, May). Blockchain-based Anonymous Authentication Key Management for Mobile Edge Computing. In 2024 27th International Conference on Computer Supported Cooperative Work in Design (CSCWD) (pp. 2102-2109). IEEE.

[33] Yuan, B., & Wu, F. (2024). Application of Blockchain Based on Fabric Consensus Network Model in Secure Encryption of Educational Information. Applied Mathematics and Nonlinear Sciences, 9(1).

[34] Zhou, J., Fu, W., Hu, W., Sun, Z., He, T., & Zhang, Z. (2024). Challenges and Advances in Analyzing TLS 1.3-Encrypted Traffic: A Comprehensive Survey. Electronics, 13(20), 4000.

[35] Lou, J., Zhang, Q., Qi, Z., & Lei, K. (2018, August). A blockchain-based key management scheme for named data networking. In 2018 1st IEEE international conference on hot information-centric networking (HotICN) (pp. 141-146). IEEE.