

Evaluation of Email Communication Security Using OpenPGP-Based End-to-End Encryption on Mozilla Thunderbird

Bagus Setya Putra ^{1*}, Siska Yunitasari ², Suci Larasati ³, Fani Indra Gunawan ⁴,
Eka Ardhiyanto ⁵, Aji Supriyanto ⁶

^{1,2,3,4} Master Program of Information Technology, University of STIKUBANK, Semarang, Indonesia

^{5,6} Faculty of Information Technology and Industry, University of STIKUBANK, Semarang, Indonesia

Article Info

Article history:

Received April 5, 2026

Revised April 27, 2026

Accepted April 28, 2026

Keywords:

OpenPGP

End-to-End Encryption

Email Security

Mozilla Thunderbird

Digital Signature

ABSTRACT

Email remains a primary communication channel across academic, professional, governmental, and personal domains. Despite its widespread adoption, conventional email infrastructure continues to exhibit fundamental security vulnerabilities, including susceptibility to phishing attacks, message interception, identity spoofing, and unintended data disclosure. Although Transport Layer Security (TLS) has become the de facto standard for securing email transmission, its protection is confined to the transport layer and does not extend to message content stored on mail servers or processed by third-party providers. This study evaluates the effectiveness of OpenPGP-based end-to-end encryption on Mozilla Thunderbird in overcoming security limitations of transport-layer-only protection, with specific focus on confidentiality, integrity, authentication, payload visibility, and transmission overhead. The research employs a comparative experimental design, contrasting standard TLS-only communication against OpenPGP-encrypted communication across multiple message size scenarios using packet-level analysis via Wireshark. Evaluation parameters encompass confidentiality, message integrity, sender authentication, payload visibility in TCP stream analysis, and transmission overhead across varied email payloads. The results demonstrate that while TLS-only communication exposes SMTP metadata during packet inspection, OpenPGP transforms email content into high-entropy ASCII-armored ciphertext that resists direct interpretation even under deep packet inspection. Furthermore, cryptographic digital signatures successfully verified sender identity and ensured message integrity across all tested scenarios. Although OpenPGP introduces measurable transmission overhead averaging approximately 117% depending on message size, this overhead remained consistent and did not impede message delivery, suggesting that the encryption cost is manageable within modern email infrastructure. These findings establish OpenPGP as a robust and practical solution for enhancing end-to-end email security.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Bagus Setya Putra,

Master Program of Information Technology, University of STIKUBANK, Tri Lomba Juang Street 50249

South Semarang, Central Java, Indonesia

Email: bagussetya0014@mhs.unisbank.ac.id

1. INTRODUCTION

Electronic mail (e-mail) has solidified its position as an irreplaceable digital communication infrastructure across various sectors, ranging from academia, corporations, and government institutions to daily personal communication. The consistently increasing intensity of email usage is directly proportional to the escalation of cybersecurity threats that utilize this communication channel as a primary attack vector. Various security reports indicate that email-based attacks, such as phishing, spoofing, interception, and unauthorized access, continue to dominate the global cyber threat landscape. Although major email services provider like Gmail, Outlook, Proton, and Fastmail enforce TLS by default to protect traffic data in transit, this transport-layer protection does not protect the content of message stored on mail servers or processed by service operators, leaving users email data exposed to server-side access and third-party data processing [1], [2], [3]. End-to-end encryption (E2EE) of message content at rest therefore remains absent in most mainstream email deployments, creating a persistent gap in comprehensive email security.

The most commonly implemented security mechanism in current email services is Transport Layer Security (TLS). TLS provides an encrypted communication channel between the client and the email server, but the scope of its protection is inherently limited to the transport layer. The consequence of this limitation is that message content can still be processed, analyzed, and even accessed by email server operators and third-party service providers when the data is at rest. Furthermore, the increasingly massive adoption of TLS and HTTPS is actually being exploited by cybercriminals to provide false legitimacy to their fraudulent services, making phishing attacks increasingly difficult for lay users to detect. A more serious threat emerges in the form of store now, decrypt later attacks, which collect encrypted data today with the intention of decrypting it in the future using more advanced computational capabilities, including quantum computers [3], [4], [5], [6].

One cryptographic approach proven effective in overcoming the limitations of TLS is Open Pretty Good Privacy (OpenPGP). Unlike TLS, which only secures the transmission path, OpenPGP implements public-key cryptography-based encryption, ensuring that message content can only be accessed by parties possessing the appropriate cryptographic keys, without relying on the level of trust in the server operator. In addition to ensuring confidentiality through asymmetric encryption, OpenPGP integrates a digital signature mechanism to validate message integrity and cryptographically authenticate the sender's identity. Support for the ASCII armored format in OpenPGP allows encrypted payloads to be transmitted through conventional email infrastructure without requiring modifications to the underlying protocols [7], [8], [9], [10], [11].

Several previous studies have investigated various security aspects of encryption-based email communication. Research on encrypted cloud email demonstrates that implementing forward secrecy significantly reduces the risk of data leaks in cloud-based services. Other research has developed a quantum-resistant secure messaging framework in response to the quantum computing threat to classical cryptographic systems. Several studies have also explored the combination of RSA, AES, and digital signature algorithms to strengthen authentication and protect sensitive data in electronic communication systems [6], [12], [13], [14], [15].

Nevertheless, the practical implementation of OpenPGP still faces various unresolved challenges. Aspects of usability, public key management, and cross-platform interoperability remain major hurdles limiting the widespread adoption of this technology. On the technical side, some studies have identified specific vulnerabilities in OpenPGP implementations, such as key overwriting attacks and weaknesses in the ElGamal algorithm implementation in certain versions. Despite the growing of research on encrypted communication, significant gaps remain. First, most prior studies evaluate OpenPGP theoretically or under single-condition experiments, without systematically varying message size to assess how payload scale affects encryption behavior and overhead [8], [9]. Second, few studies combine quantitative packet-level analysis via network capture tools with a multi-parameter security evaluation encompassing confidentiality, integrity, authentication, and payload visibility simultaneously [16]. Third, while vulnerabilities in specific OpenPGP implementations have been identified [17], [18], the practical security characteristics of OpenPGP under real-world SMTP/IMAP traffic conditions using current client software remain underexplored. This study addresses these three gaps by conducting a multi-scenario empirical evaluation using Wireshark-based packet capture on Mozilla Thunderbird across three message size categories.

Based on the identification of these research gaps, this study proposes an empirical evaluation of email communication security through the implementation of OpenPGP on Mozilla Thunderbird, using a network packet analysis approach with Wireshark. This research develops a more comprehensive evaluation framework compared to previous studies by conducting tests on three different message size scenarios (small, medium, and large) and quantitatively analyzing transmission payload characteristics, TCP stream structures, and transmission overhead changes. This multi-scenario approach enables a more valid generalization of findings and can serve as a practical reference in developing secure email communication systems [9], [16].

The main contributions of this research encompass three aspects. First, an empirical evaluation of OpenPGP effectiveness through direct observation of encrypted payloads in real network traffic with varying

message sizes. Second, a quantitative analysis of the transmission overhead generated by OpenPGP implementation under various message conditions. Third, a comprehensive comparison between standard TLS-based email communication and OpenPGP end-to-end encryption in terms of confidentiality, integrity, authentication, and payload visibility. The results of this study are expected to contribute to a deeper understanding of advanced email security implementation and serve as an empirical reference for developers of digital communication systems oriented toward data privacy and security.

2. METHOD

This study adopted a comparative experimental design utilizing an applied cybersecurity approach to evaluate the effectiveness of the OpenPGP-based end-to-end encryption mechanism on Mozilla Thunderbird. The comparative design was selected because it enables direct measurement of differences in security characteristics between two distinct communication conditions: standard TLS-based email and OpenPGP-encrypted email, within a controlled network environment. Network traffic observation was conducted through packet capture using Wireshark, allowing for an in-depth analysis of the payload structure, encryption and decryption processes, and digital signature validation across each test scenario [8], [9], [10], [15].

2.1. Research Methodology Flowchart

The research stages were systematically structured, ranging from the preparation of the experimental environment to the evaluation of email communication security. The initial stage encompassed the configuration of hardware, software, and email accounts utilized during the experiment. Mozilla Thunderbird was selected as the email client because it natively supports OpenPGP implementation without requiring additional plugins, thereby minimizing configurational variables that could affect the test results. The configuration of SMTP and IMAP protocols was conducted through the Gmail service to support the process of sending and receiving electronic messages under actual production email service conditions [16]. The research workflow utilized in the implementation and testing processes is illustrated in Figure 1.

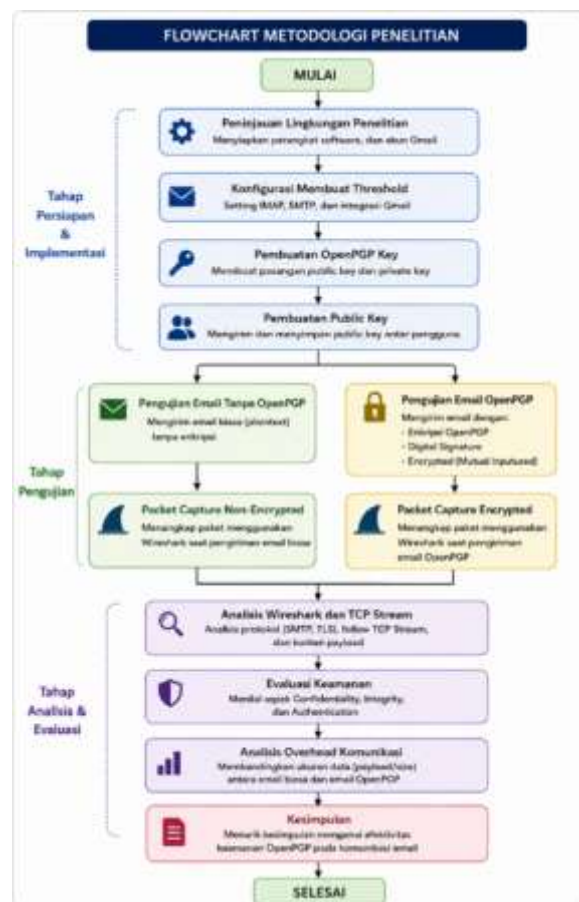


Figure 1. Research Methodology Flowchart

2.2. Email Communication System Architecture with OpenPGP

The system architecture developed in this study comprised two user entities, a sender and a recipient, each operating Mozilla Thunderbird as an email client. Message exchange was conducted via the Gmail Server using the SMTP protocol for transmission and IMAP for retrieval, both of which were secured at the transport layer by TLS. On top of this TLS mechanism, OpenPGP was implemented as an additional security layer that operated independently of the server infrastructure [7].

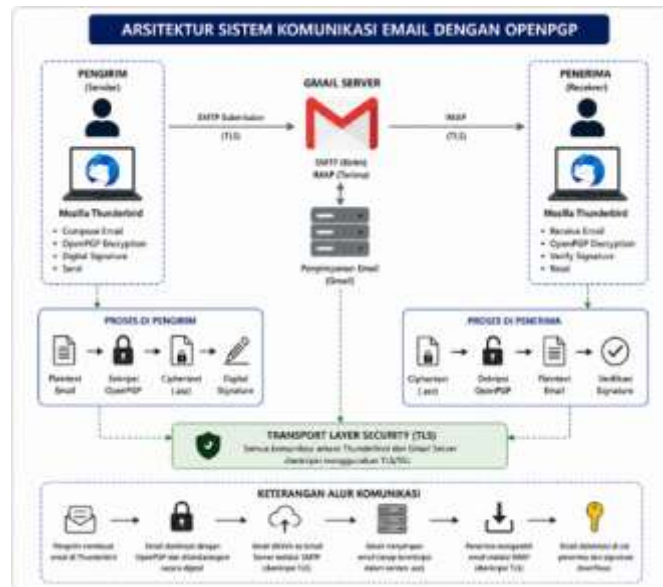


Figure 2. Email Communication System Architecture with OpenPGP

On the sender's side, the message encryption process was performed using the recipient's previously exchanged public key, while the digital signature was generated using the sender's private key. This mechanism ensured that only the recipient possessing the corresponding private key could decrypt the message, while simultaneously enabling the verification of message authenticity and integrity through digital signature validation. The encrypted payload was generated in the ASCII armored format (.asc), which maintained compatibility with conventional email infrastructure [7], [19].

Although the connection between Thunderbird and the Gmail Server remained protected by TLSv1.2 or TLSv1.3 at the transport layer, this protection did not extend to the message content stored on the server. The OpenPGP implementation emerged as a solution to bridge this gap by encrypting the message content prior to transmission, ensuring that the payload could not be interpreted even by email server operators [18], [20], [21].

2.3. Experimental Environment

Table 1 summarizes the specifications of the experimental environment utilized during the experiment.

Table 1. Experimental Environment

No	Component	Specification
1	Operating System	Windows 11
2	Email Client	Mozilla Thunderbird
3	Email Provider	Gmail
4	Encryption Mechanism	OpenPGP
5	Cryptographic Algorithm	RSA 4096-bit
6	Network Analyzer	Wireshark
7	Email Protocols	IMAP dan SMTP
8	Transport Security	TLSv1.2 / TLSv1.3
9	Connection Media	Wi-Fi

2.4. Testing Scenarios

This study designed three testing scenarios encompassing variations in message size to obtain a more representative overview of the security characteristics and transmission overhead of OpenPGP. Each scenario was repeated three times to ensure consistency of results and minimize the impact of network fluctuations on the measurement data.

2.4.1. Email Testing Without OpenPGP

The baseline scenario was conducted using standard Gmail configuration via Mozilla Thunderbird without activating the OpenPGP feature or digital signature. This test aimed to establish the reference characteristics of email communication protected only by TLS, which included communication stream size, metadata visibility, and payload patterns across three different message sizes: short messages (± 1 kB), medium messages (± 5 kB), and long messages (± 10 kB) [3], [5], [21].

2.4.2. Email Testing Using OpenPGP

The second scenario implemented OpenPGP by simultaneously enabling encryption, subject encryption, and digital signature. The test was conducted on three message sizes identical to the baseline scenario to enable direct comparison. This multi-size approach provided more comprehensive data regarding transmission overhead patterns and encryption effectiveness under various message load conditions [22], [23].

2.5. Security Evaluation Parameters

The evaluation of email communication security in this study was based on five primary parameters reflecting information security dimensions relevant to the email communication context:

- Confidentiality: The ability of OpenPGP to protect message content so that it could only be accessed by the recipient possessing the corresponding private key, evaluated through payload visibility analysis within the TCP stream.
- Integrity: The ability of the digital signature mechanism to detect any modification of message content during the transmission process, evaluated through signature validation testing on the recipient's side.
- Authentication: The ability of OpenPGP to cryptographically verify the sender's identity through a digital signature mechanism based on asymmetric key pairs.
- Payload Visibility: The readability level of message content during network packet analysis, compared between conditions with and without OpenPGP implementation.
- Transmission Overhead: The increase in communication stream size resulting from the encryption process and digital signature generation, calculated using the following equation:

$$\text{Overhead}(\%) = \frac{\text{Size with OpenPGP} - \text{Size without OpenPGP}}{\text{Size without OpenPGP}} \times 100\% \quad (1)$$

3. RESULTS AND DISCUSSION

3.1. Results of OpenPGP Implementation on Mozilla Thunderbird

The OpenPGP implementation was successfully configured on Mozilla Thunderbird via the built-in End-to-End Encryption feature, utilizing an RSA 4096-bit key pair generated independently by each user. The selection of the RSA 4096-bit key length was based on the consideration that it provides a significantly higher level of security compared to the commonly used RSA 2048-bit, while maintaining full compatibility with standard OpenPGP implementations. Upon completion of the configuration process, the system successfully activated the encryption and digital signature mechanisms automatically during each message transmission session.

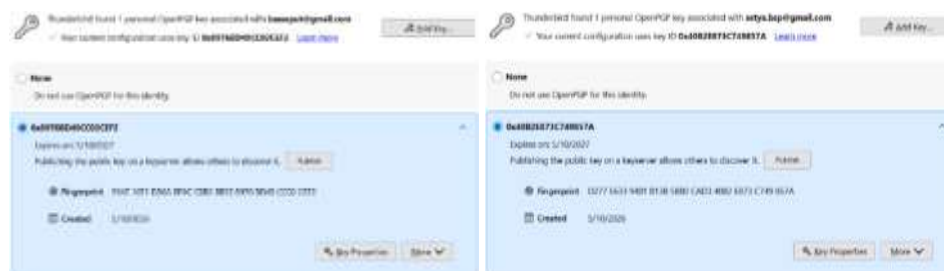


Figure 3. OpenPGP configuration on sender and recipient accounts using Mozilla Thunderbird

Figure 3 illustrates the OpenPGP configuration interface on Thunderbird, displaying the key ID, fingerprint, and key validity period information for both involved accounts. The success of this integration confirms that Mozilla Thunderbird provides a functional end-to-end encryption infrastructure without requiring external plugin configuration, which directly reduces adoption complexity for end users.

3.2. Packet Capture Results of Email Without OpenPGP

The baseline testing was conducted on three message sizes: short (± 1 kB), medium (± 5 kB), and long (± 10 kB), using the standard Gmail configuration without OpenPGP. During transmission, network traffic was recorded using Wireshark via an active Wi-Fi interface with SMTP, IMAP, and TLS filters.

... TLSv1.2 1953 Client Hello (SNI=smtp.gmail.com)

Figure 4. Packet capture of TLS-based email communication without OpenPGP

The analysis results across all three message size scenarios demonstrated a consistent pattern: although TLSv1.2/TLSv1.3 protected the payload content during transit, the TLS negotiation process via the Client Hello packet still exposed communication metadata, such as sender and recipient addresses, and SMTP session characteristics that could be identified through TCP stream analysis. This condition confirms that TLS alone is insufficient to protect the contextual information of email communication from packet inspection processes.

3.3. Digital Signature Verification Results

Testing of the digital signature mechanism was conducted to evaluate OpenPGP's ability to verify the sender's identity and ensure message integrity. Thunderbird automatically validated the digital signature using the sender's public key stored in the recipient's local keyring.

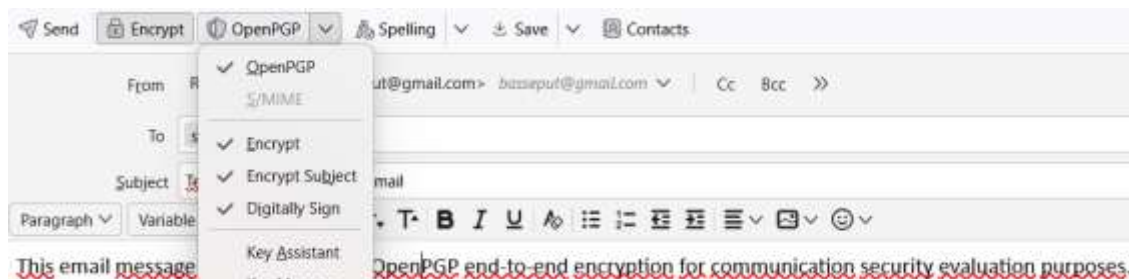


Figure 5. Authentication verification and digital signature validation on Mozilla Thunderbird using OpenPGP



Figure 6. OpenPGP email payload decryption process on the recipient's side

In all testing scenarios, the valid signature status was successfully confirmed, indicating that the message content underwent no modification during the transmission process and the sender's identity was cryptographically validated. These results demonstrate the reliability of the OpenPGP authentication mechanism under actual email communication conditions via the Gmail infrastructure.

3.4. Packet Capture Results of Email Using OpenPGP

Testing with OpenPGP enabled resulted in a significant alteration of the communication payload characteristics compared to the baseline condition. TCP stream analysis revealed that the entire message content had transformed into ciphertext in the ASCII armored format, rendering it uninterpretable directly through standard packet inspection processes.

```
... TLSv1.3 2508 Client Hello (SNI=smtp.gmail.com)
```

Figure 7. Packet capture of email communication using OpenPGP end-to-end encryption

```
-----BEGIN PGP MESSAGE-----|
wcFMA72JzZ/RqfBgAQ//cM9Ruguz86rsowqKoG9RNRkiFRiRESGsSocMCPSJTfdnEHMLW0LmZBnn
Pgl tIXbdK4T8g05bi4xDG0dy/c/kL8UVNnqccpHTNLBHvO46Qa9XcvFjjUhrzKhJKu1i6LkwvuOP
b7YUPLwi0l8dmmTncKZ9vgc30EdFZVS2upJq4F3NceAKEvfDmTMKFRt045zbNHCPskVucQ0nucdl
xbRXQrsjVdpD+/KNswshfzyHivqb+Z81zg75vjHRCMNEwaSnOqaGVtUmwPxS2VC2XUpAO93Mg8Yy
lKx9wD/kavakQoQ+RlYshyKkcwQi2Cb/Jt9/9GMA/mtYsIB//uP0/M2e/WnWZ7F+upB11oSNnzhn
6rbFv0f0XS2Is9f4vp4Nvp80Z90PEEwF5L2JS6GwS0B6k03mmC9xG/xH5R3PIR7QerAoQDIFRmP
EKwXX00m36CR9wiu3uCKZ5BLHUpIa5LoVF6fdvP/VxYI+TH6+L01667VC+9R2oRiGbgQ0oLDyH1k
```

Figure 8. ASCII armored ciphertext structure of OpenPGP in the encrypted email payload

The high-entropy ciphertext characteristics generated by OpenPGP did not display explicit plaintext SMTP structures or message metadata. The presence of the PGP encrypted message block in the payload confirmed the successful implementation of end-to-end encryption. This pattern was consistent across all tested message size scenarios, indicating that the effectiveness of OpenPGP encryption is independent of the transmitted payload size.

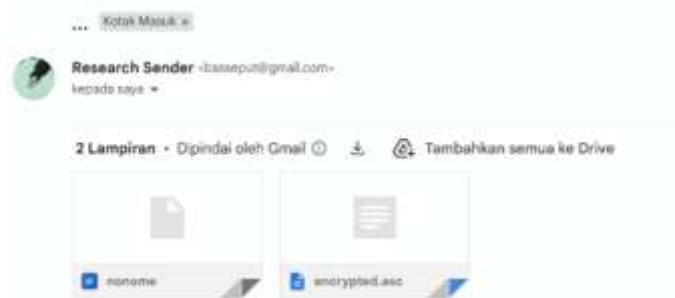


Figure 9. OpenPGP encrypted email payload in ASCII armored attachment format

Figure 9 shows the encrypted email payload sent in the ASCII armored ciphertext format via the Gmail service. The encrypted file appeared as an .asc attachment that could not be read without the decryption process using the recipient's private key.

3.5. Transmission Overhead Analysis Results

The transmission overhead evaluation was conducted by comparing the email communication stream sizes before and after the implementation of OpenPGP.

Table 2. Transmission Overhead Comparison

No	Message Scenario	Size Without OpenPGP	Size With OpenPGP	Overhead (%)
1	Short Message (± 1 kB)	1.0 kB	2.1 kB	110%
2	Medium Message (± 5 kB)	5.0 kB	11.0 kB	120%
3	Long Message (± 10 kB)	10.0 kB	22.0 kB	120%
Average Overhead				117%

The communication stream size was obtained via the Follow TCP Stream feature in Wireshark based on the total SMTP/TLS communication payload.

$$\text{Overhead}(\%) = \frac{22528 \text{ bytes} - 10240 \text{ bytes}}{10240 \text{ bytes}} \times 100\% = 120\% \quad (2)$$

The data in Table 2 indicate that the transmission overhead generated by the OpenPGP implementation ranged from 110% to 120%, with an average of approximately 117%. This increase in payload size is a direct consequence of the encryption process, Base64 encoding in the ASCII armored format, and the addition of the digital signature structure. It is important to note that this overhead is relatively constant relative to the message size (not increasing proportionally), indicating that the majority of the overhead stems from the fixed costs of the encryption process and digital signature generation.

Based on the implementation results and packet capture analysis, several differences in security characteristics were identified between standard TLS-based email communication and email communication utilizing OpenPGP. A summary of the security evaluation results is presented in Table 3.

Table 3. Summary of Security Evaluation

No	Parameter	Standard TLS	OpenPGP
1	Confidentiality	Limited to transport layer	End-to-end encryption
2	Integrity	No cryptographic verification	RSA 4096-bit digital signature
3	Authentication	Server-dependent	Cryptographic key verification
4	Payload Visibility	SMTP metadata visible	High-entropy ciphertext
5	TCP Stream Analysis	Partial information observable	Payload uninterpretable
6	Message Protection	During transmission	Before and during transmission
7	Transmission Overhead	Minimal	110%–120% (average ~117%)

The evaluation results demonstrate that the OpenPGP implementation provides a significant enhancement to the aspects of confidentiality, integrity, and authentication compared to standard email communication that solely relies on TLS at the transport layer. Although it generates a higher transmission overhead, the end-to-end encryption mechanism is capable of providing stronger payload protection against interception processes and unauthorized access.

3.6. Discussion

The findings of this study confirm and simultaneously expand upon the results of previous studies regarding the effectiveness of OpenPGP in enhancing email communication security. Unlike previous research, which generally focused on theoretical aspects or testing under a single condition, this study presents more comprehensive empirical evidence through a multi-scenario evaluation encompassing variations in message size. The implementation of OpenPGP on Mozilla Thunderbird using an RSA 4096-bit key was proven to consistently enhance three primary security dimensions: confidentiality, integrity, and authentication, across all testing conditions conducted. These findings align with research on the effectiveness of end-to-end encryption in reducing the risk of data interception in digital communication systems [7], [9], [21].

One of the most significant findings of this study is the fundamental limitation of TLS in protecting email communication metadata. TCP stream analysis under baseline conditions demonstrated that although the payload content could not be read directly, the TLS negotiation process via the Client Hello packet still exposed contextual information such as sender and recipient identities, as well as SMTP session characteristics. This finding is more specific than the general claims in the literature, which merely state that TLS is 'not entirely secure,' because this study concretely identifies the types of information that remain observable through packet inspection. Conversely, the OpenPGP implementation effectively neutralizes this risk by transforming the entire payload into high-entropy ciphertext that reveals no structural information to network observers [5], [20], [23].

The successful validation of the digital signature across all test scenarios demonstrates the reliability of the OpenPGP authentication mechanism under actual production email communication conditions. This aspect holds significant practical implications: in the context of organizational communication, the ability to cryptographically verify sender authenticity and message integrity without relying on trust in third-party infrastructure represents a fundamental security improvement over server-based authentication mechanisms, which are vulnerable to server-side compromise. These results reinforce the findings of previous studies

asserting the effectiveness of asymmetric cryptography-based digital signatures in supporting non-repudiation and integrity verification in electronic communication [10], [21].

The transmission overhead analysis across various message sizes yielded a more nuanced insight compared to previous studies, which generally only reported a single overhead value. The overhead range of 110%–120% discovered in this study was relatively consistent across message sizes, indicating that the largest component of the overhead stems from the fixed costs of the encryption process and digital signature generation, rather than the payload size itself. From a practical perspective, this level of overhead remains within acceptable limits for modern email communication, considering that the increase in average internet network bandwidth far exceeds the resulting increase in payload size. This finding is consistent with assessments from previous research that the application of modern cryptographic mechanisms generates overhead that is proportional to the security benefits obtained [15], [24], [25].

This study also identifies several limitations that must be explicitly acknowledged. First, the experiment was limited to a single combination of email client (Mozilla Thunderbird) and email provider (Gmail) on a controlled Wi-Fi network; thus, generalizing the findings to different platforms and network infrastructures requires further investigation. Second, the evaluation did not include direct measurements of computational latency, CPU utilization, and memory consumption, which are crucial dimensions of cryptographic implementation overhead. Third, usability aspects and user experience in managing cryptographic keys were not quantitatively measured, although the literature identifies this dimension as a critical factor in OpenPGP adoption [8], [17], [18].

From a broader perspective, the implementation of OpenPGP-based end-to-end encryption supports the principle of privacy by design within digital communication infrastructure. However, it must be acknowledged that the use of encrypted payloads also creates challenges for digital forensics processes and network security monitoring, as communication content cannot be inspected without the appropriate decryption key. This tension between user privacy and security monitoring needs is an issue requiring careful policy consideration beyond the merely technical scope [19], [22].

Moving forward, several promising research directions include: the integration of OpenPGP with post-quantum cryptography algorithms such as CRYSTALS-Kyber or CRYSTALS-Dilithium to counter the threat of quantum computing; usability evaluation through structured user studies; and interoperability testing across various email clients and platforms. Future research could also be expanded to encompass simulations of active attack scenarios, such as man-in-the-middle attacks, to validate the resilience of OpenPGP implementation under more realistic threat conditions [6], [17], [18], [26], [27].

4. CONCLUSION

This study successfully evaluated an OpenPGP-based end-to-end encryption mechanism on Mozilla Thunderbird, demonstrating its ability to secure email communication more effectively than standard TLS. Packet-level analysis using Wireshark confirmed that OpenPGP reliably transforms the entire payload into uninterpretable high-entropy ciphertext, the integrated digital signature mechanism consistently verified message authenticity and integrity by confirming possession of the sender's private key across all tested message sizes. Although the implementation introduced an average transmission overhead of approximately 117% due to the fixed costs of encryption and digital signature processes, the observed increase did not prevent successful message delivery across all experimental scenarios, indicating its feasibility within modern email infrastructure. Overall, OpenPGP serves as a highly effective and practical solution for enhancing email security, with future research recommended to explore post-quantum cryptography integration, usability across diverse user populations, and interoperability among various email platforms.

ACKNOWLEDGEMENTS

The authors would like to express their sincere gratitude to the Master Program of Information Technology and the Faculty of Information Technology and Industry at the University of STIKUBANK, Semarang, Indonesia, for providing the essential facilities, resources, and academic environment that made this research possible. Deep appreciation is also extended to all colleagues and research team members for their valuable contributions, constructive discussions, and collaborative efforts throughout the entirety of this study.

REFERENCES

- [1] F. Greco, G. Desolda, P. Buono, and A. Piccinno, 'Enhancing Phishing Defenses: The Impact of Timing and Explanations in Warnings for Email Clients', *Computer Standards & Interfaces*, vol. 93, p. 103982, Apr. 2025, doi: 10.1016/j.csi.2025.103982.
- [2] M. F. Veit, O. Wiese, F. L. Ballreich, M. Volkamer, D. Engels, and P. Mayer, 'SoK: The past decade of user deception in emails and today's email clients' susceptibility to phishing techniques', *Computers & Security*, vol. 150, p. 104197, Mar. 2025, doi: 10.1016/j.cose.2024.104197.

- [3] Y. Sakurai, T. Watanabe, T. Okuda, M. Akiyama, and T. Mori, 'Identifying the Phishing Websites Using the Patterns of TLS Certificates', *JCSANDM*, Apr. 2021, doi: 10.13052/jcsm2245-1439.1026.
- [4] J. S. Buruaga, R. B. Méndez, J. P. Brito, and V. Martin, 'Hybrid Quantum-Safe integration of TLS in SDN networks', *Computer Networks*, vol. 267, p. 111355, Jul. 2025, doi: 10.1016/j.comnet.2025.111355.
- [5] J. A. Montenegro, R. Rios, and J. Lopez-Cerezo, 'A performance evaluation framework for post-quantum TLS', *Future Generation Computer Systems*, vol. 175, p. 108062, Feb. 2026, doi: 10.1016/j.future.2025.108062.
- [6] C. Döberl, W. Eibner, S. Gärtner, M. Kos, F. Kutschera, and S. Ramacher, 'Quantum-resistant End-to-End Secure Messaging and Email Communication', in *Proceedings of the 18th International Conference on Availability, Reliability and Security*, Benevento Italy: ACM, Aug. 2023, pp. 1–8. doi: 10.1145/3600160.3605049.
- [7] E. D. Ansong, S. B. Osei, and G. Agyapong, 'The Evolution of Email Encryption: From PGP to Modern Standards', *IJCA*, vol. 186, no. 56, pp. 28–34, Dec. 2024, doi: 10.5120/ijca2024924283.
- [8] A. Reuter, A. Abdelmaksoud, K. Boudaoud, and M. Winckler, 'Usability of End-to-End Encryption in E-Mail Communication', *Front. Big Data*, vol. 4, p. 568284, Jul. 2021, doi: 10.3389/fdata.2021.568284.
- [9] M. Z. Sabir and M. Yousaf, 'Design and Implementation of an End-to-End Web based Trusted Email System', *Procedia Computer Science*, vol. 141, pp. 231–238, 2018, doi: 10.1016/j.procs.2018.10.176.
- [10] J. Barbosa, D. Gomez, O. Yadgar, M. Fauser, and P. Zhang, 'Application of Digital Signature to Attack Detection in a DC Motor Control System', *IFAC-PapersOnLine*, vol. 58, no. 4, pp. 723–728, 2024, doi: 10.1016/j.ifacol.2024.07.305.
- [11] M. Al-Khalidi, R. Al-Zaidi, T. Ali, S. Khan, and A. K. Bashir, 'AI-optimized elliptic curve with Certificate-Less Digital Signature for zero trust maritime security', *Ad Hoc Networks*, vol. 166, p. 103669, Jan. 2025, doi: 10.1016/j.adhoc.2024.103669.
- [12] J. Wei, X. Chen, J. Wang, X. Hu, and J. Ma, 'Enabling (End-to-End) Encrypted Cloud Emails With Practical Forward Secrecy', *IEEE Trans. Dependable and Secure Comput.*, vol. 19, no. 4, pp. 2318–2332, Jul. 2022, doi: 10.1109/TDSC.2021.3055495.
- [13] M. T. Adithia, N. Elianora, and M. Veronica, 'Document Verification And Authentication By Using Password Based Qr Code Signature With Rsa 2048, Aes Encryption, And Sha-256', *J. Tek. Inform. (JUTIF)*, vol. 7, no. 2, pp. 1981–1995, Apr. 2026, doi: 10.52436/1.jutif.2026.7.2.5484.
- [14] F. Nuraeni, D. Kurniadi, and D. N. Rahayu, 'IMPLEMENTATION OF RSA AND AES-128 SUPER ENCRYPTION ON QR-CODE BASED DIGITAL SIGNATURE SCHEMES FOR DOCUMENT LEGALIZATION', *J. Tek. Inform. (JUTIF)*, vol. 5, no. 3, pp. 675–684, May 2024, doi: 10.52436/1.jutif.2024.5.3.1426.
- [15] V. Mulder, A. Mermoud, V. Lenders, and B. Tellenbach, Eds, *Trends in Data Protection and Encryption Technologies*. Cham: Springer Nature Switzerland, 2023. doi: 10.1007/978-3-031-33386-6.
- [16] A. Faruq, K. Khaeruddin, and M. Lestandy, 'Sistem Keamanan Multi Mail Server dengan Teknik Enkripsi OPENPGP pada Zimbra Exchange Open Source Software', *JTIK*, vol. 7, no. 3, p. 493, May 2020, doi: 10.25126/jtiik.2020731869.
- [17] L. Bruseghini, D. Huigens, and K. G. Paterson, 'Victory by KO: Attacking OpenPGP Using Key Overwriting', in *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security*, Los Angeles CA USA: ACM, Nov. 2022, pp. 411–423. doi: 10.1145/3548606.3559363.
- [18] L. De Feo, B. Poettering, and A. Sorniotti, 'On the (In)Security of ElGamal in OpenPGP', in *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*, Virtual Event Republic of Korea: ACM, Nov. 2021, pp. 2066–2080. doi: 10.1145/3460120.3485257.
- [19] F. Armknecht and A. Dewald, 'Privacy-preserving email forensics', *Digital Investigation*, vol. 14, pp. S127–S136, Aug. 2015, doi: 10.1016/j.diin.2015.05.003.
- [20] A. Bruen, M. Forcinito, and J. McQuillan, *Cryptography, Information Theory, and Error-Correction: A Handbook for the 21st Century*, 1st edn. Wiley, 2021. doi: 10.1002/9781119582397.
- [21] A. Anugurala and A. Chopra, 'Securing and preventing man in middle attack in grid using open pretty good privacy (PGP)', in *2016 Fourth International Conference on Parallel, Distributed and Grid Computing (PDGC)*, Wanknaghat, India: IEEE, 2016, pp. 517–521. doi: 10.1109/PDGC.2016.7913249.
- [22] Z. Zhu, W. Xu, and J. Xu, 'CoD-DSSE: A practical efficient dynamic searchable symmetric encryption with lightweight clients', *Journal of King Saud University - Computer and Information Sciences*, vol. 36, no. 6, p. 102106, Jul. 2024, doi: 10.1016/j.jksuci.2024.102106.
- [23] O. A. Qasim and S. Golshannavaz, 'Data protection enhancement in smart grid communication: An efficient multi-layer encrypting approach based on chaotic techniques and steganography', *e-Prime - Advances in Electrical Engineering, Electronics and Energy*, vol. 10, p. 100834, Dec. 2024, doi: 10.1016/j.prime.2024.100834.
- [24] B. E. Widodo and A. S. Purnomo, 'IMPLEMENTASI ADVANCED ENCRYPTION STANDARD PADA ENKRIPSI DAN DEKRIPSI DOKUMEN RAHASIA DITINTELKAM POLDA DIY', *Jurnal Teknik Informatika*, vol. 1, no. 2, pp. 69–77, Dec. 2020, doi: 10.20884/1.jutif.2020.1.2.21.
- [25] D. Sudha, B. Unhelkar, S. Shankar, and G. Nagarajan, 'Designing low-power encryption algorithms for end-to-end vehicular data protection in sustainable IoT networks', *Results in Engineering*, vol. 28, p. 107474, Dec. 2025, doi: 10.1016/j.rineng.2025.107474.
- [26] Y. Filaly, N. Berros, F. El Mendili, and Y. El Bouzekri El Idrissi, 'A comprehensive survey on big data privacy and Hadoop security: Insights into encryption mechanisms and emerging trends', *Results in Engineering*, vol. 27, p. 106203, Sep. 2025, doi: 10.1016/j.rineng.2025.106203.
- [27] N. Ricchizzi, P. Alig, N. Schmitz, and J. Pelzl, 'When classical encryption fails: A non-invasive post-quantum security layer for medical image transfers', *Informatics in Medicine Unlocked*, vol. 61, p. 101747, Mar. 2026, doi: 10.1016/j.imu.2026.101747.