Development of a Secure Encrypted Communication System for Business Teams

Paulo NUHAJ[1]

Agim KASAJ

Abstract

In today's world, technology has advanced to such an extent that large companies and organizations increasingly rely on digital platforms to conduct their internal communication. These platforms often advertise the latest technological methods they employ, yet many of them have not placed communication security as a primary focus, leaving room for various risks such as eavesdropping, third-party interference, and data leakage. This situation is also evident in the Albanian context, where many companies face serious challenges in securing their internal communication.

Considering this problem, the objective of this project is to develop a dedicated and reliable platform for secure communication within an organization. The proposed solution is the creation of a protected environment for information exchange among company members, while adhering to the fundamental principles of information security: confidentiality, integrity, and availability of data.

The architecture of this platform has been designed using React.js for the user interface, while Node.js and Express.js were employed for the backend.

[1] Paulo Nuhaj has completed his Bachelor studies in Software Engineering at the European University of Tirana. He continued his academic path at the same institution, earning a Master of Science degree in Computer Engineering with a specialization in Cybersecurity. His research interests include secure communication systems, encryption technologies, and the design of digital platforms that enhance cybersecurity awareness and provide practical tools for improving information security practices.

Data management is handled through MongoDB. What makes this platform secure is the implementation of end-to-end encryption (E2EE), where messages are encrypted using the AES-GCM (Advanced Encryption Standard - Galois/ Counter Mode) algorithm, while the corresponding keys are encrypted with RSA-4096. During registration, each user generates an RSA key pair, and the private key is stored in encrypted form using a symmetric key derived from the user's password through the bcrypt algorithm. The platform also includes multi-factor authentication (2FA), where the user receives a unique code via email to complete the login process. This project was initiated with the aim of providing a solution to the communication security challenges faced by companies operating under high security standards.

***Keywords**: End-to-end encryption, Albania, Cybersecurity, Institutions, Threats, Risk Management.*

Introduction

With the continuous evolution of information technology, communication among business employees increasingly takes place through digital platforms. This development has made information security a fundamental challenge of today. Companies frequently face diverse threats, including the eavesdropping of communications, third-party intrusions, and the leakage of confidential data. This situation is also evident in the Albanian context, where the lack of dedicated and secure platforms for internal communication remains an ongoing issue. Based on these challenges, this project aims to create a secure system for encrypted communication in business teams, ensuring the confidentiality, integrity, and availability of information. By leveraging modern technologies and advanced security practices, the project seeks to establish a communication environment that meets the real needs of contemporary companies for data protection.

On many platforms, end-to-end encryption (E2EE) is still absent, creating the risk that data may be read or decrypted during transmission, whether by third parties or even by the service providers themselves. This is a serious concern for information security, particularly when sensitive organizational data is involved.

In addition, many users continue to rely on weak passwords and do not enable multi-factor authentication (MFA), making it easier for attackers to gain access to accounts. In the absence of activity logging and proper access control, it becomes increasingly difficult to determine who performed which actions in the event of an incident. Another common issue is the sharing of sensitive files without any

form of protection, such as encryption or restrictions on time and conditions of access. This exposes the organization to the risk of data leakage, especially when external tools are used for communication or storage.

Taking all these risks into account, the creation of a secure and centralized platform for internal communication is essential. Such a system should integrate E2EE, MFA, secure file storage, and activity auditing. This would help any organization preserve the confidentiality and integrity of the information it possesses.

The primary objective of this project is to design and develop a secure platform for internal communication within companies, ensuring a high level of protection for the exchange of information among users inside the organization. At a time when cyber threats are on the rise and many existing communication platforms fail to provide adequate safeguards against intrusions or data breaches, this project aims to deliver a solution that guarantees confidentiality, integrity, and authentication of communication.

The platform is intended to include advanced functionalities such as multi-factor authentication (MFA), end-to-end encryption (E2EE) for both messages and files, encrypted file sharing, automatic deletion of sensitive messages, and auditing of critical user activities. Through this work, the aim is not only to build a functional and practical system but also to demonstrate the application of modern security methods in the development of collaborative applications. Ultimately, the platform will serve as a clear example of how modern technologies can be combined with best security practices to create a safe digital environment for internal company communication.

To achieve the objective of this study and to provide clear results and answers, a set of research questions has been formulated, serving as key points in the design and implementation of this work:

- How does the use of end-to-end encryption (E2EE) contribute to ensuring the confidentiality of internal communication within companies?
- Does multi-factor authentication (MFA) improve access security in the internal communication platform?
- What are the advantages and technical challenges of implementing a centralized platform with advanced security functionalities (auditing, secure file storage)?
- How do users perceive the use of such a secure platform compared to existing communication platforms (e.g., email, external applications)?
- How does activity auditing contribute to increasing traceability and transparency in the use of the system?

This paper is organized into several main sections that present the key components of the research and the development of the proposed platform.

- Section 1 – Introduction presents the background of the topic, its relevance, and the objectives of the study. It also outlines the research questions, the hypothesis, the methodology, and the overall structure of the paper.
- Section 2 – Literature Review reviews existing literature and best practices related to digital communication security, including end-to-end encryption, multi-factor authentication, and other security mechanisms.
- Section 3 – Methodology describes the research methodology and the approach used for the development of the platform. It explains the technologies applied, the development process, and the testing procedures used to evaluate the system.
- Section 4 – Methods and analysis present the architecture of the system, the implemented functionalities, and the security mechanisms integrated into the platform. It also explains how the platform operates.
- Section 5 – Conclusions and Recommendations summarize the main findings of the study and provides recommendations for future improvements and further research in this field.

2. Literature Review

The security of digital communication has been widely discussed in academic and professional literature, as organizations increasingly rely on digital platforms for collaboration and information sharing. According to Stallings (2022), communication security is founded on the principles of confidentiality, integrity, and availability, which remain the cornerstone of modern information systems. Shannon's early theories of communication security (1949) provide the theoretical basis for understanding how encryption ensures the protection of data against unauthorized access.

One of the most effective mechanisms highlighted in recent studies is **End-to-End Encryption (E2EE)**. Diffie and Hellman (1976) introduced the concept of public key cryptography, which underpins E2EE, ensuring that only the sender and recipient can access the communication content. Modern implementations, such as AES-GCM and RSA-4096, are considered industry standards due to their robustness against brute-force attacks (Anderson, 2020). Research also emphasizes that while E2EE offers strong protection, challenges remain regarding key management and usability for non-technical users (ENISA, 2023).

Another crucial mechanism is **Multi-Factor Authentication (MFA)**. As highlighted by the National Institute of Standards and Technology (NIST, 2020), MFA significantly reduces the risk of unauthorized access by requiring multiple

credentials beyond a password. Academic and industry reports agree that the combination of something the user knows (password), something the user has (token, email code), and something the user is (biometric data) provides a higher assurance level for identity verification.

Beyond encryption and authentication, literature stresses the importance of **auditing and secure file management**. According to Bishop (2018), system auditing improves traceability and accountability, which are essential for detecting anomalies and responding to incidents. Similarly, secure storage and controlled file sharing are recognized as fundamental to preventing data leakage in organizational environments (ENISA, 2023).

International practices also demonstrate the necessity of combining technological and organizational measures. Frameworks such as the NIST Cybersecurity Framework and the EU Cybersecurity Strategy highlight the importance of user awareness, continuous monitoring, and compliance with standards. These approaches serve as valuable references for the design of secure communication platforms.

In conclusion, the literature highlights that E2EE, MFA, auditing, and secure file management represent the most effective practices for ensuring secure internal communication. However, challenges related to usability, adoption, and institutional awareness remain open issues, especially in contexts such as Albania where cybersecurity culture is still developing.

Methodology

This research adopts a practical and applied approach, combining theoretical insights from existing literature with the development of a functional prototype for secure internal communication. The purpose of this methodology is to design, implement, and evaluate a platform that demonstrates how advanced security mechanisms can be integrated into a collaborative digital environment.

Research Approach

The study followed a design-oriented methodology. First, a literature review was conducted to identify the best practices in communication security, focusing on end-to-end encryption (E2EE), multi-factor authentication (MFA), auditing, and secure file storage. Based on these findings, the project was developed using an iterative development model, allowing continuous refinement of features and security mechanisms.

System Design and Technologies

The platform architecture was built using modern web technologies:

- **Frontend:** React.js for the user interface, ensuring interactivity and usability.
- **Backend:** Node.js with Express.js for secure communication handling and API services.
- **Database:** MongoDB for storing user data and encrypted file metadata.

For security mechanisms, AES-GCM was implemented for symmetric encryption of messages, while RSA-4096 was used to encrypt session keys. Private keys were securely stored using password-derived symmetric encryption with bcrypt. In addition, the platform incorporated email-based two-factor authentication (2FA) to strengthen access security.

Development Process

The system was built iteratively. Each component—authentication, message encryption, file sharing, and auditing—was implemented and tested individually. Unit and functional tests ensured that components worked as expected. Basic penetration testing was also conducted to evaluate the platform's resilience against unauthorized access attempts.

Evaluation and User Feedback

To assess usability and effectiveness, the platform was tested by a small group of users who provided feedback on functionality, ease of use, and perceived security. Their insights helped refine the user interface and improve security workflows, particularly around authentication and message handling.

Summary

The chosen methodology ensured a balance between theoretical grounding and practical implementation. By combining secure architectural design, rigorous testing, and user validation, the study demonstrates the feasibility of building a secure, user-friendly communication system tailored to organizational needs.

Methods and Analysis

Security of Digital Communication

Rapid technological advances and pervasive online platforms have increased exposure to sophisticated threats such as malware, ransomware, phishing, and data-exfiltration attacks (Anderson, 2020). ENISA (2023) reports that 81% of European businesses have faced incidents compromising internal communications, underscoring the need to combine strong encryption, access controls, and monitoring. Foundational work by Shannon (1949) established encryption to protect data in transit; Diffie and Hellman (1976) later introduced public-key cryptography, now central to secure online communications. Modern security systems must also provide authentication, message integrity, anti-replay protection, and session management (Stallings, 2022). Group-messaging security adds complexity: protocols such as the Signal Group Protocol focus on forward secrecy and post-compromise security amid dynamic membership (Cohn-Gordon et al., 2020). Effective programs integrate symmetric and asymmetric encryption, MFA, strong access controls, and continuous monitoring/auditing (Reddy & Rajendran, 2024). Technology alone is insufficient without clear policies and user education (Garfinkel, 2003). Contemporary architectures increasingly adopt **Zero Trust**, avoiding implicit trust even inside organizational networks (Kaufman et al., 2019). Ultimately, success depends on technology, processes, and culture working together (Von Solms & Van Niekerk, 2013).

End-to-End Encryption (E2EE)

E2EE ensures that only senders and recipients can access message content, excluding intermediaries, including service providers. In enterprise E2EE, encryption occurs on the user device, protecting data at rest and in transit; private keys remain inaccessible to providers/admins and should be securely stored on user-controlled devices (Paterson & Poettering, 2022).

The Signal Protocol combines public-key and symmetric cryptography. Using ECDH on Curve25519 to establish a shared secret, it derives session keys for message encryption/authentication and calls (e.g., AES-256 and HMAC-SHA256), achieving strong security guarantees (Karbasi, 2021).

AES-256 (NIST, 2001; FIPS 197, 2001) is widely standardized, hardware-accelerated, and resistant to brute force, making it a core building block for E2EE. **HMAC-SHA-256** provides efficient integrity and authentication and is recommended by international standards (FIPS 198-1, 2008; Grassi et al., 2017).

Modern platforms (e.g., Signal, WhatsApp) pair AES-GCM with Curve25519 to scale E2EE to large user bases (Cohn-Gordon et al., 2020). Users must still manage devices/keys responsibly; usability and operational practices are crucial to realizing E2EE's benefits. Ongoing cryptographic advances continue to strengthen E2EE against evolving threats.

Multi-Factor Authentication (MFA)

MFA verifies identity using at least two factor categories—something known (password), something possessed (token), and something inherent (biometric)—substantially reducing unauthorized access. Large-scale measurements show MFA can cut account-takeover risk by orders of magnitude (Meyer et al., 2023; Microsoft, 2022). In cloud and **Zero Trust** settings, MFA is now a standard control, though design must balance security and usability (Alotaibi, 2022; Bonneau et al., 2012). SMS codes remain common but are weaker due to SIM-swapping and interception risks; authenticator apps and biometrics offer stronger protection (Grassi et al., 2017). Adaptive MFA, which adjusts requirements based on context and behavior, is increasingly prevalent (Alotaibi, 2022).

Token Presence (Physical/Digital)

Tokens (smartcards, hardware keys, smartphones, or software OTPs) provide possession proof; radio interfaces (e.g., NFC/Bluetooth) or TOTP apps enable deployment. Combined with other factors, tokens significantly raise attack cost (Ometov et al., 2018).

Voice Biometrics

Voice-based factors leverage microphones ubiquitously on modern devices. Because AI can synthesize/imitate voices, voice biometrics should be combined with other factors (Ometov et al., 2018).

Facial Recognition

Face recognition has matured from easily spoofed 2D checks to more robust 3D/liveness approaches, yet privacy concerns and deepfake risks persist; best practice is to use it within a multi-factor scheme (Ometov et al., 2018).

Ocular Biometrics (Iris/Retina)

Iris/retina patterns are highly stable and hard to imitate; IR-based imaging supports accurate matching, though specialized sensors and controlled environments are often required (Rasheed et al., 2023; Springer, 2022).

Hand Geometry

Convenient but less accurate than fingerprints/vein patterns; environmental factors affect reliability, so it is best used as part of MFA (Guillen et al., 2012).

Vein Recognition

Vein patterns are difficult to copy, but spoofing remains possible without anti-spoofing measures; robust liveness checks are necessary (Tome et al., 2014).

Fingerprints

Ubiquitous and easy to deploy but vulnerable to presentation attacks should be combined with other factors (MSU & NYU, 2018; Liu et al., 2023).

Behavioral Biometrics

Keystroke dynamics, mouse/touch patterns, and motion sensors can provide continuous, unobtrusive authentication and anomaly detection, reducing reliance on OTPs (Wahab et al., 2023; Sharma & Elmiligi, 2022).

ECG Recognition

ECG signals are inherently live and individual-specific, offering strong anti-spoofing potential; practical deployment requires suitable sensors and robust signal processing (Al Alfi et al., 2025; Narain Singh & Singh, 2012; Liu et al., 2023).

EEG Recognition

EEG-based biometrics can achieve high accuracy with lightweight models and may even be "revocable" by changing stimuli or mental states; sensor practicality and signal variability remain challenges (Hossain et al., 2022; Al Alfi et al., 2025).

Summary of MFA

MFA is one of the strongest controls for access security; maximum effectiveness comes from layered factors, careful UX design, and sustained user awareness.

Auditing of User Actions

Auditing monitors, records, and analyzes system actions to enforce policies and detect suspicious behavior. NIST (2006) recommends logging authentications, data changes, and administrative operations to enable investigation and incident response. Logs should be immutable, encrypted, and stored off-site or in decentralized stores to prevent tampering (Ali et al., 2021). Modern infrastructures integrate real-time auditing with detection/response systems and advanced analytics for compliance and anomaly detection (Barabanov & Makrushin, 2021). Increasingly, AI-assisted behavior analytics enhances proactive risk identification. Beyond technical value, auditing supports legal/regulatory obligations for transparency and data protection.

Encrypted File Storage

Encryption at rest protects sensitive data even if storage media are accessed physically. Combined with granular access controls, it limits exposure and supports legal/regulatory requirements (Sultan et al., 2020; ENISA, 2023). A central challenge is **key management**. Role-Based Encryption (RBE) can support dynamic key rotation and role changes across multi-organization settings without major performance penalties (Sultan et al., 2020). Monitoring and access auditing should complement encrypted storage to detect abuse (Chen et al., 2021). Under GDPR/HIPAA, encryption is recommended as part of a risk-based compliance program, including DPIAs, key-rotation processes, and access monitoring (European Parliament and Council, 2016; EDPB, 2021; ENISA, 2023).

Existing Platforms

- **Signal** is widely regarded as a gold-standard E2EE protocol—open-source, audited, and employing AES-GCM, Curve25519, and the Double Ratchet for forward secrecy and post-compromise security (Cohn-Gordon et al., 2017; Marlinspike & Perrin, 2016; Pindrop, 2024). However, common enterprise needs such as detailed audit logs, rich role management, and private file-storage integration are often absent (Cohn-Gordon et al., 2020; Pindrop, 2024).

- **WhatsApp** also uses Signal Protocol but collects metadata, which can be sensitive in corporate contexts (Greenberg, 2021).
- **Wire** provides E2EE for messages/calls/files, supports role management, and integrates audit logs, aligning better with organizational use cases (Wire, 2023).
- **Threema** enhances privacy (no phone number required; Swiss hosting) but faces similar enterprise-integration gaps.
- **Telegram** offers E2EE only in Secret Chats; standard chats are cloud-based (encrypted but not end-to-end), making it less suitable for high-security business use (Grassi et al., 2017).
- **Matrix/Element** supports decentralized, E2EE communication with organizational features such as audit logs and role management, providing greater control and flexibility (Matrix.org, 2023).

Overall, no single platform perfectly combines strong E2EE, granular auditing, private encrypted file storage, strict metadata controls, and formal compliance certifications (GDPR/HIPAA). This gap motivates customized platforms designed for enterprise requirements, especially amid cloud adoption and hybrid work (Ali et al., 2021; Sultan et al., 2020; Pindrop, 2024).

Summary

This chapter reviewed core components of secure communication platforms. **E2EE** remains central to confidentiality, while **MFA** strengthens access control, and **auditing** provides accountability and incident visibility. **Encrypted storage** and **role-based controls** reduce exposure and support compliance. Despite mature technologies, usability, key management, metadata privacy, and enterprise-grade governance features remain areas where tailored solutions can add significant value—particularly in organizational contexts that demand comprehensive security and regulatory alignment.

Case Study: User Interface and System Workflow

The developed application consists of several integrated modules, each with a specific role in enabling secure communication within an organization. To ensure usability and a clean visual design, the interface was built with **React.js** and styled using **TailwindCSS**. The following case study illustrates the main functional components of the system:

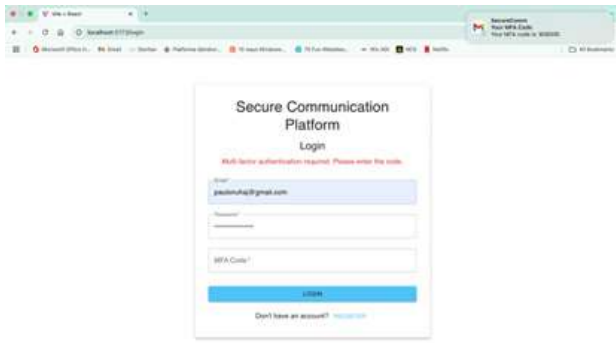
Register Page

FIGURE 1: Register Page

The registration interface provides a form with essential fields: username, email, password, and password confirmation. Upon submission, an RSA key pair is generated, and the private key is encrypted with a symmetric key derived from the user's password. This process takes place entirely on the frontend, ensuring the server never has access to the private key. An OTP is then sent via email for initial verification.

Login Page with MFA

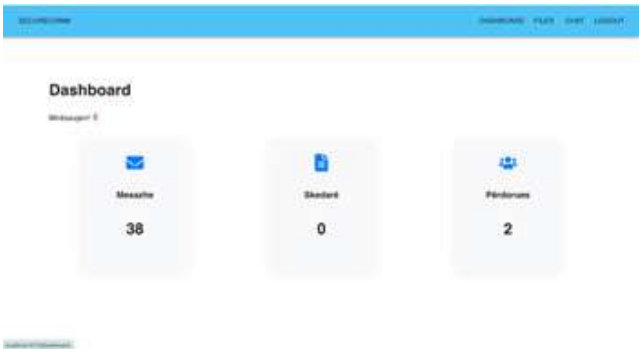
FIGURE 2: Login Page + MFA



For authentication, the user must provide their email and password. If these credentials are correct, the backend sends a one-time verification code (OTP) to the user's email, which must be entered to complete the authentication process. Once this step is successfully completed, the system applies the process of deriving a symmetric key to decrypt the locally stored private key, which is then used for decrypting both messages and AES session keys.

Dashboard

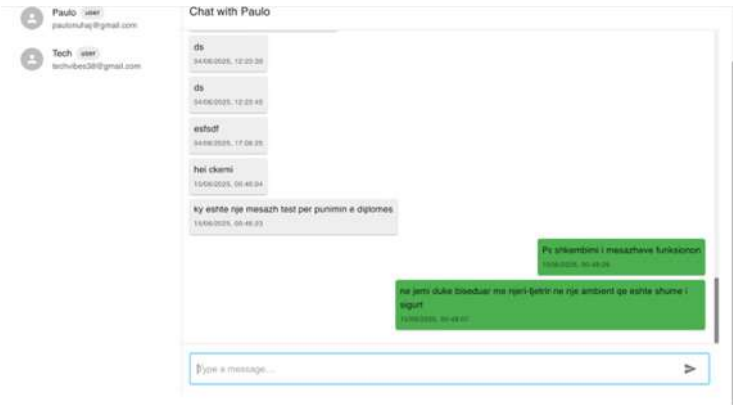
FIGURE 3: Dashboard



After successful login, the user is redirected to the dashboard, which provides access to the core system functionalities, including encrypted chats and secure file storage/sharing.

Chat Page

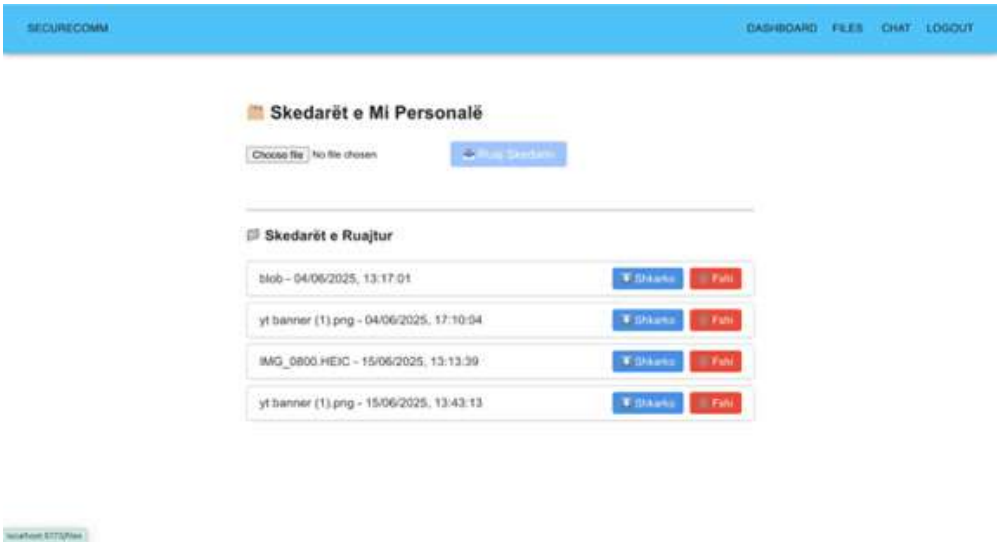
FIGURE 4: Chat Page



This is the page where live communication between users takes place. The user selects the person to chat with from the list of active contacts. Each message sent is securely encrypted with AES, and its key is encrypted using the recipient's public key. The message is stored on the server in encrypted form, making it unreadable to anyone else. The recipient uses their private key to decrypt the content. Messages are displayed chronologically, with indicators showing whether they have been read and whether the other user is typing.

Files Page

FIGURE 5: Files Page



This module enables the secure uploading of files by encrypting them in advance on the client side. For each file that is sent, a unique AES key is generated for encryption, which is then encrypted with the recipient's RSA public key. The file and its associated metadata are stored on the server in protected form. During the download process, the file remains encrypted and is only decrypted locally with the corresponding key, ensuring that the content is accessible solely to the authorized recipient.

Conclusions

This project aimed to build a secure platform for internal communication within companies by integrating modern encryption technologies and advanced security mechanisms. Throughout the development and testing process, the impact of end-to-end encryption (E2EE) on ensuring communication confidentiality was analyzed. The results showed that storing data in encrypted form and using public/private key pairs guarantees that only the intended recipient can read the message, significantly enhancing protection against eavesdropping or data leakage.

At the same time, the implementation of multi-factor authentication (MFA) yielded very positive results in strengthening access control. The addition of a

second verification step beyond the password made it much more difficult for unauthorized individuals to access the system, even in cases where a credential was compromised. This mechanism, combined with the logging of every action in the audit log, significantly increased transparency and user accountability within the system.

The construction of a centralized platform, where functionalities such as encrypted file storage and activity auditing coexist, provided several clear advantages. A higher level of control over data and its security was achieved, though some technical challenges were encountered, such as key management, protection of the private key, and educating users who are not always familiar with cryptographic concepts. Nevertheless, the use of technologies such as AES-GCM for file encryption and RSA-OAEP for key exchange proved to be an effective and balanced solution between security and performance.

From user feedback, it was observed that although well-known platforms such as email or external applications provide a simple and familiar experience, the platform developed in this project was valued for the security it offered and the sense of trust it created. This is particularly important for organizations that handle confidential data and require transparency in every action system.

This project confirmed that a comprehensive approach to security, including E2EE, MFA, auditing, and secure file storage, is not only feasible but represents a practical model for any company seeking to strengthen its internal communication. Building such a system requires care and planning, but the benefits it brings in protecting privacy, ensuring data integrity, and maintaining control make this work fully worthwhile.

Bibliography

1. Alotaibi, B. (2022). Adaptive multi-factor authentication for dynamic security needs. *International Journal of Information Security, 21*(3), 512–524.
2. Anderson, R. (2020). *Security engineering* (3rd ed.). Wiley.
3. Bonneau, J., Herley, C., van Oorschot, P. C., & Stajano, F. (2012). The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In *2012 IEEE Symposium on Security and Privacy* (pp. 553–567). IEEE. https://doi.org/10.1109/SP.2012.44
4. Borisov, N., Goldberg, I., & Brewer, E. (2004). Off-the-record communication, or why not to use PGP. In *Proceedings of the ACM Workshop on Privacy in the Electronic Society* (pp. 77–84).
5. Chen, Y., Wang, S., & Zhang, X. (2021). Secure and efficient cloud data storage with audit and anomaly detection. *IEEE Transactions on Cloud Computing, 9*(4), 1200–1212.
6. Cohn-Gordon, K., Cremers, C., Garratt, L., Millican, T. P., & Paterson, K. G. (2017). A formal security analysis of the Signal messaging protocol. *Journal of Cryptology, 30*(3), 709–741.

7. ENISA. (2023). *ENISA threat landscape 2023*. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023
8. European Parliament and Council of the European Union. (2016). *Regulation (EU) 2016/679 (General Data Protection Regulation – GDPR)*. *Official Journal of the European Union*.
9. Ganji, A., Orand, M., & McDonald, D. W. (2018). *Ease on down the code: Complex collaborative qualitative coding simplified with "Code Wizard"*. *Proceedings of the ACM on Human-Computer Interaction, 2*(CSCW), Article 132, 1–24. https://doi.org/10.1145/3274401
10. Grassi, P. A., Garcia, M. E., & Fenton, J. L. (2017). *Digital identity guidelines (NIST Special Publication 800-63B)*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-63b
11. Hassani Karbasi, A., & Shahpasand, S. (2021). *SINGLETON: A lightweight and secure end-to-end encryption protocol for sensor networks in the Internet of Things based on cryptographic ratchets*. *The Journal of Supercomputing, 77*. https://doi.org/10.1007/s11227-020-03411-x
12. Kaufman, C., Perlman, R., & Speciner, M. (2019). *Network security: Private communication in a public world* (3rd ed.). Prentice Hall.
13. McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2017). The effect of experience on security behaviours and knowledge. *Computers & Security, 70*, 663–674.
14. Microsoft. (n.d.). *How it works: Microsoft Entra multifactor authentication*. Microsoft Learn. https://learn.microsoft.com/en-us/entra/identity/authentication/concept-mfa-howitworks
15. Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T., & Koucheryavy, Y. (2018). Multi-factor authentication: A survey. *Cryptography, 2*(1), 1. https://doi.org/10.3390/cryptography2010001
16. Paterson, K. G., & Poettering, B. (2022). Strong optimality of double ratchet style key updating against state compromise. In *Advances in Cryptology – CRYPTO 2022* (Lecture Notes in Computer Science, Vol. 13508). Springer.
17. Perrin, T., Marlinspike, M., & Schmidt, R. (2025). *The Double Ratchet algorithm* (Revision 4). https://signal.org/docs/specifications/doubleratchet/
18. Stallings, W. (2022). *Cryptography and network security: Principles and practice* (8th ed.). Pearson.
19. Sultan, K., Al-Bassam, B., & Al-Rodhaan, M. (2020). Role-based encryption for secure cloud data sharing with dynamic key management. *Journal of Cloud Computing, 9*(1), 25.
20. von Solms, R., & van Niekerk, J. (2013). From information security to cyber security. *Computers & Security, 38*, 97–102.
21. Wahab, D. A. W., Hou, D., & Schuckers, S. (2023). A user study of keystroke dynamics as second factor in web MFA. In *Proceedings of the 13th ACM Conference on Data and Application Security and Privacy (CODASPY '23)*. https://doi.org/10.1145/3577923.3583642