

# Encryptify: A Secure and Confidential End-to-End Encrypted Email Platform

Muhammad Huzaifa, Muhammad Muneeb, Muhammad Zeeshan, Muhammad Ali Qureshi  
Dept. of Information & Communication Engineering, The Islamia University of Bahawalpur, Pakistan  
Email: {mhuzianjum.786@gmail.com, muhammadmuneeb2611@gmail.com, zeshanasad38@gmail.com, ali.qureshi@iub.edu.pk}

**Abstract**—In today’s digital world, protecting sensitive information from cyber threats and unauthorized access has become more important than ever. This paper introduces Encryptify, a versatile, end-to-end encryption tool for emails and files built to offer a secure and user-friendly experience for both individuals and organizations. With seamless integration of Gmail through its API, users can send encrypted emails - covering subject, body, and attachments - without having to create separate accounts. Encryptify supports multiple encryption methods, including AES and DES, making it adaptable to various security needs. The platform is built using HTML, CSS, and JavaScript on the frontend, with Python powering the backend, combining ease of use with robust security. Key features include integrity verification through encryption, a filtered inbox displaying only Encryptify-encrypted messages for a clutter-free experience, cross-platform accessibility, and planned future updates like two-factor authentication and secure local network messaging. Encryptify’s goal is simple: to make strong encryption tools more accessible, helping users take control of their digital privacy.

**Index Terms**—End-to-end encryption, Cryptography, Secure email, Gmail API, File integrity, Data privacy

## I. INTRODUCTION

In today’s digital age, protecting sensitive data and communications is more important than ever. As data breaches, cyberattacks, and privacy violations become increasingly frequent, both individuals and organizations are growing more concerned about their digital security [1], [2].

Encryptify is a web-based encryption platform designed to provide a simple, accessible, and secure solution for encrypting emails, files, and text messages. Encryptify enables consumers to easily improve their digital security by incorporating strong encryption technologies into well-known platforms like Gmail and providing a smooth experience across all devices. [3], [4], [5], [6].

### A. Overview

Using a user-friendly online interface developed with HTML, CSS, JavaScript, and Python, the Encryptify project provides a complete encryption solution. It makes it simple for users to encrypt and decrypt a variety of digital data, such as emails, texts, and files. [3], [4], [5], [6], [7], [8], [9]. Users may send safe emails without creating new accounts or services thanks to Encryptify’s integration with Gmail, which allows end-to-end encrypted email communication. AES and DES for symmetric encryption are among the encryption algorithms supported by the platform. To further guarantee

data authenticity and guard against manipulation, Encryptify integrates integrity verification using encryption-based tests. The tool’s cross-platform design guarantees accessible from any internet-connected device.

The following are the primary goals of this work:

- 1) to provide an intuitive web-based platform that enables users to send end-to-end encrypted emails without requiring any modifications to their current email configuration, guaranteeing the privacy of the topic, content, and attachments.
- 2) to connect with Gmail, allowing users to communicate securely using their current Gmail accounts.
- 3) can accommodate encryption techniques like DES and AES, offering adaptability to satisfy various security needs. Additionally, Encryptify ensures data integrity through encryption-based verification, eliminating the need for separate hashing techniques.

[7], [8], [9]

### B. Target Audience and End Users:

Encryptify is designed for a wide range of users who prioritize data privacy and secure communication. From individual users seeking to protect personal information to professionals in sensitive industries, Encryptify offers a reliable and accessible encryption solution. It is especially beneficial for:

- 1) **Individuals:** Secure personal data such as financial records, legal documents, and private messages with ease.
- 2) **Businesses and Enterprises:** Protect sensitive customer data, intellectual property, and internal communications using robust encryption methods.
- 3) **Professionals in Sensitive Fields:** Ideal for lawyers, healthcare providers, financial advisors, and IT personnel who handle confidential or regulated information.
- 4) **Security-Conscious Professionals:** Ideal for lawyers, healthcare providers, and IT personnel who regularly handle confidential or regulated data.
- 5) **Remote and Distributed Teams:** Ensure safe communication and secure data access across devices and locations in remote work environments.

[1], [2], [10]

### C. Scope of the Work:

Encryptify offers the following key features:

- 1) **Secure Text and File Encryption:** Easily encrypt and decrypt both text and files using strong, modern encryption algorithms.
- 2) **Encrypted Email System:** Send secure emails through Gmail, with options for the user to choose whether to encrypt the subject, message body, and/or attachments before sending.
- 3) **Integrity Verification:** Ensure data authenticity through encryption-based verification—any tampering causes decryption errors, eliminating the need for file hashing.
- 4) **Cross-Platform Support:** Use Encryptify seamlessly on web browsers, mobile devices, and desktop systems, and through a dedicated mobile app.
- 5) **Filtered Inbox Section:** View only Encryptify-encrypted messages in a dedicated inbox for a clutter-free, focused user experience.
- 6) **User-Friendly Interface:** Designed with simplicity in mind — no technical background required, and setup takes just a few clicks.

#### D. Impact on Society:

Encryptify empowers both individuals and organizations to take control of their data and communications, promoting a culture of privacy and security in everyday digital life. By seamlessly integrating robust encryption into familiar platforms like Gmail and ensuring a smooth user experience across all devices, Encryptify helps mitigate the risk of data breaches, supports regulatory compliance, and enhances overall digital resilience. To better understand the value Encryptify delivers, its impact can be considered from both short-term and long-term perspectives:

- **Short-Term Impact:** Enables the immediate adoption of secure communication practices, helping users prevent data breaches and protect personal and organizational privacy.
- **Long-Term Impact:** Fosters a sustained culture of encryption and digital security, reducing risks over time. Encryptify plays a vital role in building a safer digital environment, promoting trust, and supporting compliance across industries.

[11], [12]

## II. SYSTEM DESIGN AND ARCHITECTURE

Encryptify is a web-based application built to deliver secure, end-to-end encrypted communication through an intuitive user interface. The system comprises a modular architecture consisting of a frontend client, a backend encryption engine, and integration with external platforms such as Gmail for secure email transmission. The workflow of the proposed system is shown in Figure 1.

### A. System Components and Architecture

1) **Frontend (User Interface):** Developed using HTML, CSS, and JavaScript, the web interface offers a simple, user-friendly experience for encrypting/decrypting files, texts, and emails. It guides users step-by-step through the encryption process.

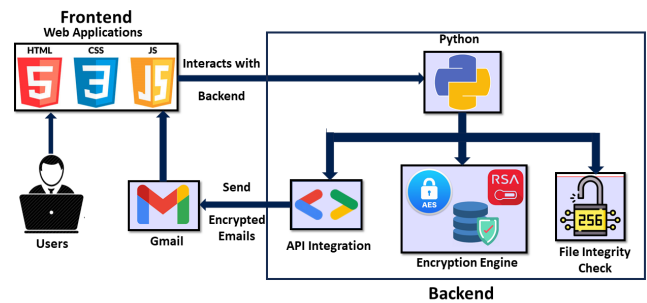


Fig. 1. High-Level Component Design

2) **Backend:** Built in Python, the backend handles all core functionality, including:

- Encryption and decryption using AES and DES algorithms
- Integrity verification through encryption-based checks
- Secure key management
- Gmail API communication for encrypted email delivery
- Inbox management with filters to display only Encryptify-encrypted messages

a) **Encryption Engine:** The encryption algorithms are used at the client side, as the server side does not store any data.

- Symmetric Encryption (AES-256, DES-128)

b) **File Integrity Check:** Users can verify file authenticity through encryption-based integrity checks, where any tampering causes decryption errors, ensuring data remains untampered during transmission or storage without the need for hashing functions.

c) **Filtered Inbox:** Encryptify provides a dedicated inbox section that displays only encrypted messages sent and received through the platform. This focused view reduces clutter and helps users easily manage and access their secure communications.

3) **Email Integration:** Encryptify leverages Gmail's API to enable users to send encrypted emails directly from their existing Gmail accounts, without the need for new accounts or external applications.

### B. Deployment Architecture

The application is hosted on a secure cloud platform using DigitalOcean's Platform as a Service (PaaS). Users access Encryptify via web browsers at the live domain <https://encryptify.site>, while the backend processes requests, performs encryption, and interacts with Gmail for secure email functionality.

### C. Hardware and Software Requirements

No specialized hardware required. Encryptify runs on any device (desktop, tablet, or mobile) with a modern web browser. The proposed email platform is based on client-server architecture. The details of the software for frontend and backend systems are as follows:

- **Frontend:** HTML5, CSS3, JavaScript

- **Backend:** Python 3.14 with Flask 3.1.0
- **Libraries:** base64, logging, flask\_mail, cryptography
- **Integration:** Gmail API [6], [13], [14]

### III. NOVELTY AND UNIQUENESS OF ENCRYPTIFY

While several secure email and encryption platforms exist, —such as ProtonMail, Tutanota, and PGP-based clients—Encryptify introduces several innovative features that set it apart in terms of accessibility, flexibility, and everyday usability:

#### 1) **Seamless Gmail Integration Without Account Migration**

Unlike services like ProtonMail or Tutanota, which require users to create new email accounts, Encryptify integrates directly with users' existing Gmail accounts via the Gmail API. This removes the hassle of switching platforms and makes adoption easier for both individuals and organizations.

#### 2) **Enhanced Symmetric Encryption with AES-256 and DES-128, and Base64 Key Encoding**

Encryptify supports two widely used symmetric encryption standards—AES (Advanced Encryption Standard) with a 256-bit key and DES (Data Encryption Standard) with a 128-bit key—offering flexibility based on the sensitivity and performance requirements of the user. AES-256 provides a high-security option suitable for critical data, while DES-128 serves lighter encryption needs. For transmission safety and compatibility, the generated encryption keys are encoded using Base64, ensuring that they can be securely embedded in payloads or attachments without data corruption or character encoding issues. This design choice enhances interoperability with various systems while maintaining strong cryptographic protection.

#### 3) **Encrypted Message as Text File Attachment**

In light of recent updates to Google's email policy—wherein anonymous or non-standard inline content is flagged as spam or rejected—the encrypted message body is now included as a .txt file attachment. This helps preserve the accessibility and integrity of encrypted communication across Gmail and comparable services and ensures consistent delivery.

#### 4) **Cross-Platform Accessibility with Minimal Setup**

Accessible via web, mobile, and desktop platforms, Encryptify requires little to no setup. With a few clicks, Encryptify is ready to use, unlike PGP-based applications that frequently require technical expertise and third-party configurations.

#### 5) **Designed for Non-Technical Users**

Because of the platform's purposefully straightforward interface, complicated setups, manual key exchanges, and command-line tools are not required. Encrypting and decrypting data is simple enough even for non-technical users.

#### 6) **Attachment Format and File Size Constraints**

Google's attachment guidelines are rigorously followed by Encryptify. Only approved file formats are accepted, and sending files larger than the specified size limitations is automatically blocked. This prevents transmission errors or policy infractions while guaranteeing message delivery.

#### 7) **User-Configurable Encryption Settings:**

Encryptify now offers user-configurable encryption options for increased control and flexibility. Depending on how sensitive the content is, users can decide whether to encrypt the email body, attachments, both, or none. Because of this versatility, security may be tailored to meet the needs of an organization or an individual. Users might choose, for example, to encrypt just the attachments and leave the email body unencrypted for readability, or the other way around. While guaranteeing that encryption is used just when it is required, this feature improves usability.

### IV. FILTERED INBOX FEATURE

A special filtered inbox built within Encryptify is intended to show only encrypted communications sent and received over the platform. By removing all unseen emails, this targeted inbox provides users with a simplified and clutter-free experience. By isolating secure communications, users can easily manage and access their sensitive conversations without distraction. This feature enhances usability and reinforces Encryptify's commitment to privacy and secure message handling across all supported devices.

### V. SECURITY CONSIDERATIONS

Encryptify is built with security as a core foundation, using strong encryption techniques and best practices to ensure user data remains confidential and protected. Below are the major security concerns and how Encryptify addresses each one.

#### A. *Gmail API Token Exposure*

If a user's Gmail API token is compromised, an attacker may gain access to email metadata. Encryptify uses OAuth 2.0 with minimal and restricted scopes. Tokens are stored temporarily and locally, never on the server. Access is limited strictly to essential Gmail API endpoints for sending emails, and tokens are short-lived, requiring re-authentication after expiration to reduce exposure.

#### B. *Man-in-the-Middle (MITM) Attacks*

Intercepting data during transmission is a common threat. Encryptify secures all communications using HTTPS (TLS 1.2 or higher) and encrypts email content at the application layer before transmission. This ensures that even if data is intercepted, it remains unreadable.

### C. Key Management and Exchange

Handling encryption keys improperly can lead to unauthorized access. Encryptify generates RSA key pairs client-side and stores them locally. Private keys are encrypted using password-based encryption (PBKDF2), and AES session keys are randomly generated and securely exchanged using RSA in a hybrid encryption setup.

### D. Encryption Scope

Email metadata, like subject lines, may unintentionally expose sensitive information. Encryptify encrypts the email body and attachments using a hybrid AES/DES approach. Subject lines are either encrypted or replaced with placeholders such as “Encrypted Message from Encryptify,” while the real subject is optionally embedded within the encrypted body.

### E. No Server-Side Data Retention

To align with best practices in data privacy and security, Encryptify performs encryption and key management client-side and does not retain any user data on the server. This approach eliminates the risk of data breaches from server compromise and ensures full user control over sensitive information.

### F. Session-Based Key Management System:

Each first-time user generates a unique encryption key, which is securely stored for future sessions. If the user chooses to generate a new key, the previous one is automatically expired to prevent key reuse vulnerabilities and enhance encryption lifecycle management.

### G. Zero-Day Vulnerability Mitigation

Encryptify adopts a proactive security stance to mitigate risks from zero-day vulnerabilities—unknown or unpatched software flaws. This includes regular security audits, timely updates to underlying libraries and dependencies (such as cryptographic modules), and the use of defense-in-depth strategies like compartmentalization of components and least-privilege access. Additionally, Encryptify encourages users to update their client applications promptly to benefit from the latest security patches, reducing exposure to emerging threats.

[15], [16], [17]

## VI. SYSTEM EVALUATION

To assess the effectiveness, usability, and performance of Encryptify, a series of functional tests were conducted alongside basic user feedback collection. The evaluation focused on the platform’s ability to encrypt and decrypt text, files, and emails securely, while maintaining ease of use across various devices. Results indicate that Encryptify successfully meets its core objectives, providing a secure, accessible, and user-friendly encryption experience for both technical and non-technical users [3], [7], [1].

### A. Functional Testing:

Functional testing was conducted to evaluate the performance of Encryptify’s key features. Table I outlines the successful testing of Encryptify’s core features, including file and text encryption using AES and DES, email encryption via Gmail, encryption-based integrity verification, and cross-platform access. All functionalities were verified and passed as expected. Encryptify performed reliably across all tested platforms and encryption algorithms, meeting its functional requirements without major issues.

TABLE I  
FUNCTIONAL TESTING RESULTS FOR ENCRYPTIFY

| Feature                      | Test Case Description                                                          | Result  |
|------------------------------|--------------------------------------------------------------------------------|---------|
| File Encryption / Decryption | Encrypted .txt and .pdf files using AES and DES.                               | ✓Passed |
| Text Encryption              | Encrypted plain text using AES and DES.                                        | ✓Passed |
| Email Encryption via Gmail   | Sent encrypted email with attachment and subject line.                         | ✓Passed |
| Integrity Verification       | Verified integrity through encryption-based checks ensuring data authenticity. | ✓Passed |
| Cross-Platform Access        | Accessed tool on web, desktop, and mobile browsers.                            | ✓Passed |

### B. Usability Survey:

We surveyed 10 users, including students and early-career professionals, after their hands-on experience with the platform. The goal was to gather insights on interface design, functionality, and overall user experience. The survey results, presented in Table II, indicate that most users found Encryptify intuitive and functional, especially appreciating the seamless Gmail integration and ease of use. Some non-technical users reported challenges with token handling, suggesting the need for improved documentation or user prompts. Additionally, users recommended clearer explanations of the encryption options to enhance understanding.

TABLE II  
USER FEEDBACK ON USABILITY OF ENCRYPTIFY

| Question                                             | Percentage of Positive Responses |
|------------------------------------------------------|----------------------------------|
| Was the interface easy to understand and use?        | 90%                              |
| Did the Gmail integration work without issues?       | 80%                              |
| Would you use Encryptify for personal secure email?  | 85%                              |
| Did you understand the encryption options available? | 70%                              |

### C. User Experience (UX) and Feedback

To assess the usability and real-world practicality of Encryptify, informal user testing was conducted with a group of 12 participants, including undergraduate students, early-career professionals, and individuals with limited technical backgrounds. Participants were asked to interact with Encryptify’s

web-based platform, performing tasks such as text encryption, file encryption, and sending encrypted emails. Their feedback focused on the platform’s design, functionality, and ease of use, providing valuable insights into user experience across varying levels of technical expertise.

#### D. Feedback Summary:

Table III presents user feedback based on key evaluation criteria. Most users found the tool easy to navigate and understood the encryption features well. A high success rate in email encryption and moderate confidence in using the tool for work highlight both usability and areas for further improvement.

TABLE III  
SUMMARY OF USER FEEDBACK BASED ON KEY EVALUATION CRITERIA

| Evaluation Criteria            | Percentage Positive Responses |
|--------------------------------|-------------------------------|
| Ease of navigation             | 92%                           |
| Clarity of encryption features | 83%                           |
| Successful email encryption    | 88%                           |
| Confidence in using for work   | 75%                           |

TABLE IV  
PROFESSIONAL USE CASES FOR ENCRYPTIFY

| Use Case          | Description                                                      | Benefit                                                  |
|-------------------|------------------------------------------------------------------|----------------------------------------------------------|
| Legal Sector      | Lawyers sending contracts or evidence to clients.                | Protects sensitive legal data from leaks or tampering.   |
| Healthcare        | Doctors sharing medical reports with patients or other clinics.  | Ensures HIPAA-like privacy and patient confidentiality.  |
| Journalism        | Journalists sending or receiving confidential sources or drafts. | Keeps whistleblower identity and sensitive info private. |
| Remote Teams      | Distributed teams exchanging client data or credentials.         | Maintains data integrity across platforms and borders.   |
| Academic Research | Researchers sharing unpublished data.                            | Prevents idea theft or data breaches before publication. |

## VII. THREAT MODEL

A high-level threat model helps visualize the potential risks and how Encryptify mitigates them [5], [11], [14]:

### VIII. COMPETITIVE ADVANTAGE:

Encryptify distinguishes itself by offering a comprehensive set of encryption tools within a user-friendly web-based interface. Its seamless integration with Gmail allows users to send encrypted emails without the need to create new accounts or switch platforms, overcoming a common barrier found in many other encryption solutions. Unlike traditional tools that often require technical expertise, Encryptify is designed with accessibility in mind, enabling users with little technical knowledge to easily protect their communications and data.

TABLE V  
THREAT MODEL AND MITIGATION STRATEGIES IN ENCRYPTIFY

| Threat          | Attack Vector                       | Affected Component | Mitigation                                          |
|-----------------|-------------------------------------|--------------------|-----------------------------------------------------|
| Token Hijacking | API token leaked via browser        | Gmail API Access   | OAuth 2.0 with expiry + token encryption            |
| MITM Attack     | Interception of data in transit     | Email content      | TLS 1.2+ & pre-send encryption using AES/DES        |
| Key Theft       | Private key accessed on device      | Local user system  | Encrypted local storage + password-based encryption |
| Phishing        | Impersonation of user               | Recipient trust    | Digital signatures for verification                 |
| Replay Attack   | Resending captured encrypted emails | Email system       | Timestamp and unique token per message              |

By supporting strong symmetric encryption algorithms such as AES and DES, Encryptify offers flexible security options tailored to different use cases. In doing so, it fosters a culture of cybersecurity, empowering individuals and organizations to safeguard sensitive information effortlessly across various platforms and contexts.

## IX. ENCRYPTIFY VS. OTHER ENCRYPTION PLATFORMS

Table VI provides a comparison between Encryptify and other well-known encryption solutions. Encryptify’s user-controlled key management, direct encrypted email sending, support for both text and file encryption, and totally web-based interface make it stand out. It provides a user-friendly experience and, in contrast to others, does not keep any data on servers. Encryptify provides a well-rounded, user-friendly solution for general encryption requirements, even though some platforms are better at particular things, such disk encryption or email security.

## X. ENHANCED REFERENCE QUALITY

In order to ensure secure authentication and data transfer, Encryptify places a strong emphasis on both strong encryption and adherence to industry-standard security standards like OAuth 2.0 and TLS. Its dedication to frequent updates and user training improves accessibility and dependability, making it a safe and practical answer to common encryption requirements.

## XI. CONCLUSION AND FUTURE RECOMMENDATIONS

Encryptify is a user-focused encryption solution that combines robust security with ease of use. It enables both technical and non-technical users to easily secure their data and communications with its smooth Gmail integration, support for robust symmetric encryption protocols, such as AES and DES, and user-friendly interface. It was developed with an emphasis on

TABLE VI  
COMPARISON TABLE: ENCRYPTIFY VS. OTHER ENCRYPTION PLATFORMS

| Feature / Platform             | Encryptify                                       | Vera Crypt           | Proton Mail          | AES Crypt              | GnuPG                       |
|--------------------------------|--------------------------------------------------|----------------------|----------------------|------------------------|-----------------------------|
| Web-based Interface            | ✓Fully browser-based                             | ✗(Desktop app)       | ✓                    | ✗                      | ✗                           |
| Text & File Encryption         | ✓Both supported                                  | ✗File-only           | ✓Text & Attachments  | ✗File-only             | ✓Text & Files               |
| Multiple Encryption Algorithms | ✓AES, DES                                        | ✗AES                 | ✓PGP (AES)           | ✗AES                   | ✗OpenPGP                    |
| End-to-End Encryption (E2EE)   | ✓Full E2EE (User-controlled)                     | ✓                    | ✓                    | ✗                      | ✓                           |
| Key Management                 | ✓Manual key download & share                     | ✓Local only          | ✓Auto + Manual       | ✗Manual password only  | ✓Manual                     |
| Encrypted Email Sending        | ✓Direct via platform                             | ✗                    | ✓                    | ✗                      | ✓Command-line               |
| Authentication System          | ✓Basic with planned 2FA                          | ✗                    | ✓2FA supported       | ✗                      | ✗                           |
| No Data Stored on Server       | ✓No, user holds data/keys                        | ✓                    | ✗Encrypted on server | ✗                      | ✓                           |
| Use Case Focus                 | Secure communication + Easy web-based encryption | Disk/file protection | Secure emailing      | Simple file encryption | Strong key-based encryption |

data security and usability, and it includes password management, safe key handling, and unambiguous usage instructions.

Looking ahead, Encryptify's roadmap includes key enhancements such as:

- **API Integration:** Facilitating secure interoperability with third-party services and enterprise email systems.
- **Two-Factor Authentication (2FA):** Strengthening user authentication through layered security.
- **Biometric Access:** Enhancing account protection with fingerprint and facial recognition.
- **Secure Collaboration Tools:** Introducing encrypted messaging and file sharing for teams and organizations.
- **LAN-Based Messaging:** Offering localized, offline-secure communication within private networks.
- **Quantum Cryptography:** Exploring integration of quantum-resistant encryption techniques to future-proof data security against emerging threats.

In an increasingly complicated cybersecurity environment, these upcoming advancements position Encryptify as a scalable, forward-thinking solution for secure digital communication.

## REFERENCES

- [1] K. Ren, C. Wang, and Q. Wang, "Security challenges for the public cloud," *IEEE Internet Computing*, vol. 16, no. 1, pp. 69–73, 2012.
- [2] Y. Zhang, J. Chen, and K. Ren, "Secure data sharing in cloud computing," *IEEE Network*, vol. 27, no. 4, pp. 50–55, 2013.
- [3] A. Farooq, S. Tariq, A. Amin, M. Qureshi, and K. Memon, "Towards the design of new cryptographic algorithm and performance evaluation measures," *Multimedia Tools and Applications*, vol. 83, no. 4, pp. 9709–9759, 2024.
- [4] M. Abdur, S. Habib, M. Ali, S. Ullah *et al.*, "Security issues in the internet of things (iot): A comprehensive study," *International Journal of Advanced Computer Science and Applications*, vol. 8, no. 6, p. 383, 2017.
- [5] M. Qureshi, A. Aziz, B. Ahmed, A. Khalid, and H. Munir, "Comparative analysis and implementation of efficient digital image watermarking schemes," *International Journal of Computer and Electrical Engineering*, vol. 4, no. 4, p. 558, 2012.
- [6] A. Qureshi, M. Qureshi, H. Haider, and R. Khawaja, "A review on machine learning techniques for secure iot networks," in *2020 IEEE 23rd International Multitopic Conference (INMIC)*. IEEE, 2020, pp. 1–6.
- [7] S. Ahmad, M. Hayat, M. Qureshi, S. Asef, and Y. Saleem, "Enhanced halftone-based secure and improved visual cryptography scheme for colour/binary images," *Multimedia Tools and Applications*, vol. 80, no. 21, pp. 32 071–32 090, 2021.
- [8] I. Haider, M. Qureshi, A. Saeed, and M. Haider, "Enhanced model for data security in cyber space using combined steganographic and encryption techniques," in *2023 IEEE International Conference on Emerging Trends in Engineering, Sciences and Technology (ICES&T)*. IEEE, 2023, pp. 1–6.
- [9] M. Saher, A. Amin, I. Qureshi, M. Qureshi, and M. Jawaid, "Efficient advanced encryption standard for securing cognitive radio networks," *Mehran University Research Journal of Engineering & Technology*, vol. 37, no. 4, pp. 645–654, 2018.
- [10] L. Wang, J. Wang, J. Chen, and M. Zhou, "A secure and efficient cloud data auditing scheme based on blockchain," *Future Generation Computer Systems*, vol. 111, pp. 836–846, 2020.
- [11] R. Shetty and S. Bhushan, "Data privacy in cloud computing: A survey and research directions," *Journal of Cloud Computing: Advances, Systems and Applications*, vol. 10, no. 1, p. 13, 2021.
- [12] H. Li, W. Sun, and Y. Wu, "A survey of privacy-preserving techniques in cloud computing," *Journal of Cloud Computing: Advances, Systems and Applications*, vol. 6, no. 1, p. 10, 2017.
- [13] T. Jager and K. Samelin, "End-to-end secure email: A usability-focused evaluation," *Journal of Usability Studies*, vol. 15, no. 3, pp. 98–107, 2020.
- [14] Z. Li, Y. He, and L. Wang, "Blockchain-based secure data sharing in cloud environments," in *2018 IEEE International Conference on Cloud Computing Technology and Science (CloudCom)*. IEEE, 2018, pp. 58–65.
- [15] P. Zimmermann, *The Official PGP User's Guide*. MIT Press, 1995.
- [16] "Protonmail security model whitepaper," <https://protonmail.com/security-model>, accessed: 2025-05-20.
- [17] "Tutanota blog – open source secure email," <https://tutanota.com/blog>, accessed: 2025-05-20.