Indian Journal of Modern Research and Reviews

This Journal is a member of the *'Committee on Publication Ethics'*

Online ISSN:2584-184X

Research Article

Secure Messaging Website with Time-Bound and Encrypted File Sharing

M R Nithya [1*], Dr. S Aarthi [2], Arthyvarshini E [3], Meenatchi V [4], Yuvasree P [5]

[1] Assistant Professor, Department of Computer Science and Engineering, Meenakshi Sundararajan Engineering College, Kodambakkam, Chennai

[2-5] Dept of Computer Science and Engineering, Meenakshi Sundararajan Engineering College (Anna University - An Autonomous Institution) Chennai, India

Corresponding Author: * M R Nithya

DOI: https://doi.org/10.5281/zenodo.20069902

Abstract

In modern digital communication, protecting sensitive information during transmission has become increasingly important. This project proposes a secure web-based messaging system that supports encrypted communication and controlled file sharing with time-restricted access. The platform encrypts messages and files before transmission so that only authenticated recipients can retrieve the shared data through secure credentials such as tokens or passwords. Unlike traditional file-sharing systems that store data permanently, the proposed platform allows the sender to define the access duration for each shared file. After the specified time limit expires, the file is automatically removed from the system to prevent long-term storage or unauthorised reuse. The system also integrates security mechanisms that scan attachments, links, and messages to detect potential malware or harmful content. If suspicious activity is identified, access to the content is restricted to protect users. By integrating encryption, temporary access control, automated file removal, and threat detection features, the proposed solution enhances confidentiality and provides a safer environment for digital communication and file exchange.

Manuscript Information

- **ISSN No:** 2584-184X
- **Received:** 06-04-2026
- **Accepted:** 28-04-2026
- **Published:** 07-05-2026
- **MRR:**4(5); 2026: 01-09

- **Plagiarism Checked:** Yes
- **Peer Review Process:** Yes

How to Cite this Article

Nithya M R, Aarthi S, E A, V M, P Y. Secure Messaging Website with Time-Bound and Encrypted File Sharing. Indian J Mod Res Rev. 2026;4(5):01-09.

Access this Article Online

www.mrrjournal.in

KEYWORDS: Secure messaging, encrypted file sharing, time-limited access, access control, malware detection, data privacy.

I. INTRODUCTION

The widespread use of internet-based communication platforms has made digital information sharing a routine activity in both personal and professional environments. Despite their convenience, many existing messaging and file-sharing services provide limited security controls, which increases the risk of unauthorized access, data leakage, and cyber threats. Sensitive files are often stored for long periods,

making them vulnerable to misuse or unauthorized distribution. To address these challenges, this project introduces a secure messaging website designed to support encrypted communication and time-restricted file sharing. In this system, all transmitted messages and files are encrypted to ensure that only authorized recipients can access the shared information. Authentication methods such as tokens or passwords are used to verify the identity of users before granting access. A key feature of the proposed platform is sender-controlled access management. The sender can specify the duration for which a file remains accessible to the receiver. Once the defined time limit expires, the file is automatically deleted from the system, preventing permanent storage and reducing the risk of unauthorized reuse. By combining encryption techniques, time-limited file access, automated deletion, and threat detection mechanisms, the system aims to improve the security of digital communication while ensuring better control over shared information.

II. LITERATURE SURVEY

Previous research in secure communication systems primarily focuses on techniques such as encryption, authentication protocols, and secure data transmission methods to protect digital information. Many studies highlight the use of hybrid cryptographic approaches that combine symmetric and asymmetric encryption to enhance both performance and security. Other approaches explore technologies such as end-to-end encryption, proxy re-encryption, blockchain-based verification, and zero-trust security models to strengthen data confidentiality and access management. Although these technologies provide strong theoretical frameworks for secure communication, most existing solutions concentrate on infrastructure-level security or specific application

domains rather than practical user-oriented messaging systems. In many cases, features such as temporary file availability, sender-controlled access duration, and automatic deletion of shared data are not sufficiently addressed. Furthermore, several current messaging platforms lack integrated mechanisms to identify malicious attachments or harmful links during the communication process. Without such protection, users remain vulnerable to malware distribution and phishing attacks.

These limitations highlight the need for a secure messaging platform that not only applies strong encryption techniques but also incorporates time-bound file access, automated expiration of shared data, and built-in threat detection. The proposed system attempts to address these challenges by providing a comprehensive and user-focused secure messaging solution.

S. No	Title	Year	Authors	Methodology	Architecture / Model Used	Advantages	Disadvantages / Limitations
1	Secure Data Storage and Sharing Techniques for Data Protection in Cloud Environments: A Systematic Review	2022	Ishu Gupta, Ashutosh Kumar Singh, Chung-Nan Lee, Rajkumar Buyya	Systematic review and comparative analysis of data protection methods	Cloud data protection framework using cryptography, watermarking, differential privacy, and access control	Comprehensive analysis of data protection techniques; identifies research gaps and future directions	Does not implement a specific security model; mainly a theoretical review
2	Enabling Secure Time-Series Data Sharing via Homomorphic Encryption in Cloud-Assisted IIoT	2022	Subir Halder, Thomas Newe	Secure encrypted database and analytics using homomorphic encryption	SmartCrypt architecture for IIoT time-series data sharing	Supports analytics over encrypted data; improves throughput and scalability	Computational overhead due to encryption; complex implementation
3	A Framework for Digital Forensics of Encrypted Real-Time Network Traffic	2023	Soliman Abd Elmonsef Sarhan, Hassan A. Youness, Ayman M. Bahaa-Eldin	Traffic analysis of encrypted messaging and VoIP data	Network forensic framework analysing encrypted IM traffic	Enables detection of user activities even with encryption	Cannot decrypt content; relies on traffic patterns only
4	An Improved Random Bit-Stuffing Technique with Modified RSA Algorithm (RBMRSA)	2022	Falowo O. Mojisola, Sanjay Misra, C. Falayi Febisola, Olusola Abayomi-Alli, Gokhan Sengul	Enhanced RSA cryptographic algorithm using random bit insertion	RBMRSA encryption architecture	Higher security strength and better avalanche effect compared to classical RSA	Increased execution time and computational complexity
5	Secure File Sharing System with Strong Password and OTP Authentication	2025	Chee Lee Chong, Nur Ziadah Harun	Multi-factor authentication with OTP and password security	Secure file sharing platform with authentication and encryption modules	Improved user authentication and secure file access	Requires OTP infrastructure and may introduce login delays
6	Interoperability in End-to-End Encrypted Messaging	2023	Julia Len, Esha Ghosh, Paul Grubbs, Paul Rösler	Analysis of interoperability requirements for E2EE messaging	Cross-platform encrypted messaging architecture	Enables secure communication between different messaging platforms	Security challenges in identity management and abuse

				systems			prevention
7	Zero-Trust Network Access (ZTNA)	2023	Vasilios Mavroudis	Zero-trust security framework for network access	ZTNA architecture with continuous authentication and policy-based access control	Prevents insider threats; supports cloud and IoT environments	Implementation complexity and infrastructure changes required
8	A Secure and Anonymous Communication Scheme over IoT	2022	Qindong Sun, Kai Lin, Chengxiang Si, Yanyue Xu, Shancang Li, Prosanta Gope	Anonymous communication using P2P crowds network model	Lightweight IoT communication scheme using virtual spaces	Provides anonymity and secure data exchange	Not suitable for real-time latency-sensitive applications
9	Analysis of End-to-End Encryption and Authentication Ceremonies in Secure Messaging Systems	2023	Mashari Alatawi, Nitesh Saxena	Systematic evaluation of E2EE messaging authentication methods	E2EE messaging protocol analysis (Signal, WhatsApp etc.)	Identifies weaknesses in authentication ceremonies	Many systems remain vulnerable to MitM attacks
10	Quantum-Resistant End-to-End Secure Messaging and Email Communication	2023	Christoph Döberl, Wolfgang Eibner, Simon Gärtner, Manuela Kos, Florian Kutschera, Sebastian Ramacher	Integration of post-quantum cryptography in messaging systems	Quantum-resistant secure messaging architecture using PQC algorithms	Protects against future quantum attacks; improves cryptographic resilience	Implementation complexity and higher computational cost
11	Titanium: A Metadata-Hiding File-Sharing System with Malicious Security	2022	Weikeng Chen, Thang Hoang, Jorge Guajardo, Attila A. Yavuz	Secure metadata-hiding storage system using cryptographic ORAM techniques	Metadata-hiding file-sharing architecture protecting access patterns	Provides confidentiality and integrity even with malicious servers; improves efficiency compared to MCORAM	Higher computational overhead due to access pattern hiding
12	An End-To-End Encrypted Real-Time Multimedia Messaging Service System for Unicast and Multicast Communication	2023	T. C. Adeniran, E. U. Abah, H. B. Akande, S. O. Onidare	Real-time encrypted messaging using RSA encryption	ElectronJS + ReactJS client, NodeJS server, Firebase database with Socket.io communication	Enables secure real-time multimedia communication with minimal latency	RSA encryption may introduce computational overhead
13	Comparative Analysis of Energy Costs of Asymmetric vs Symmetric Encryption-Based Security Applications	2022	Basel Halak, Yildiran Yilmaz, Daniel Shiu	Experimental comparison of symmetric and asymmetric cryptographic schemes	Wireless embedded device network architecture for energy evaluation	Shows symmetric encryption is more energy efficient and reduces global energy consumption	Asymmetric algorithms still necessary for key exchange; symmetric alone not sufficient
14	Using Identity-Based Cryptography as a Foundation for an Effective and Secure Cloud Model for E-Health	2022	Shikha Mittal, Ankit Bansal, Deepali Gupta, Sapna Juneja, Hamza Turabieh, Ashish Sharma	Identity-based cryptographic algorithm for cloud healthcare systems	Cloud-based E-Health security framework	Reduces decryption time and energy consumption for healthcare data security	Limited scalability testing in large healthcare systems
15	Data Secure De-Duplication and Recovery Based on Public Key Encryption With Keyword Search	2023	Le Li, Dong Zheng, Haoyu Zhang, Baodong Qin	Secure deduplication using PEKS and Proxy Re-Encryption	Cloud storage architecture with encrypted deduplication mechanism	Reduces cloud storage redundancy while maintaining privacy	Complexity in key management and trapdoor generation
16	Efficient Personal Health Records Sharing in IoMT Using Searchable Symmetric Encryption, Blockchain, and IPFS	2023	Abhishek Bisht, Ashok Kumar Das, Dusit Niyato, Youngho Park	Secure PHR sharing with searchable encryption and decentralized storage	Blockchain + IPFS decentralized architecture	Ensures confidentiality, verifiable search results, and forward security	Blockchain overhead may increase latency and computational cost
17	Improved Secure Encryption with Energy Optimization Using Random Permutation Pseudo Algorithm in IoT-WSN	2023	S. Nagaraj et al.	Proposed SERPPA algorithm for secure communication and energy optimization	Cluster-based IoT Wireless Sensor Network architecture	Improves throughput, reduces energy consumption and computation cost	Implementation complexity in large-scale IoT environments
18	Identity-Based Threshold Proxy Re-	2022	Liqiang Wu, Yiliang Han,	Lattice-based threshold proxy	Identity-based threshold	Resistant to quantum attacks	High computational

	Encryption Scheme from Lattices and its Applications		Xiaoyuan Yang, Minqing Zhang	re-encryption using Shamir secret sharing	cryptographic architecture	and eliminates certificate management	complexity due to lattice operations
19	Privacy Preserving Data Sharing Method for Social Media Platforms	2023	Snehlata Yadav, Namita Tiwari	Anonymous revocable identity-based broadcast encryption	Secure broadcast encryption model for social media messaging	Ensures message privacy and protects user identity during broadcasting	Revocation and update key distribution may increase system overhead
20	User Perceptions of the Security and Privacy Benefits of WhatsApp Mods	2025	Collins W. Munyendo et al.	User study analyzing security perceptions of WhatsApp modified apps	Security analysis and interview-based behavioural model	Provides insights into real-world security practices and user behaviour	Mods may contain malware and over-permissioned features
21	Efficient Lattice-Based Revocable Attribute-Based Encryption Against Decryption Key Exposure for Cloud File Sharing	2023	Boxue Huang, Juntao Gao, Xuelian Li	Lattice-based CP-ABE encryption scheme with dynamic revocation	Multi-authority cloud file sharing system using RLWE-based ABE	Resistant to quantum attacks, supports dynamic user revocation	Large parameter sizes and higher computational cost
22	Secure Blockchain Integration Approach for Knowledge Discovery in Industrial Internet of Things	2025	Rohan Tripathi, Ritam Rao, Vivekananda Bhat K., Abhishek Kumar Pandey, Ashok Kumar Das	Blockchain integration with proxy re-encryption and whitelist access control	Four-layer IIoT architecture using Ethereum blockchain and PoA consensus	Ensures data integrity, secure knowledge discovery, and device authentication	Blockchain overhead and scalability challenges in large IIoT networks
23	Secure Message Handling in Vehicular Energy Networks Using Blockchain and Artificially Intelligent IPFS	2022	Muhammad Umar Javed et al.	Blockchain-based secure announcement dissemination system	Three-layer architecture: dissemination layer, IPFS storage layer, blockchain layer	Enhances trust, reduces storage overhead and computation time	Implementation complexity and blockchain latency
24	Securing Cloud Storage Data Using Hybrid AES–ECC Cryptographic Approach	2022	Sunil Kumar, Dilip Kumar	Hybrid cryptographic technique combining symmetric AES and asymmetric ECC	Secure cloud storage encryption framework	High security with improved encryption efficiency	Key management complexity and computational overhead
25	A Critical Cybersecurity Analysis and Future Research Directions for the Internet of Things	2023	Usman Tariq, Irfan Ahmed, Ali Kashif Bashir, Kamran Shaukat	Comprehensive review and analysis of IoT security threats and countermeasures	Layered IoT security architecture analysing connectivity and communication protocols	Identifies vulnerabilities and future research directions	Does not provide a concrete implementation solution
26	End-to-End Encrypted Message Distribution System for IoT Based on Conditional Proxy Re-Encryption	2024	Shi Lin, Li Cui, Niu Ke	Conditional Proxy Re-Encryption for secure message distribution	Publish–Subscribe IoT architecture using MQTT broker and HiveMQ	Prevents broker from accessing plaintext data; improves security	Slight encryption overhead and complexity in re-encryption key management
27	Performance Analysis of Security Protocols for Distributed Measurement Systems Based on IoT	2024	Antonio Francesco Gentile et al.	Evaluation of TLS/SSL protocols in IoT-based distributed measurement systems	VLAN-based IoT network architecture with MQTT broker and cloud communication	Identifies optimal encryption protocols for constrained IoT devices	Focuses on analysis rather than proposing a new security method
28	Timestamp-Based OTP and Enhanced RSA Key Exchange Scheme with SIT Encryption to Secure IoT Devices	2023	V. N. Hemanth Kollipara et al.	Lightweight cryptographic framework using OTP, enhanced RSA, and SIT encryption	Three-module IoT security system (authentication, key exchange, encryption)	Improves authentication and encryption with lower computational cost	RSA operations may still affect very low-power devices
29	Advanced Security Model for Multimedia Data Sharing in Internet of Things	2022	Shalini Dhar, Ashish Khare, Rajani Singh	Blockchain-based decentralized multimedia data	IoT distributed multimedia sharing architecture using blockchain and	Improves security and data availability in multimedia sharing	Increased latency and scalability issues

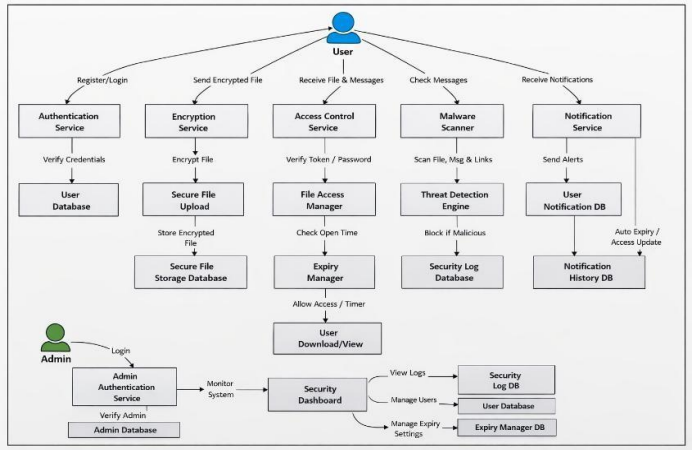
				sharing with IPFS	IPFS		
30	Importance of Encrypting Data in Transit and at Rest Using TLS and Other Security Protocols	2023	Sandeep Kumar Jangam	Analysis of TLS and encryption protocols for secure data transmission and storage	Secure communication architecture using TLS, HTTPS, and API security practices	Protects confidentiality, integrity, and availability of data	Implementation complexity and dependency on proper key management

III. MAJOR OBSERVATIONS

1. The majority of existing secure messaging and file-sharing systems primarily focus on encryption strength (AES, RSA, ECC, TLS) without integrating application-layer time-bound access enforcement or automated file lifecycle management mechanisms. This results in systems that ensure confidentiality but fail to control how long shared content remains accessible. **[1][5][9][10][12][24][26][30]**
2. Current authentication mechanisms such as password-based systems or OTP-based models operate independently of content lifecycle control, failing to link identity verification with sender-defined access duration and automatic expiry policies. As a result, authentication succeeds even when content should no longer be accessible.
   [4][8][28]
3. Most secure file-sharing and cloud storage frameworks provide persistent storage by design, lacking enforced temporary access, automatic deletion, and receiver-side access revocation once the defined time window expires. This persistence increases the risk of unauthorized retention and misuse of sensitive files.
   [1][15][16][21][24]
4. Blockchain and decentralised storage approaches prioritise immutability and data integrity but inherently conflict with temporary, revocable, and auto-expiring file-sharing requirements needed in controlled messaging systems. Their permanent ledger design makes controlled deletion technically challenging.
   [16][22][23][29]
5. End-to-end encrypted messaging platforms ensure confidentiality in transit but do not incorporate sender-controlled monitoring, real-time access duration tracking, or automatic post-expiry restriction mechanisms. Consequently, senders lose control once the message is delivered.
   [5][9][12][26]
6. Existing attribute-based and revocable cryptographic systems implement policy-driven revocation but do not enforce deterministic time-based expiry integrated directly with user sessions and access tokens. Revocation often depends on administrative intervention rather than automated expiry.
   [18][21]
7. Most research focuses on securing transmission layers using TLS and secure socket protocols, while application-layer lifecycle enforcement, expiry blocking, and secure deletion remain underdeveloped. This creates a security gap between transport protection and actual content control.
   [13][27][30]
8. Malware and phishing detection are rarely integrated directly into secure messaging architectures, leaving encrypted communication systems vulnerable to malicious file or link propagation. Encryption alone does not prevent the distribution of harmful payloads. **[20][25]**
9. Storage-centric security models emphasize encryption at rest but overlook user-centric temporary sharing workflows, sender-defined control, and prevention of unauthorized retention. These systems prioritize data protection but not controlled accessibility.
   [1][15][24]

Existing secure communication systems rarely integrate encryption, OTP authentication, time-bound access, automatic expiry, sender monitoring, malware scanning, and audit logging into a unified lightweight web-based architecture. Most solutions address these features in isolation rather than as a combined framework. **[4][12][21][26][28]**

IV. PROPOSED METHODOLOGY



The proposed system architecture follows a layered secure communication and protected file-sharing design to ensure confidential data exchange, controlled access, encryption enforcement, and audit-ready traceability across all operations.

1. User Layer

The User Layer represents the external entities interacting with the system, such as organizational staff, emergency response teams, law enforcement agencies, NGOs, or other authorized users. This layer initiates communication and file-sharing requests through a secure interface. All user actions, including sending messages, uploading files, and accessing shared content, are routed through secure channels and are subject to strict authentication and authorization policies enforced by lower layers.

2. Web Interface / API Layer

The Web Interface / API Layer acts as the entry point into the system. It contains the Secure Messaging Module, which manages user communication, file uploads, secure link generation, and interaction with backend services. This layer ensures that all incoming and outgoing requests are transmitted securely using HTTPS and token-based mechanisms. It integrates authentication standards such as OAuth 2.0, JSON Web Tokens (JWT), and Role-Based Access Control (RBAC) to enforce identity verification before granting access to backend services.

3. Backend Layer

The Backend Layer forms the core of the system's security architecture and enforces encryption, access control, and lifecycle management of shared files.

3.1 Authentication & Authorization Module

This module verifies user identities and assigns access privileges based on predefined roles. It ensures that only authenticated users can send, receive, or access shared files. Techniques such as Diffie-Hellman key exchange and Perfect Forward Secrecy strengthen session security.

3.2 End-to-End Encryption

All messages and files are protected using strong cryptographic algorithms such as AES-256 for symmetric encryption and RSA-2048 or ECC for key exchange. End-to-end encryption ensures that only the sender and intended recipient can decrypt and access the content, preventing interception or unauthorized disclosure.

3.3 Time-Bound File Sharing Module

This module allows the sender to define a specific access window for shared files. Access is granted only within the defined duration using mechanisms such as Time-Based Access Control (TBAC) and secure token expiration policies.

3.4 Auto File Expiry and Revocation

Once the access period expires, the system automatically revokes permissions and deletes the file from accessible storage. Expired links are permanently disabled, preventing further access attempts.

3.5 User-Specific Secure Storage Module

Temporary, encrypted storage is allocated for each user session. Files are encrypted before being stored, and access is strictly limited to authorized users. No permanent personal storage is provided for recipients.

3.6 Secure Link Sharing and Key Management

Secure link generation is tightly coupled with cryptographic key management. Public Key Infrastructure (PKI), Hardware Security Modules (HSM), and secure key rotation policies ensure that encryption keys remain protected and periodically refreshed to prevent compromise.

4. Key Management System / Service

The Key Management System centrally manages cryptographic keys used for encryption and decryption. It ensures secure key generation, distribution, rotation, and revocation. By isolating key management from application logic, the system enhances overall cryptographic security and resilience.

5. Database / Storage Layer

The Database and Storage Layer provide secure, encrypted cloud storage for messages and shared files. Access to storage resources is controlled through Access Control Lists (ACLs) and encrypted file storage mechanisms. The encrypted data flow ensures confidentiality throughout the storage lifecycle.

6. Audit and Logging Module

The Audit and Logging Module continuously monitors system activities. It supports Security Information and Event Management (SIEM) logging, integrity monitoring, tamper detection. All file access attempts, successful or. failed authentication events, and suspicious behaviours are logged for accountability and forensic analysis. This module enhances transparency and supports regulatory compliance.

7. Integrated Cybersecurity Techniques

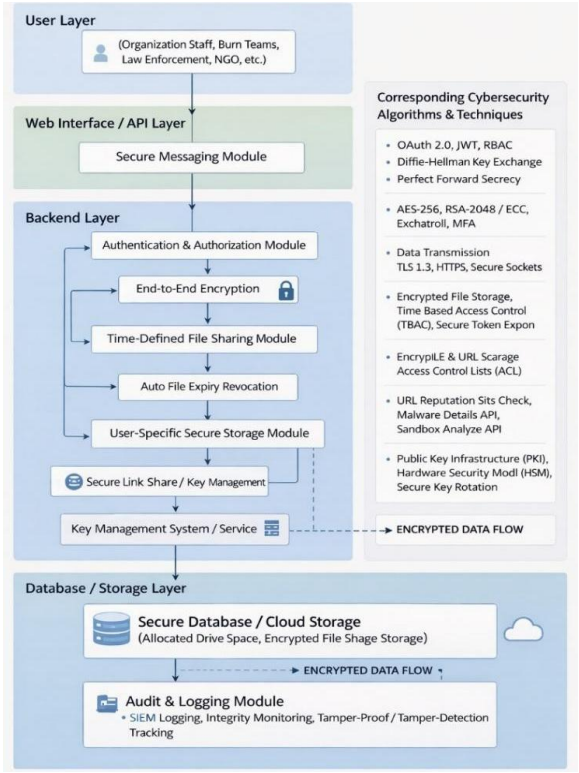
The diagram also highlights supporting cybersecurity mechanisms applied across layers, including:

- TLS 1.3 and HTTPS for secure transmission
- Perfect Forward Secrecy for session protection
- Malware detection APIs and URL reputation checks for threat prevention
- Encrypted file storage with time-based access control
- Public Key Infrastructure and secure key rotation Together, these mechanisms ensure confidentiality, integrity, availability, and controlled data lifecycle management.

8. Encrypted Data Flow

The entire architecture operates under a continuous encrypted data flow, meaning that data remains encrypted during transmission, processing, and storage. From the user interface to backend processing and final storage, encryption is enforced at every stage, minimizing exposure risk and preventing unauthorized access.

V. RESULT AND DISCUSSION

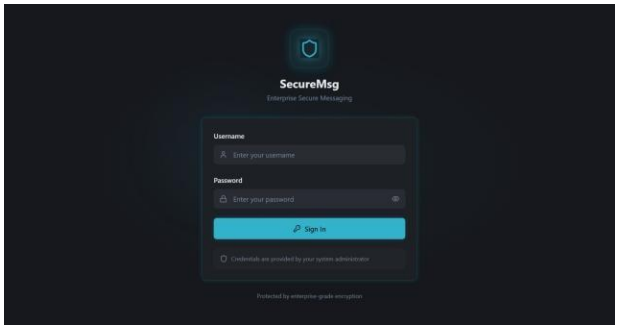


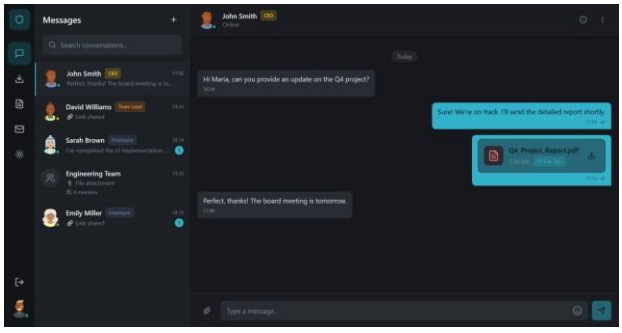
1. A layered secure messaging architecture has been implemented that integrates encryption, authentication, time-bound access control, and lifecycle enforcement into a unified web-based platform.
2. Sender-defined time window functionality is introduced, enabling controlled and temporary file access strictly limited to a predefined validity period.
3. An automatic file expiry and revocation mechanism is implemented to permanently block access and securely delete files once the access duration expires.
4. Token-based authentication and secure password validation are integrated with time-bound access enforcement, preventing unauthorized access after the defined expiry period.
5. Receiver-side access control is strengthened by eliminating permanent personal storage and restricting content availability to temporary encrypted sessions only.
6. A secure link generation and key management framework is introduced, incorporating encrypted key exchange and controlled key management policies.
7. Built-in malware and phishing detection mechanisms are implemented, including file scanning and URL reputation analysis before content access is granted.
8. Continuous encrypted data flow is enforced across transmission, processing, and storage layers using strong cryptographic standards.
9. Comprehensive audit logging and traceability mechanisms are integrated to record access attempts, expiry events, and suspicious behaviours for accountability.
10. The system is designed as a lightweight, privacy-first secure messaging web application that prioritizes controlled sharing, minimal data retention, and strong lifecycle enforcement over persistent storage models.

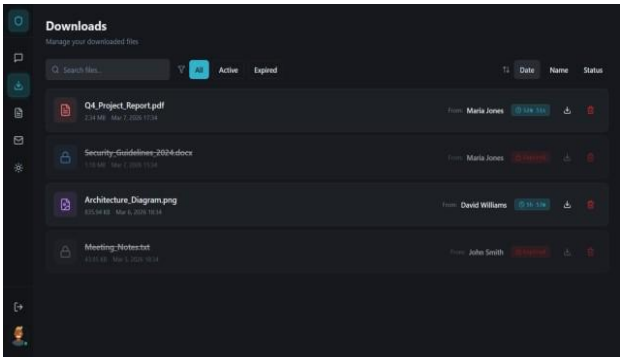
The proposed secure messaging system with time-bound encrypted file sharing was evaluated through controlled functional scenarios inspired by prior works on secure file sharing, authentication, encrypted messaging, and threat analysis. Evaluation scenarios included authenticated access, unauthorized access attempts, expired file access, repeated access after expiry, and interaction with potentially malicious files. Experimental observations indicate that enforcing encryption prior to transmission, combined with token-based authentication and password validation, effectively prevents unauthorized access, consistent with findings in secure file-sharing and authentication studies [4], [8], [27].

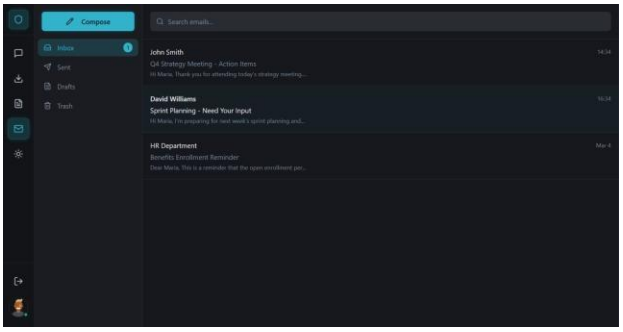
Time-bound access control and automatic file expiry successfully restricted access beyond the sender-defined validity window, addressing a major limitation identified across existing encrypted messaging and cloud-sharing systems [1], [2], [12], [19]. Once the expiry time elapsed, files became permanently inaccessible, even if access credentials were previously valid. This behaviour directly mitigates prolonged or unauthorized data retention, a gap repeatedly noted in prior literature.

Malware and threat scanning performed prior to file access ensured that potentially malicious content was blocked before delivery, addressing security risks highlighted in user behaviour and modded messaging studies [20]. Unlike several prior systems that focus solely on encryption or transport security [24], [30], the proposed system enforces application-layer security by combining access control, expiry enforcement, and content validation. Overall, the results demonstrate that integrating time-bound access, strong authentication, and threat detection significantly enhances secure messaging reliability and user trust without relying on complex cryptographic frameworks or AI-based misinformation detection.









VI. CONCLUSION

The Secure Messaging Website with Time-Bound Encrypted File Sharing presented in this work addresses critical security and privacy challenges commonly observed in modern messaging and file-sharing platforms. By integrating encryption prior to transmission, strong authentication mechanisms such as secure tokens, passwords, and one-time passwords, and strict access control policies, the system ensures that only authorized users can access shared messages and files. The introduction of time-bound access and automatic file expiry effectively prevents prolonged or unauthorized data retention, which is a major limitation in many existing secure communication systems.

The proposed solution emphasizes sender-controlled access by allowing users to define precise validity periods for shared content and by enforcing permanent access revocation once the expiry condition is met. This approach significantly reduces the risk of data misuse, leakage, or unintended redistribution. Unlike traditional secure messaging platforms that rely solely on encryption, the system enforces application-layer controls that govern the entire lifecycle of shared content, from upload and access to automatic deletion.

By scanning files, messages, and embedded links before granting access, the system mitigates risks associated with malicious content, phishing attacks, and unsafe file sharing. This proactive security measure addresses real-world Overall, the proposed system demonstrates that combining encryption, strong authentication, time-bound access control, and threat detection can provide a practical and effective solution for secure messaging and controlled file sharing. The architecture remains lightweight, user-centric, and deployable without reliance on complex cryptographic frameworks or heavy infrastructure. As a result, this work contributes a robust foundation for secure digital communication and establishes a clear pathway for future enhancements such as mobile platform support and advanced access control mechanisms.

REFERENCES

1. Gupta I, Singh AK, Lee CN, Buyya R. Secure data storage and sharing methods for data protection in cloud environments: a systematic review, analysis, and future directions. IEEE Access. 2022;10:71247–71282. doi:10.1109/ACCESS.2022.3188110.
2. Halder S, Newe T. Enabling secure time-series data sharing via homomorphic encryption in cloud-assisted IIoT. Future Gener Comput Syst. 2022;133. doi:10.1016/j.future.2022.03.032.
3. Sarhan SAE, Youness HA, Bahaa-Eldin AM. A framework for digital forensics of encrypted real-time network traffic, instant messaging, and VoIP: a case study. Ain Shams Eng J. 2023;14(7):102069. doi:10.1016/j.asej.2022.102069.
4. Mojisola FO, Misra S, Febisola CF, Abayomi-Alli O, Sengul G. An improved random bit-stuffing technique with a modified RSA algorithm (RBMRSA) for enhancing information security. Egypt Inform J. 2022;23(2):291–301. doi:10.1016/j.eij.2022.02.001.
5. Chong CL, Harun NZ. Secure file sharing system with strong password and one-time password authentication. J Comput Res Innov. 2025;10(1):98–107. doi:10.24191/jcrinn.v10i1.500.
6. Len J, Ghosh E, Grubbs P, Rösler P. Interoperability in end-to-end encrypted messaging. 2023.
7. Mavroudis V. Zero-trust network access (ZTNA). 2024. doi:10.48550/arXiv.2410.20611.
8. Sun Q, Lin K, Si C, Xu Y, Li S, Gope P. A secure and anonymous communication scheme over the Internet of Things. ACM Trans Sens Netw. 2022;18(3):1–25. doi:10.1145/3508392.
9. Alatawi M, Saxena N. SoK: analysis of end-to-end encryption and authentication ceremonies in secure messaging systems. In: Proc ACM Conf Security and Privacy in Wireless and Mobile Networks (WiSec). 2023:238–250. doi:10.1145/3558482.3581773.
10. Döberl C, Eibner W, Gärtner S, Kos M, Kutschera F, Ramacher S. Quantum-resistant end-to-end secure messaging and email communication. In: Proc Int Conf Availability, Reliability and Security (ARES). 2023. doi:10.1145/3600160.3605049.
11. Chen W, Hoang T, Guajardo J. Titanium: a metadata-hiding file-sharing system with malicious security. 2022. doi:10.14722/ndss.2022.24161.
12. Adeniran TC, Akande HB, Abah EU, Onidare SO. An end-to-end encrypted real-time multimedia messaging service system for unicast and multicast communication. Int J Inf Comput Secur Priv Digit Forensics. 2023;7(2):14–22. doi:10.4314/jispdf.v7i2.2.
13. Halak B, Yilmaz Y, Shiu D. Comparative analysis of energy costs of asymmetric vs symmetric encryption-based security applications. IEEE Access. 2022;10:76702–76719. doi:10.1109/ACCESS.2022.3192970.
14. Mittal S, Bansal A, Gupta D, Juneja S, Turabieh H, Sharma A. Using identity-based cryptography as a foundation for an effective and secure cloud model for e-

health. Comput Intell Neurosci. 2022;2022:1–8. doi:10.1155/2022/7016554.
15. Li L, Zheng D, Zhang H, Qin B. Data secure de-duplication and recovery based on public key encryption with keyword search. IEEE Access. 2023;11:22353–22363. doi:10.1109/ACCESS.2023.3251370.
16. Bisht A, Das AK, Niyato D, Park Y. Efficient personal health records sharing in Internet of Medical Things using searchable symmetric encryption, blockchain, and IPFS. IEEE Open J Commun Soc. 2023;4:2160–2177. doi:10.1109/OJCOMS.2023.3316922.
17. Nagaraj S, Kathole AB, Arya L, et al. Improved secure encryption with energy optimization using random permutation pseudo algorithm in IoT-WSN. Energies. 2023;16(1):8. doi:10.3390/en16010008.
18. Wu L, Han Y, Yang X, Zhang M. Identity-based threshold proxy re-encryption scheme from lattices and its applications. Front Inf Technol Electron Eng. 2022;23(2):258–277.
19. Yadav S, Tiwari N. Privacy-preserving data sharing method for social media platforms. PLoS One. 2023;18(1):e0280182. doi:10.1371/journal.pone.0280182.
20. Munyendo CW, Owens K, Strong F, et al. "You have to ignore the troubles": user perceptions of the security and privacy benefits of WhatsApp mods. 2025. doi:10.1109/SP61157.2025.00087.
21. Huang B, Gao J, Li X. Efficient lattice-based revocable attribute-based encryption against decryption key exposure for cloud file sharing. J Cloud Comput. 2023;12(1):37. doi:10.1186/s13677-023-00414-w.
22. Tripathi R, Rao R, Bhat VK, Pandey AK, Das AK. Secure blockchain integration approach for knowledge discovery in industrial Internet of Things. IEEE Open J Commun Soc. 2025;6:4774–4787. doi:10.1109/OJCOMS.2025.3574816.
23. Javed MU, Jamal A, Alkhammash EH, Hadjouni M, Bahaja SA, Javaid N. Secure message handling in vehicular energy networks using blockchain and intelligent IPFS. IEEE Access. 2022;10:82057–82075. doi:10.1109/ACCESS.2022.3194513.
24. Kumar S, Kumar D. Securing cloud storage data using hybrid AES–ECC cryptographic approach. J Cyber Secur Mobil. 2022;11(3):371–392. doi:10.13052/jcsm2245-1439.1132.
25. Tariq U, Ahmed I, Bashir AK, Shaukat K. A critical cybersecurity analysis and future research directions for the Internet of Things: a comprehensive review. Sensors. 2023;23(8):4117. doi:10.3390/s23084117.
26. Lin S, Cui L, Ke N. End-to-end encrypted message distribution system for IoT based on conditional proxy re-encryption. Sensors. 2024;24(2):438. doi:10.3390/s24020438.
27. Gentile AF, Macrì D, Carnì DL, Greco E, Lamonaca F. Performance analysis of security protocols for distributed measurement systems based on IoT. Sensors. 2024;24(9):2781. doi:10.3390/s24092781.
28. Kollipara VNH, Kalakota SK, Chamarthi S, Ramani S, Malik P, Karuppiah M. Timestamp-based OTP and enhanced RSA key exchange scheme with SIT encryption to secure IoT devices. J Cyber Secur Mobil. 2023;12(1):81–102. doi:10.13052/jcsm2245-1439.1214.
29. Dhar S, Khare A, Singh R. Advanced security model for multimedia data sharing in Internet of Things. Trans Emerg Telecommun Technol. 2022;33(11):e4621. doi:10.1002/ett.4621.
30. Jangam SK. Importance of encrypting data in transit and at rest using TLS and other security protocols. Int J AI Big Data Comput Manag Stud. 2023;4(3):82–91. doi:10.63282/3050-9416.IJAIBDCMS-V413P109.

About the Corresponding Author

M. R. Nithya is an Assistant Professor in the Department of Computer Science and Engineering at Meenakshi Sundararajan Engineering College, Kodambakkam, Chennai. She is engaged in teaching and research in computer science, with interests in emerging technologies, data systems, and software engineering, contributing to academic development and student learning.