SecureLine: End-to-End Encrypted Peer-to-Peer Messaging and File Sharing System

Karan Gobade[1], Jayesh Girathe[2], Nehal Meshram[3], Diya Madane[4], Kajal Jamgade[5], Prof. Devki Nandgaye[6]
[1,2,3,4,5,6]*Department of Information Technology, Nagpur Institute of Technology, Nagpur, India*

***Abstract*— Secure communication has become a fundamental requirement in modern digital environments due to increasing cyber threats and privacy concerns. Centralized messaging platforms often suffer from vulnerabilities such as data breaches, surveillance risks, and single points of failure. This paper presents SecureLine, an End-to-End Encrypted Peer-to-Peer (P2P) Messaging and File Sharing System designed to provide confidentiality, integrity, and decentralization. The system eliminates dependency on centralized servers and ensures that only communicating users can access the transmitted data. SecureLine integrates cryptographic key exchange mechanisms, authenticated encryption techniques, and peer discovery protocols to create a secure communication framework. The implementation demonstrates secure text messaging and encrypted file sharing over a distributed network. Experimental evaluation indicates improved privacy protection and resilience against common network-level attacks.**

***Index Terms*—End-to-End Encryption, Peer-to-Peer Communication, Secure Messaging, File Sharing, Cryptography, Network Security, Decentralized Communication**

I. INTRODUCTION

In recent years, instant messaging platforms have become one of the primary modes of communication. However, increasing cyber threats and privacy concerns have highlighted the limitations of centralized messaging systems. Traditional server-based architectures require users to trust third-party providers with their sensitive data. Even when encryption is implemented, centralized storage of metadata and routing information remains a vulnerability.

End-to-end encryption (E2EE) provides a mechanism ensuring that message content remains accessible solely to the intended participants. Despite its advantages, many encrypted messaging systems still depend on centralized servers for authentication and message routing.

Peer-to-peer (P2P) networking offers a decentralized alternative. In a P2P system, users communicate directly without relying on an intermediary server. This approach enhances fault tolerance, scalability, and censorship resistance. However, designing a secure P2P messaging system requires careful integration of cryptographic mechanisms and peer discovery protocols.

SecureLine is proposed to combine decentralized P2P networking with robust end-to-end encryption techniques to ensure secure and private communication.

II. LITERATURE REVIEW

Early cryptographic research introduced secure key exchange mechanisms enabling two parties to establish a shared secret over insecure channels. The Diffie–Hellman approach laid the groundwork for secure communication protocols.

Authenticated encryption methods combine encryption and message authentication, preventing tampering and forgery attacks. These methods ensure that transmitted messages remain confidential and unaltered.

Peer-to-peer networking models such as structured and unstructured overlays have been widely studied. The distributed hash table protocol proposed in Kademlia demonstrates efficient node discovery and routing in decentralized systems.

File-sharing systems such as BitTorrent-inspired architectures discussed in Peer-to-Peer File Sharing Systems highlight scalability and distributed resource

utilization. Additionally, modern secure chat frameworks described in Secure End-to-End Chat Application: A Comprehensive Guide emphasize encryption integration with application-layer protocols.

Recent academic implementations such as Secure and Scalable Peer-to-Peer File Distribution for Smart Campus Laboratories demonstrate that decentralized systems can be effectively deployed in institutional environments.

However, many existing solutions either focus solely on messaging or file sharing, lacking an integrated secure framework. SecureLine addresses this research gap by combining both functionalities under a unified encrypted P2P architecture.

III. PROBLEM STATEMENT

With the increasing reliance on digital communication platforms, users frequently exchange sensitive messages and files over the internet. Most commonly used messaging and file-sharing applications are built on centralized server-based architectures. Although these systems provide convenience and scalability, they introduce significant security and privacy concerns. Centralized servers often become attractive targets for cyberattacks and act as single points of failure. A successful attack or system failure can result in data breaches, service disruption, or unauthorized access to user information. Even when encryption is applied, centralized platforms may still expose user metadata, including communication patterns, identities, and file-sharing activity. Secure file sharing presents additional challenges, as traditional systems may allow unauthorized interception, modification, or misuse of shared data. In group communication scenarios, managing encryption keys and access control becomes more complex, especially when group membership changes frequently. These issues highlight the need for a communication system that provides strong security guarantees while preserving user privacy. Such a system should eliminate dependence on centralized infrastructure, ensure end-to-end protection for both messaging and file sharing, and remain scalable and user-friendly. The SecureLine system is proposed to address these challenges by combining decentralized peer-to-peer communication with robust cryptographic security mechanisms.

IV. PROPOSED SYSTEM

The SecureLine system was developed as a functional prototype to demonstrate secure peer-to-peer messaging and file sharing without relying on centralized infrastructure. The primary objective of the system is to provide strong confidentiality, integrity, and authentication while maintaining usability and reliability.

Unlike traditional messaging platforms that depend on central servers for routing and data management, SecureLine follows a decentralized communication model. Each user device operates as an independent peer node capable of establishing secure connections with other peers directly. This architectural decision reduces dependency on trusted third parties and eliminates single points of failure.

The system integrates networking mechanisms with cryptographic security modules to ensure protected communication. By combining decentralized peer discovery with end-to-end encryption, SecureLine addresses both privacy and security limitations commonly found in centralized platforms.

A. System Architecture

The architecture of SecureLine follows a decentralized peer-to-peer model consisting of multiple interacting components. Each user operates a peer node that can securely communicate with other peers in the network. A decentralized peer discovery mechanism enables users to locate and connect with available peers dynamically, without maintaining a centralized directory or server. Once a peer connection is established, a secure key exchange process is initiated between the communicating peers. The cryptographic keys generated during this process are used exclusively for encrypting and decrypting messages and files. An encryption and authentication module ensures that all transmitted data is protected against unauthorized access and modification. The messaging and file-sharing module handles secure data transmission between peers. Text messages are encrypted before being sent and decrypted only at the receiver's end. Similarly, files are transferred in encrypted form, ensuring confidentiality and data protection throughout the transmission.

B. Working of SecureLine

The operation of SecureLine begins with peer discovery, during which users identify and connect with other available peers in the network. After a secure connection is established, the system performs a cryptographic key exchange to generate shared secret keys. These keys are never transmitted in plaintext and remain known only to the communicating peers. Following successful key establishment, all messages are encrypted at the sender's device before transmission. The encrypted data is sent directly to the receiving peer and decrypted using the shared secret key. This process ensures that no intermediate entity can access the communication content. For file sharing, SecureLine encrypts files before transmission and securely transfers them over the peer-to-peer network. After reception, integrity checks are performed to verify that the file has not been altered during transit. This ensures both confidentiality and reliability in file transfers.

C. Security Objectives

The proposed SecureLine system is designed to achieve the following security objectives:

1. Confidentiality Only authorized peers possessing the shared secret key can access message or file content.
2. Integrity Any unauthorized modification during transmission is detected through cryptographic verification mechanisms.
3. Authentication Secure key exchange and verification procedures allow peers to confirm the identity of communicating parties.
4. Privacy Preservation By eliminating centralized servers, the system minimizes metadata exposure and reduces surveillance risks.
5. Fault ToleranceThe decentralized architecture improves system resilience and prevents total service failure caused by single server compromise.

V. METHODOLOGY

The methodology adopted for the SecureLine system focuses on integrating decentralized peer-to-peer communication with strong cryptographic security mechanisms. The system was designed and tested in a controlled local network environment to evaluate its ability to securely exchange messages and transfer files between multiple peers without relying on centralized servers.

The development process followed a modular implementation strategy. Networking functionality was implemented using socket-based communication to enable direct peer connectivity. Each device running the application operates as an independent peer node capable of initiating and accepting secure connections.

To ensure security, cryptographic mechanisms were incorporated into the communication workflow. A secure key exchange process is executed when two peers establish a connection. This process generates a shared secret key, which is then used for encrypting and decrypting transmitted data. The shared key remains known only to the communicating peers and is never exposed in plaintext form.

Once a secure channel is established, all messages are encrypted before transmission. The encrypted data is sent directly to the intended recipient, where it is decrypted using the shared secret key. This ensures that communication content remains confidential throughout the transmission process.

For file transfer, the system applies encryption before sending the file over the peer-to-peer network. After receiving the encrypted file, the recipient performs integrity verification to confirm that the file has not been modified during transit. Only after successful verification is the file decrypted and made accessible to the user.

The overall methodology emphasizes:

- Decentralized communication without centralized control
- Secure key generation and management
- End-to-end encryption for both messages and files
- Integrity verification during file transfer
- Reliable and efficient peer communication

The experimental testing confirmed that SecureLine successfully provides secure and private communication between peers while maintaining usability and system stability.

VI. SECURITY ANALYSIS

The security performance of SecureLine was assessed during implementation and testing under different communication scenarios. The evaluation focuses on

essential security objectives such as confidentiality, integrity, authentication, resilience against attacks, and comparison with traditional centralized architectures. The integration of peer-to-peer networking with modern cryptographic techniques strengthens the overall security framework of the system.

A. Confidentiality

SecureLine ensures privacy of communication by applying end-to-end encryption at the source device. All messages and shared files are encrypted before leaving the sender's system and remain encrypted during transmission. Decryption is performed only at the receiver's endpoint using a secret key generated through a secure key exchange mechanism.

Because encryption keys are accessible only to the communicating peers, no intermediate node or external observer can interpret the transmitted data. Even if network traffic is captured, the encrypted content cannot be converted into readable form without the correct cryptographic key. This design prevents unauthorized disclosure and protects sensitive information from interception.

B. Integrity

Data integrity is preserved using authenticated encryption techniques that verify message authenticity and detect alterations. Each transmitted message includes cryptographic validation data that enables the receiver to confirm that the content has not been modified during transit.

If any discrepancy is detected, the system discards the affected message or file automatically. This mechanism ensures that users receive accurate and untampered information, maintaining trustworthiness of communication.

C. Authentication

Before secure communication begins, peers undergo a verification process based on cryptographic key exchange. This procedure confirms the legitimacy of participating users and establishes a trusted communication channel.

By validating identities prior to data exchange, SecureLine prevents impersonation attempts and reduces the risk of man-in-the-middle attacks. Only authorized participants with valid credentials can join encrypted sessions, ensuring mutual authentication within the decentralized network.

D. Resistance to Common Attacks

Unlike centralized systems, SecureLine does not rely on a single server for communication management. This eliminates a critical point of failure often targeted in large-scale cyberattacks. The absence of centralized storage significantly reduces risks related to database breaches and server-side surveillance.

Additionally, because network responsibilities are distributed across peers, the system demonstrates improved tolerance to denial-of-service (DoS) attempts. Even if some nodes become unavailable, communication among remaining peers continues without complete service interruption. The decentralized structure ensures that communication remains functional even if individual nodes become unavailable, thereby maintaining consistent network operation.

E. Comparison with Centralized Systems

Conventional messaging platforms typically store user data and routing information on centralized servers, requiring users to trust service providers. Although many such platforms encrypt message content, metadata such as communication patterns and timestamps often remain accessible to service operators.

Secure Line follows a distributed trust model, where control is shared among participating peers rather than concentrated in a single authority. Because data handling and message forwarding are distributed across participating nodes rather than managed by a central entity, the system limits the accumulation of communication metadata and enhances overall user privacy protection. As a result, the decentralized approach provides stronger confidentiality guarantees compared to traditional server-based communication systems.

VII. CONCLUSION

This study introduced Secure Line, a decentralized peer-to-peer messaging and file-sharing application designed to overcome privacy and security challenges associated with centralized communication platforms. By removing dependence on central servers, the proposed system reduces vulnerability to data breaches, unauthorized surveillance, and large-scale service disruptions.

Secure Line combines peer-to-peer networking principles with established cryptographic techniques to provide secure message exchange and file transfer. The implementation incorporates secure key exchange protocols and authenticated encryption mechanisms to maintain confidentiality, integrity, and authentication. Since cryptographic operations occur exclusively at user endpoints, third parties cannot access or manipulate transmitted data.

The evaluation indicates that SecureLine enhances privacy protection, strengthens system resilience, and reduces metadata exposure compared to centralized alternatives. The peer-based communication model reduces dependency on any single infrastructure component, allowing the system to remain stable under partial network disruption. Overall, the results demonstrate that decentralized encrypted communication systems can effectively address modern security requirements while preserving user privacy.

REFERENCES

[1] W. Diffie and M. Hellman, “New directions in cryptography,” IEEE Transactions on Information Theory, 1976.

[2] P. Rogaway, “Authenticated encryption with associated data,” 2002.

[3] C. K. Wong, M. Gouda, and S. S. Lam, “Secure group communication using key graph structures,” IEEE/ACM Transactions on Networking, 2000.

[4] J. Buford et al., “Comparative study of peer-to-peer overlay network architectures,” IEEE Communications Surveys & Tutorials, 2007.

[5] P. Maymounkov and D. Mazieres, “Kademlia: Peer-to-peer information system using XOR distance metric,” in Proc. International Workshop on Peer-to-Peer Systems (IPTPS), 2002.

[6] A. Langley et al., “The state of knowledge in secure messaging systems,” in Proc. IEEE Symposium on Security and Privacy, 2016.

[7] B. Cohen, “Incentives build robustness in BitTorrent,” 2003.

[8] J. Benet, “IPFS – Content addressed, versioned, P2P file system,” 2014.

[9] S. Patel et al., “Secure end-to-end chat application design,” 2019.

[10] R. Kumar et al., “Cross-platform peer-to-peer file sharing system,” 2018.

[11] A. Sharma et al., “Secure and scalable peer-to-peer file distribution,” 2020.

[12] J. Jayaraj and P. Antony, “Overview of peer-to-peer file sharing systems,” 2017.

[13] M. Sireesha and A. Sirisha, “Encrypted multimedia distribution in P2P networks,” 2015.