MANTECH Publications

Journal of Research in Computer Science and Engineering
Volume 11, Issue 1, January-April 2026
ISSN: 2457-0818 (Online)

CrypTalk: A Secure Multi-Modal Communication Framework Using Kyber and AES

Gouri Boragi[1], Ashwini N. H[2], Priya Shivapur [3], Kurhade Varun Vijay[4], Priyanka Desurkar[5]

Student[1,2,3,4], Associate Professor[5]

Department of Computer Science and Engineering

Jain College of Engineering and Research, Belagavi

Corresponding Authors' Email: *boragigouri@gmail.com*

DOI: *https://doi.org/10.5281/zenodo.19143744*

ABSTRACT

This project introduces CrypTalk, a secure and user-friendly communication platform designed to make online conversations safer and more organized. CrypTalk allows users to send encrypted messages, join video calls, share files, and collaborate in real time through two types of communication rooms: public rooms, which anyone can join, and private rooms, which require admin approval or invitation. This structure ensures open discussions when needed, while sensitive or confidential conversations remain protected.

To guarantee strong security, CrypTalk uses a hybrid encryption model that combines Kyber, a post-quantum encryption algorithm built to resist future quantum-based attacks, with AES, a widely trusted standard for securing fast, real-time communication. In this system, Kyber is used to safely exchange encryption keys, while AES handles the actual message and media encryption. This layered approach keeps user data protected from both current and future security threats. The platform also includes practical features such as voice messaging, emoji reactions, typing indicators, and admin moderation tools like accepting or rejecting join requests and removing participants during chats or video sessions. These features help maintain safety while keeping communication smooth and engaging. Overall, CrypTalk combines modern cryptographic techniques with everyday communication features to provide a secure, efficient, and easy-to-use platform suitable for academic,

professional, and privacy-focused users.

KEYWORDS: *CrypTalk, Hybrid Encryption, Kyber Algorithm, AES Encryption, Secure Communication, Real Time Collaboration*

INTRODUCTION

In today's fast-growing digital environment, online communication has become a core part of everyday life, supporting everything from education and teamwork to personal conversations. As more interactions move to virtual spaces, the need for secure, private, and reliable communication tools has never been more important. Many existing platforms prioritize convenience but often overlook strong security practices, leaving users vulnerable to unauthorized access, data leaks, and privacy breaches. With emerging technologies—especially quantum computing—traditional encryption techniques may soon be easier to break, creating an urgent demand for communication systems that can withstand both current and future security threats.

CrypTalk is designed to address these rising concerns by offering a secure, web-based communication framework built on strong cryptographic foundations. The platform integrates encrypted messaging, controlled video conferencing, and real-time collaboration into a simple and user-friendly interface. To ensure robust data protection, CrypTalk uses a hybrid encryption model that combines Kyber, a post-quantum algorithm designed to resist advanced cyberattacks, with AES, a highly efficient symmetric encryption standard widely trusted for securing real-time communication. Along with features such as public and private rooms, admin-level access control, file sharing, voice messages, and typing indicators, CrypTalk creates a safe and flexible environment for both open discussions and sensitive exchanges. This makes the platform suitable for academic, professional and privacy-focused applications, offering a modern and resilient solution to the challenges of secure digital communication.

LITERATURE REVIEW

The rapid growth of digital communication has prompted extensive research into more resilient security mechanisms capable of protecting users from both current and emerging cyber threats. While classical encryption algorithms such as AES remain widely used due to their speed and

effectiveness in securing real-time data transmission, recent technological advances—particularly in quantum computing—pose significant risks to traditional cryptographic systems. This has led researchers to investigate quantum-resistant methods that can withstand future computational capabilities. Chen and Sharma (2022)

[1] Emphasize that lattice-based Key Encapsulation Mechanisms (KEMs), including the CRYSTALS-Kyber family, demonstrate strong potential for safeguarding communication platforms against quantum-enabled attacks. Their findings reinforce the need for adopting post-quantum cryptography in applications that manage sensitive interactions such as messaging, file transfers, and video conferencing.

Parallel to this, several studies have explored encryption strategies for real-time communication systems to prevent threats such as unauthorized access, interception, and session manipulation. Joseph, Banerjee, and Fernandes (2021) [2] show that a combination of asymmetric encryption and hashing algorithms can effectively secure cloud-based file-sharing processes; however, their work does not extend to interactive multimedia exchanges. Likewise, Patel and Desai (2020) [3] investigated secure video communication by integrating AES encryption with the Secure Real-Time Transport Protocol (SRTP). Their results indicate that symmetric encryption remains highly efficient for protecting real-time audio and video. Nonetheless, these models primarily address conventional threats and do not consider vulnerabilities introduced by future quantum computing advancements.

In addition to cryptographic concerns, literature also highlights significant challenges in establishing secure multi-party communication environments. Kulkarni and Prasad (2021) [4] observed that collaborative platforms often lack strong authentication, structured room-level access control, and mechanisms to prevent unauthorized participation. Their work stresses the necessity of administrative tools such as controlled user entry, moderated sessions, and secure room management to maintain integrity in-group communication. Dsouza and George (2019) [5] similarly demonstrated that although AES-based messaging applications support confidentiality, many existing systems do not provide modular communication channels or multi-layer authentication, restricting their utility in academic, organizational, and professional settings .To overcome such limitations, researchers have increasingly examined hybrid cryptographic frameworks that combine the speed of symmetric encryption with the

robustness of asymmetric key exchange. Kumar, Verma, and Rao (2019) [6] demonstrated that pairing AES-256 encryption with the classical Diffie–Hellman method can deliver secure end-to-end communication. However, their approach does not incorporate post-quantum security considerations. Earlier work by Sharma, Singh, and Gupta (2018) [7] introduced a double-encrypted hybrid RSA model, highlighting the advantages of layered cryptographic protection. While effective in strengthening confidentiality, the study focused primarily on algorithmic security and did not address communication features such as group coordination, user privileges, or multimedia collaboration.

To overcome such limitations, researchers have increasingly examined hybrid cryptographic frameworks that combine the speed of symmetric encryption with the robustness of asymmetric key exchange. Kumar, Verma, and Rao (2019) [8] demonstrated that pairing AES-256 encryption with the classical Diffie–Hellman method can deliver secure end-to-end communication. However, their approach does not incorporate post-quantum security considerations. Earlier work by Sharma, Singh, and Gupta (2018) [9] introduced a double-encrypted hybrid RSA model, highlighting the advantages of layered cryptographic protection. While effective in strengthening confidentiality, the study focused primarily on algorithmic security and did not address communication features such as group coordination, user privileges, or multimedia collaboration.

Taken together, existing literature reveals a strong emphasis on encryption techniques, multi-party communication issues, and the urgent need for cryptographic systems that remain secure in the post-quantum era. Although AES continues to serve as a high-performance option for real-time data protection, post-quantum algorithms like Kyber are increasingly recognized as essential for future-proof security. Despite these advancements, most prior systems do not offer an integrated platform that combines real-time chat, video communication, collaborative tools, administrative controls, and hybrid quantum-resistant encryption. CrypTalk addresses these shortcomings by merging Kyber-based key exchange with AES encryption and incorporating structured access management, thereby delivering a communication framework that ensures strong protection today while remaining resilient against emerging quantum-era threats.

Problem Statement

As digital communication becomes a core part of daily life covering everything from casual conversations to academic discussions and professional collaboration, security and privacy concerns continue to rise. Many existing platforms offer convenience but rely on traditional encryption methods that may soon become vulnerable, especially with the advancement of quantum computing. At the same time, most communication tools fail to provide strong participant control, secure room-based collaboration, or protection for multimedia interactions such as files, voice messages, and video calls. Current systems either focus only on basic messaging, lack structured access control, or do not integrate post-quantum–safe encryption. This leaves users exposed to risks such as unauthorized access, eavesdropping, data interception, and long-term cryptographic weaknesses. There is no unified platform that combines real-time collaboration features with modern and future-proof security.

Therefore, the core problem is the absence of a secure, user-friendly communication framework that offers encrypted messaging, protected video conferencing, controlled access rooms, and reliable defense against both present-day cyberattacks and emerging quantum threats.

Methodology

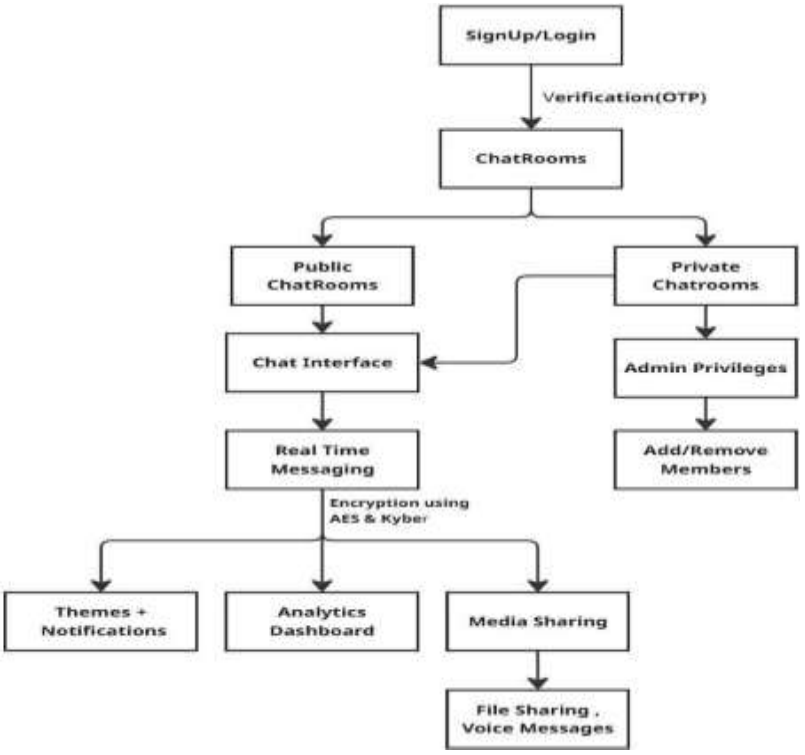

Figure 1: Flow diagram

The methodology followed in developing CrypTalk focuses on creating a secure, user-friendly communication platform that supports messaging, group collaboration, and real-time video calling. The system workflow begins with user verification and extends through group creation, communication features, and collaborative tools. Figure 1 illustrates the overall flow of the proposed system.

1. **User Registration and Verification:** The process begins with users creating an account using their email. To ensure the identity of every new user, an OTP is sent to their registered email. Only after entering this OTP can the user access the platform. This step prevents fake accounts and strengthens the platform's overall security.

2. **Login Authentication and Secure Access:** Once verified, users can log in at any time. During login, secure authentication techniques check their credentials and create a protected session. This ensures that only authorized users can enter their chats, preventing unauthorized access.

3. **Chat System:** Personal, Private, and Public Groups After logging in, users can communicate through personal chats or join group conversations. CrypTalk supports both private groups—accessible only through invitations—and public groups that any verified user can join. The group creator becomes the admin and can manage members and permissions. All messages are delivered instantly and stored securely, ensuring smooth and confidential communication.

4. **Real-Time Encrypted Messaging:** In CrypTalk, every text message is protected through a two-layer encryption process to ensure secure and uninterrupted communication. Before a message is sent, the system performs a Kyber-based key exchange to generate a shared session key between the sender and receiver. This session key is then used by the AES algorithm to encrypt the message content, ensuring that even if the data is intercepted, it remains unreadable. Each encrypted message includes essential metadata—such as the sender, timestamp, and group details—to preserve the natural flow of conversation while maintaining strict confidentiality.

5. **Audio and Video Calling with Secure Links:** CrypTalk also supports audio and video

calls. When a user starts a call, a unique and secure link is generated and shared through email. Only users with this link can join the session. Calls run on encrypted peer-to-peer technology, ensuring privacy and low latency.

6. **Profile Settings and Privacy Options:** Users can update their profile details and choose what they want to show to others. They can manage group memberships, block unwanted users, or report suspicious activity. All profile changes are protected with secure database storage.

7. **End-to-End Workflow Visualization:** The complete flow—from registration to secure communication—is presented in Figure 1. It shows how each module interacts, highlighting the smooth transition between verification, chatting, calling, and collaboration.

RESULT

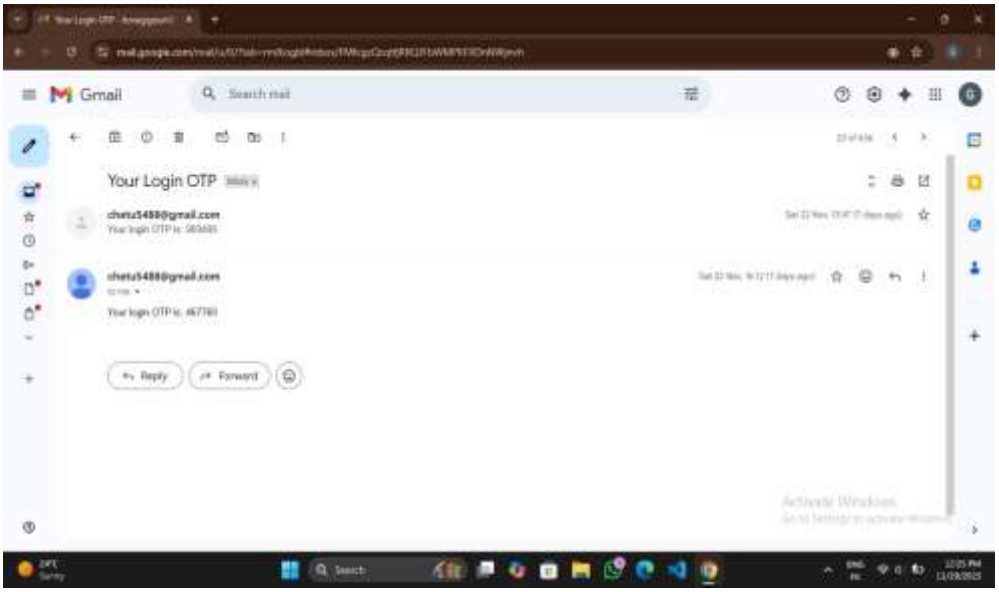

Figure: 2

The fig 2, illustrates the operational flow of the secure communication system, showing how users authenticate through email-based OTP verification before accessing the messaging and collaboration features. It highlights the transition from registration to real-time interaction, demonstrating the system's ability to manage secure login, message exchange, and group communication within a unified platform.

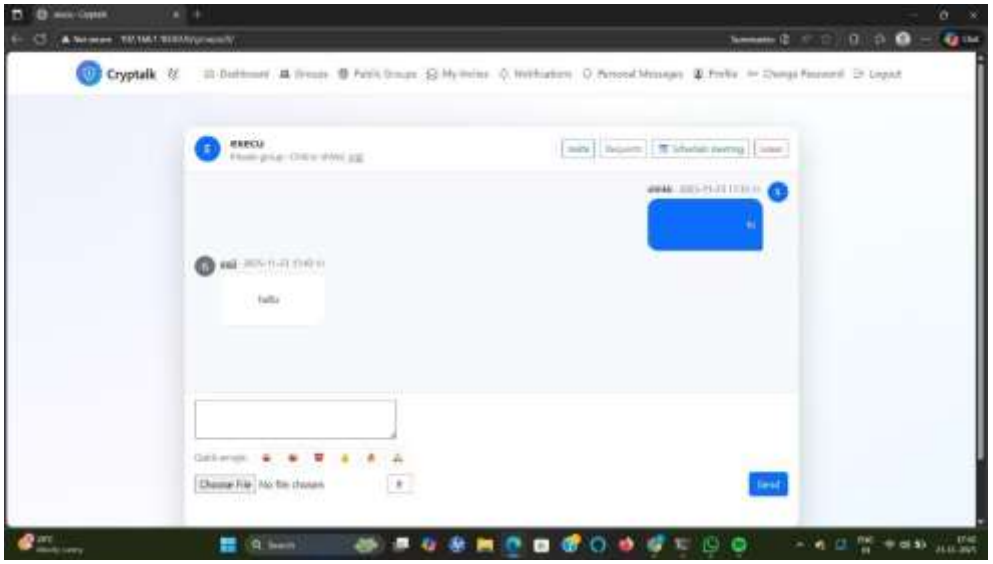

Figure: 3

Fig 3, illustrates how authenticated users interact with the group management module, showing the creation and functioning of both public and private groups. Public groups enable open participation for all verified users, whereas private groups operate on invitation-based access. This structure, as visualized in the figure, supports flexible collaboration while ensuring controlled and privacy-focused communication for sensitive interactions.

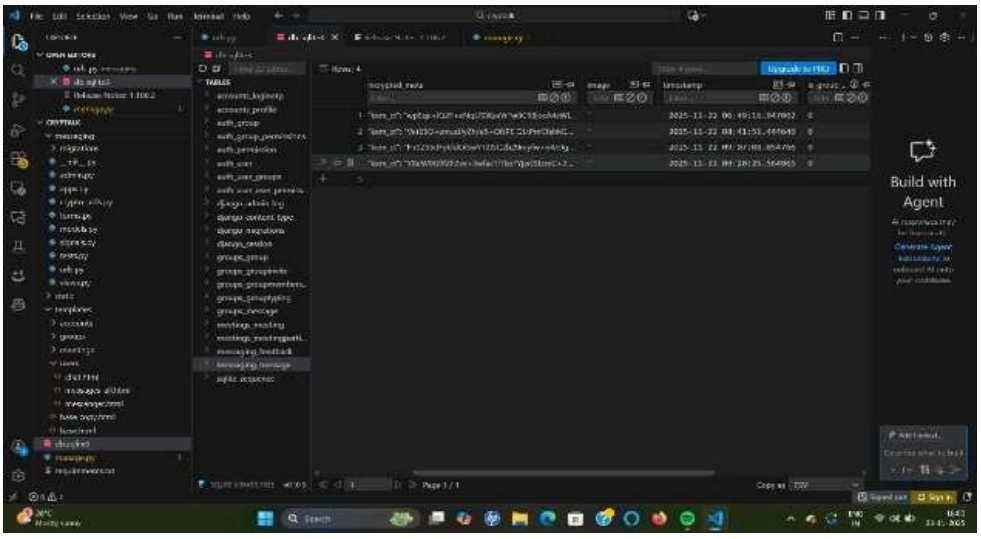

Figure: 4

Fig 4, shows how CrypTalk encrypts messages using a hybrid approach that combines Kyber with AES. The figure highlights the generated ciphertext, which appears before the message is sent to the receiver. This clearly shows that the system never shares or stores the original message

in readable form. By using Kyber for secure key exchange and AES for fast encryption, the platform maintains strong privacy without slowing down real-time chat performance.

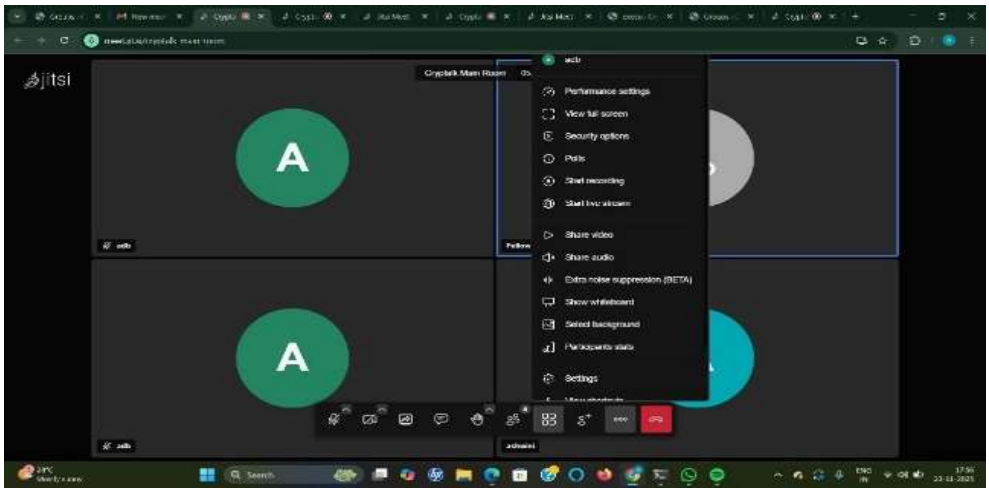

Figure: 5

Fig 5, presents the meeting interface of CrypTalk, showing how real-time collaboration tools are integrated within a single video conferencing space. The interface supports stable video communication while providing additional features such as a shared whiteboard, quick polling options, noise reduction, and both group and private messaging. As shown in the figure, these elements work together to create a secure, smooth, and interactive environment, making the platform highly suitable for efficient communication within small teams.

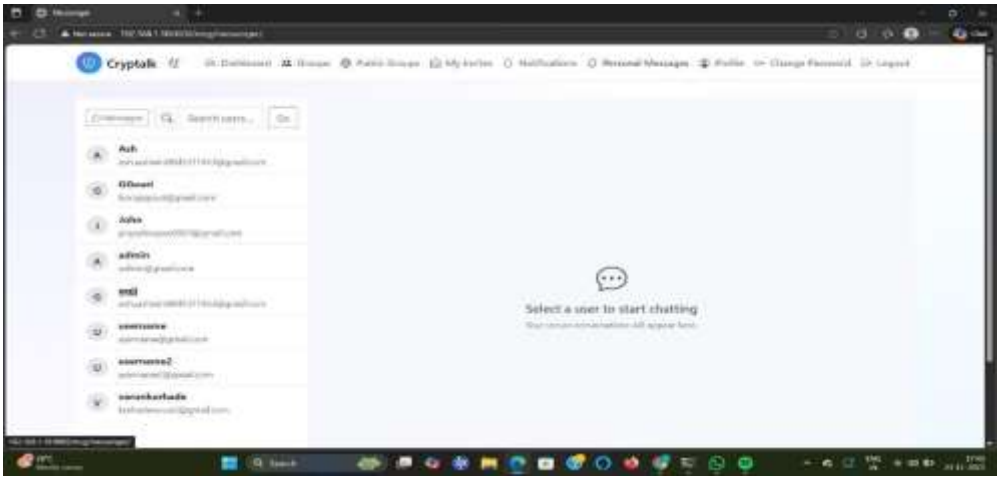

Figure: 6

Fig 6, illustrates the group creation interface in CrypTalk, demonstrating how the platform enables users to build structured and secure communication spaces. As shown in the figure, users can create private groups restricted to invited members, ensuring that sensitive or confidential discussions remain protected. They can also create public groups that any authenticated user may join, supporting open and collaborative interaction. This dual group-creation model provides flexibility while maintaining strong access control, allowing teams to organize their communication efficiently and securely.

CONCLUSION

CrypTalk demonstrates that secure digital communication can be achieved without compromising usability or accessibility. By integrating Kyber-based post-quantum encryption with AES symmetric encryption, the system offers a robust defense against both conventional cyberattacks and emerging quantum-level threats. Its dual-room architecture—public rooms for open collaboration and private rooms with strict admin control—ensures that users can participate in discussions with the appropriate level of privacy and oversight. The inclusion of admin-level permissions such as participant approval, user removal, and controlled access to meetings strengthens the reliability of group communication and helps maintain a safe, trustworthy environment for sensitive discussions.

Beyond security, CrypTalk prioritizes practical, real-time collaboration by supporting encrypted messaging, video communication, file sharing, voice messages, and user interactions such as reactions. The use of HTML for the interface, Django with Python for backend logic, and SQLite for lightweight data management illustrates that powerful communication tools can be built using accessible technologies. Overall, CrypTalk provides a balanced framework where strong cryptography, structured access control, and modern communication features work together seamlessly. This project highlights a promising direction for future secure communication systems and sets the groundwork for expanding advanced,user-centric,and quantum-resilient communication platforms.

REFERENCES

1. Cherkaoui and I. Dey, “QMA Complete Quantum-Enhanced Kyber: Provable Security

through CHSH Nonlocality," arXiv, 2025.

2. E. D. Demir, B. Bilgin, and M. C. Onbasli, "Performance Analysis and Industry Deployment of Post-Quantum Cryptography Algorithms," arXiv, 2025.
3. M. A. Ehsan, W. Alayed, A. U. Rehman, W. Hassan, and A. Zeeshan, "Post-Quantum KEMs for IoT: A Study of Kyber and NTRU," Symmetry, 2025.
4. Y. Ahmed, N. Elmrabit, and M. Yousefi, "Enhancing the Security of Classical Communication with Post-Quantum Authenticated-Encryption Schemes," Computers, 2024.
5. A. Mamun, A. Abrar, M. Rahman, and M. S. Salek, "Enhancing Transportation Cyber-Physical Systems Security: A Shift to Post-Quantum Cryptography," arXiv, 2024.
6. T.-T. Nguyen, N.-Q. Luc, and T.-T. Dao, "Developing Secure Messaging Software Using Post-Quantum Cryptography," Engineering, Technology & Applied Science Research, 2023.
7. V. Maram and K. Xagawa, "Post-Quantum Anonymity of Kyber," IACR ePrint, 2022.
8. S. Fluhrer, "The Use of AES-256-GCM and Related Modes in Secure Messaging Systems," *Journal of Applied Cryptographic Engineering*, pp. 1–15.

Cite as:

Gouri Boragi, Ashwini N. H, Priya Shivapur, Kurhade Varun Vijay, Priyanka Desurkar. (2026). CrypTalk: A Secure Multi-Modal Communication Framework Using Kyber and AES. Journal of Research in Computer Science and Engineering, 11(1), 33-43.

https://doi.org/10.5281/zenodo.19143744