Design and Implementation of a Secure College Campus Chat Application using AES Encryption

Aditi Mulay , Vaibhavi Sutar , Mahek Shaikh
Department of Computer Engineering (CO) D Y Patil Polytechnic, Ambi Pune, Maharashtra, India

Guide: Shubhangi Shiwankar

How to Cite this Article:
Mulay, A., Sutar, V. & Shaikh, M. (2026). Design and Implementation of a Secure College Campus Chat Application using AES Encryption. International Journal of Creative and Open Research in Engineering and Management, 02(04). https://doi.org/10.55041/ijcope.v2i4.212

https://doi.org/10.55041/ijcope.v2i4.212

ABSTRACT

In the digital era, communication through messaging applications has become an essential part of daily life, especially among students in a college environment. However, most existing chat applications lack sufficient security measures to protect sensitive user data and ensure controlled communication. This paper presents the design and implementation of a College Campus Secure Chat Application, which focuses on providing secure, reliable, and moderated communication within a campus.

The proposed system uses AES (Advanced Encryption Standard) to encrypt messages before transmission and decrypt them upon reception, ensuring confidentiality. In addition to encryption, the system incorporates device-level security features such as root detection, debugger detection, and emulator detection to prevent unauthorized access. Furthermore, the application includes abuse detection and temporary user blocking mechanisms to maintain a disciplined communication environment. The integration of Firebase enables real-time messaging and efficient data handling.

The results demonstrate that the application successfully ensures secure communication while maintaining usability. The combination of encryption, device validation, and user moderation provides a comprehensive solution for secure campus communication.

Keywords: AES Encryption, Secure Chat Application, Firebase, Android Security, Abuse Detection, Data Protection

INTRODUCTION

Communication plays a vital role in the academic and social interactions of students within a college environment. With the increasing use of mobile applications, students rely heavily on digital platforms to exchange information. However, most general-purpose chat applications are not designed to meet the specific requirements of a controlled campus environment, where both security and discipline are essential.

This project introduces a secure chat application designed specifically for college campuses. The application is developed using Android for the frontend and Firebase for backend services, enabling real-time communication between users. The system is designed to provide a seamless and user- friendly experience while ensuring data security and privacy.

A key aspect of this application is the implementation of multiple security layers. AES encryption is used to protect messages, while additional features such as device validation, screenshot blocking, and abuse detection ensure that the platform remains secure and controlled.
This makes the application suitable for safe and reliable communication among students.

Furthermore, the increasing number of cyber threats and data breaches has raised serious concerns regarding the safety of digital communication platforms. Many widely used messaging applications store or transmit data without sufficient protection, making them vulnerable to unauthorized access. In a college environment, where students frequently share academic information, personal details, and important updates, ensuring secure communication becomes highly essential. Therefore, there is a strong need for a system that not only supports communication but also prioritizes data security and user privacy.

In addition to security, maintaining a respectful and disciplined communication environment is equally important. Traditional chat applications do not provide effective mechanisms to monitor or control user behavior, which can lead to misuse such as sharing inappropriate or abusive content. This can negatively impact the overall communication experience within the campus. To address this issue, the proposed system incorporates user moderation features that help in detecting and restricting such behavior, thereby promoting responsible communication among users.

LITERATURE REVIEW

The rapid growth of digital communication has led to the widespread adoption of chat applications across various domains, including educational environments. Several studies have focused on the development of real-time messaging systems that enable instant communication using cloud-based platforms. Technologies such as Firebase have been widely used to support real-time data synchronization, scalability, and efficient message delivery. However, many of these systems primarily focus on functionality and performance, often overlooking critical aspects of data security and user privacy.

To address security concerns, researchers have explored the use of encryption techniques in chat applications. Among these, the Advanced Encryption Standard (AES) is one of the most commonly used symmetric encryption algorithms due to its efficiency, speed, and strong security capabilities. Various studies highlight that implementing AES encryption at the application level ensures that messages remain confidential during transmission. Despite its effectiveness, encryption alone is not sufficient to guarantee complete security, as vulnerabilities may still exist at the device or application level.

Recent research has emphasized the importance of incorporating additional security mechanisms beyond encryption. These include device-level security features such as root detection, emulator detection, and protection against debugging tools. Such mechanisms help in preventing unauthorized access, reverse

engineering, and execution of applications in compromised environments. Furthermore, studies suggest that secure application design should also consider protection against data leakage through features like screenshot prevention and secure storage practices.

Another significant area of research focuses on user behavior monitoring and content moderation in communication platforms. Many existing chat applications lack effective mechanisms to detect and control abusive or inappropriate content, leading to misuse and negative user experiences. Researchers have proposed the integration of automated filtering systems and rule-based detection methods to identify offensive language and enforce communication guidelines. These approaches contribute to maintaining a safe and disciplined environment, especially in restricted domains such as educational institutions.

In conclusion, the literature indicates that while significant progress has been made in developing chat applications with real-time capabilities and basic encryption, there remains a gap in integrating comprehensive security and moderation features within a single system. This project builds upon existing research by combining AES-based encryption, device-level security, and user moderation techniques to develop a secure and controlled chat application tailored for a college campus environment.

Problem Statement

With the increasing use of digital communication platforms, students heavily rely on chat applications for academic and personal interactions. However, most existing messaging applications are designed for general use and do not meet the specific security and control requirements of a college campus environment. These platforms often lack strong data protection mechanisms, making sensitive user information vulnerable to unauthorized access, interception, and misuse.

Another major issue is the absence of effective user moderation systems in existing chat applications. Users can easily send inappropriate or abusive messages without any restriction, which can negatively impact the communication environment. In a college setting, maintaining discipline and respectful interaction is essential, but current systems fail to enforce such standards effectively.

Additionally, many chat applications do not include sufficient protection against insecure devices such as rooted phones, emulators, or debugging environments. These vulnerabilities increase the risk of data breaches, reverse engineering, and manipulation of application behavior. Therefore, there is a need for a secure communication system that ensures data confidentiality, restricts access from insecure environments, and promotes responsible user behavior.

Proposed Solution

To address the identified challenges, this project proposes a secure college campus chat application that integrates multiple layers of security along with real-time communication capabilities. The system is designed using Android for the frontend and Firebase as the backend, enabling efficient and seamless message exchange between users. The primary focus is to ensure that communication remains secure, private, and controlled within the campus environment.

The proposed system implements AES (Advanced Encryption Standard) to encrypt messages before transmission and decrypt them at the receiver end. This ensures that even if data is intercepted, it remains unreadable to unauthorized users. In addition to encryption, device-level security features such as root detection, emulator detection, and debugger detection are incorporated to prevent the application from running on compromised devices.

Furthermore, the system includes a user moderation mechanism to maintain discipline within the platform. Messages are analyzed for abusive or inappropriate content, and users who violate guidelines are warned and temporarily restricted from sending messages. Screenshot blocking is also implemented to prevent data leakage from the application interface. By combining encryption, device security, and user behavior control, the proposed solution provides a comprehensive and secure communication

Methodology

The proposed system follows a structured and secure workflow to ensure safe communication between users. When a user composes a message, the system first performs validation to check for any inappropriate or abusive content using a predefined filtering mechanism. If the message passes the validation stage, it is processed further; otherwise, a warning is generated, and necessary restrictions are applied.

After validation, the message is encrypted using the Advanced Encryption Standard (AES) before being transmitted. The encrypted message is then sent to the backend using Firebase, which handles real-time data synchronization and storage. On the receiver's end, the encrypted message is fetched and decrypted using the same encryption key, allowing the original content to be displayed securely.

In parallel, device-level security checks such as root detection, emulator detection, and debugger detection are continuously performed to ensure that the application is running in a trusted environment. Additional measures such as screenshot blocking are implemented to prevent data leakage. This layered approach ensures both data security and controlled communication throughout the system.

Technologies Used

The development of the proposed system involves a combination of modern technologies to ensure efficiency, scalability, and security. The frontend of the application is developed using Android Studio with Java, providing a user-friendly interface for interaction. Firebase is used as the backend platform to enable real-time messaging, user authentication, and cloud-based data storage.

For securing communication, AES (Advanced Encryption Standard) is implemented to encrypt and decrypt messages, ensuring confidentiality. Device-level security mechanisms such as root detection, emulator detection, and debugger detection are integrated to prevent unauthorized access. Additional features like abuse detection and screenshot blocking are incorporated to enhance overall system security and reliability.

System Architecture

The system architecture follows a client-server model where users interact through an Android application connected to a cloud-based backend. The architecture consists of three main components: the user interface (frontend), the security layer, and the backend services.

The frontend handles user interactions such as message input and display. Before any message is transmitted, it passes through the security layer, where validation and encryption are performed. The encrypted message is then sent to Firebase, which acts as the central server for storing and synchronizing data in real time.

On the receiver side, the message is retrieved from Firebase, passed through the decryption module, and then displayed to the user. Security mechanisms operate continuously in the background to ensure that the system remains protected from threats. This architecture ensures secure, efficient, and real- time communication between users.

Performance Analysis

The performance of the proposed system was evaluated based on security, efficiency, and usability. The encryption and decryption processes using AES were found to be fast and efficient, with minimal impact on message delivery time. Real-time communication through Firebase ensured quick synchronization of messages between users without noticeable delays.

The device-level security checks successfully prevented the application from running on insecure environments such as rooted devices and emulators. The abuse detection system effectively identified inappropriate content and enforced restrictions without affecting normal communication.
Overall, the system demonstrated reliable performance with strong security features, making it suitable for practical implementation in a college environment. The balance between security and usability ensures a smooth user experience.

In addition to system efficiency, the application was also analyzed in terms of security performance under different scenarios. The AES encryption mechanism ensured that all transmitted messages remained secure and unreadable during data transfer. Even when tested with multiple message exchanges, the encryption and decryption processes maintained consistency without causing noticeable delays. This demonstrates that the system is capable of handling secure communication without compromising performance.

The application was further evaluated for its reliability and robustness. Features such as abuse detection and temporary user restriction operated effectively without interrupting normal user interactions. The system maintained stability even during continuous usage, and no major performance issues were observed. These results indicate that the proposed system not only provides strong security but also maintains a smooth and reliable user experience, making it suitable for real-world deployment in a college environment.

Advantages of Proposed System

1. Provides secure communication using AES encryption, ensuring that messages remain confidential and protected from unauthorized access.

2. Ensures data privacy and confidentiality during transmission and storage of messages.

3. Implements device-level security such as root detection, emulator detection, and debugger detection to prevent usage on insecure devices.

4. Reduces risk of data breaches and hacking attempts by restricting access from compromised environments.

5. Includes abuse detection system to identify and block inappropriate or offensive messages. Maintains a disciplined communication environment by warning and temporarily blocking users who violate rules.

6. Prevents data leakage through screenshot blocking feature.

7. Supports real-time messaging using Firebase, ensuring fast and efficient communication.

8. Maintains good performance even with multiple security layers applied.

9. Provides a user-friendly interface, making it easy for students to use without technical knowledge.

10. Offers scalability, allowing the system to handle multiple users simultaneously.

11. Ensures reliable and stable performance during continuous usage.

12. Combines multiple security features into a single integrated system, making it more effective than traditional chat applications.

Suitable for college campus environment, where both security and discipline are important.

Future Scope

The proposed College Campus Secure Chat Application provides a strong foundation for secure communication; however, there are several opportunities for further enhancement and expansion. One of the primary areas for future development is the implementation of more advanced security mechanisms. Although AES encryption ensures a high level of data protection, incorporating advanced encryption techniques along with secure key management strategies can further strengthen the system. Additionally, integrating multi-factor authentication can significantly improve account security by ensuring that only authorized users can access the application, thereby reducing the risk of unauthorized login attempts.

Another important area of improvement lies in enhancing the abuse detection mechanism. Currently, the system uses a predefined set of keywords to identify inappropriate content. In the future, this can be upgraded by incorporating Artificial Intelligence and Machine Learning techniques to enable context-based detection. AI-driven models can analyze user behavior and message patterns more effectively, allowing the system to detect subtle forms of misuse that may not be identified through simple keyword filtering. This will result in a more intelligent and adaptive moderation system, ensuring a safer communication environment.

The functionality of the application can also be extended by adding new communication features such as voice calling, video calling, and secure file sharing. These features will make the application more versatile and capable of meeting a wider range of user needs. Additionally, implementing end-to-end encryption with dynamic key exchange can further enhance the privacy and security of communication. Such improvements will make the application comparable to modern communication platforms while maintaining its focus on security and control.

From a scalability perspective, the system can be expanded to support a larger number of users across multiple colleges or institutions. By optimizing the backend infrastructure and database management, the application can handle high traffic efficiently without compromising performance. Integration with existing college systems, such as academic notifications, attendance tracking, and administrative announcements, can transform the application into a comprehensive campus management and communication platform.

Furthermore, improving the user interface and overall user experience is another key aspect of future development. A more intuitive and visually appealing design can increase user engagement and satisfaction. Providing cross-platform compatibility by developing versions for iOS and web browsers will also enhance accessibility, allowing users to access the application from different devices seamlessly.

CONCLUSION

The proposed College Campus Secure Chat Application successfully addresses the key limitations of existing messaging systems by integrating multiple layers of security with real-time communication capabilities. In today's digital environment, where data privacy and secure communication are of utmost importance, the need for a controlled and reliable messaging platform is more significant than ever. This project provides a practical solution by combining advanced encryption techniques, device- level security, and user moderation features into a single unified system.

One of the major achievements of the system is the implementation of AES (Advanced Encryption Standard), which ensures that all messages exchanged between users remain confidential and protected from unauthorized access. By encrypting messages before transmission and decrypting them at the receiver's end, the application guarantees secure data exchange. Additionally, the integration of device-level security mechanisms such as root detection, emulator detection, and debugger detection ensures that the application operates only in trusted environments, thereby reducing the risk of potential security threats and attacks.

The system also emphasizes maintaining a disciplined communication environment by incorporating an effective abuse detection and user restriction mechanism. By identifying inappropriate content and temporarily blocking users who violate communication guidelines, the application promotes responsible behavior among users. This feature is particularly important in a college campus setting, where maintaining a respectful and safe communication space is essential. Furthermore, the inclusion of screenshot blocking enhances data protection by preventing the leakage of sensitive information.

Another significant contribution of the proposed system is its ability to balance security with performance and usability. Despite the integration of multiple security layers, the application ensures smooth and efficient real-time communication through Firebase. The user-friendly interface makes the system accessible to students without requiring technical expertise, thereby increasing its usability and acceptance. The system demonstrates that strong security measures can be implemented without compromising user experience.

In conclusion, the College Campus Secure Chat Application presents a comprehensive and robust approach to secure communication within an academic environment. By addressing issues related to data security, unauthorized access, and user behavior, the system provides a safe and controlled platform for interaction. The integration of multiple security features, along with real-time communication capabilities, makes the application a valuable solution for modern digital communication challenges.

REFERENCES

Afreen, A. & Ivaturi, S. (2025). A Systematic Literature Review on End-to-End Cryptographic Protocols in Secure Messaging Applications. SSRN.

— A comprehensive survey of cryptographic protocols like forward secrecy, metadata protection, and group messaging security.

SSRN

Saharan, M., Kumar, N., Kumar, V., & Juneja, A. (2024). Secure End-to-End Chat Application: A Comprehensive Guide. IIETA Journal of Radiocommunications and Electromagnetics.

— Covers technical design of secure chat systems with end-to-end encryption and implementation considerations. iieta.org

Durge, S. C. & Tiwari, S. S. (2025). SecureLink: A Serverless Peer-to-Peer Messaging System for Confidential Conversations. IJRASET.

— Proposes a secure peer-to-peer messaging architecture without centralized server reliance, relevant for campus chat scenarios. IJRASET

Dabola, S., Tomer, V., Singh, N., Madan, P., & Jhinkwan, A. (2024). Chat Secure-Messaging Application Based on Secure Encryption Algorithm. IJRASET.

— Focuses on integrating cryptography with chat applications for data security, useful for encryption strategy sections.

IJRASET

Ali, A. H. & Sagheer, A. M. (2017). Design of Secure Chatting Application with End-to-End Encryption for Android Platform. Iraqi Journal for Computers and Informatics.

— Discusses ECC key exchange (ECDH) + AES encryption for a mobile secure chat, good reference for implementation choices.

ResearchGate

Onik, A. R., Brown, J., & Walker, C. (2025). A Systematic Literature Review of Secure Instant Messaging Applications from a Digital Forensics Perspective. ACM Computing Surveys, 57(9).

— Reviews security features and dangers in secure messaging systems, valuable theoretical context.