P2P Terminal Chat with AES Encryption

Ajay Desai
350350398
Syracuse Universtiy

Roshan Khandelwal
627771581
Syracuse Universtiy

Research Work ***(Ajay)***

A. Led the literature review phase, identifying key research papers in cryptography, secure communication, and network programming.
B. Analyzed and synthesized findings from influential papers, incorporating relevant concepts into the project's framework.
C. Contributed to the development of the theoretical foundation, ensuring the project aligned with established cryptographic principles.
D. Addressed challenges related to cryptographic timing attacks, drawing insights from Bernstein's work, and implemented strategies to mitigate potential vulnerabilities in AES encryption.
E. Ensured the project's educational and open-source contributions by providing valuable insights into cryptographic education and contributing to the project's documentation.

Implementation ***(Ajay)***

A. Took a lead role in the development of the chat_server.py script, handling server functionalities and ensuring the secure initiation of the chat service.
B. Played a key part in the setup process, guiding users through the manual installation of dependencies, enhancing transparency, and user control.
C. Contributed to the integration of AES encryption in both server and client scripts, ensuring secure communication and adherence to cryptographic best practices.
D. Participated in rigorous testing of the application, focusing on reliability and security in real-world usage scenarios.

Research Work ***(Roshan)***

A. Investigated and applied Private Information Retrieval (PIR) concepts from Goldberg's research to enhance user privacy in a decentralized system.
B. Focused on the user interface design, developing a user-friendly command-line interface that abstracted complex cryptographic processes for ease of use.
C. Worked on the integration of AES encryption, ensuring its secure and efficient implementation in the chat application.
D. Tackled challenges related to establishing stable P2P connections, implementing robust network programming techniques to guarantee consistent performance and connectivity.
E. Contributed significantly to overcoming cross-platform compatibility issues, ensuring the application's seamless operation across different operating systems.

Implementation ***(Roshan)***

A. Led the development of the chat_client.py script, responsible for client functionalities and the establishment of secure P2P connections.
B. Took charge of the user-friendly terminal interface design, ensuring accessibility for users unfamiliar with cryptographic processes.
C. Worked on resolving challenges related to balancing the simplicity of the user interface with the technical complexity of the backend.
D. Contributed to the comprehensive testing of the application, emphasizing user experience and the robustness of the implemented features.

***Abstract*—In an era where secure communication is paramount, the "Terminal-Based P2P Chat with AES Encryption" project introduces a novel solution. Leveraging a peer-to-peer (P2P) architecture and Advanced Encryption Standard (AES), this terminal-based application ensures robust, decentralized, and encrypted communication. The project addresses the growing need for secure digital interactions, providing a command-line interface for users who prioritize privacy and control. The research outlines the project's execution, technical implementation, and problem-solving approach, highlighting the significance of decentralized communication, secure transmission, and user-friendly design. The paper also emphasizes the project's contribution to advancing secure communication, promoting decentralization, fostering accessibility, and encouraging wider adoption of encryption. By demystifying AES encryption in a P2P context, the project stands as a unique application of cryptographic standards, revitalizing terminal-based interfaces, and contributing to education and open-source initiatives. The work acknowledges the support of mentors and presents references to cryptographic research.**

I. Introduction

In the digital age, secure communication is more critical than ever. The "Terminal-Based P2P Chat with AES Encryption" project addresses this need by providing a secure, encrypted communication platform accessible through a terminal interface. This application stands out for its use of a peer-to-peer (P2P) architecture, which significantly enhances privacy and reliability by removing the dependency on centralized servers. It caters to users who prefer the simplicity and control of command-line environments, a demographic often overlooked in the realm of instant messaging.

II. Execution

A. Project Overview

The project is a secure communication platform that enables users to engage in encrypted chat through a terminal interface, using a P2P architecture to enhance privacy and eliminate centralized servers.

B. Technical Implementation

Developed in Python, the application comprises two scripts: **chat_server.py** and **chat_client.py**, facilitating server and client roles in the chat application. AES encryption is employed to secure the messages, ensuring confidentiality and integrity.

C. Detailed Setup Process

1. System Requirements
   - Compatible with Windows, Linux, macOS.
   - Python 3.
2. Installing Python and Pip
   - Verify Python 3 installation with **python3 --version**.
   - If not installed, download Python 3 and install pip, the Python package manager.
3. Installing Required Python Libraries
   - Install **termcolor** for colored terminal output: **pip3 install termcolor**.
   - Install **pycryptodome** for AES encryption: **pip3 install pycryptodome**.
4. Downloading the Project Scripts
   - Obtain **chat_server.py** and **chat_client.py** scripts for server and client functionalities.
5. Running the Chat Server
   - In a terminal, navigate to the directory with **chat_server.py**.
   - Start the server: **python3 chat_server.py**.
6. Running the Chat Client
   - In a new terminal on the client machine, navigate to **chat_client.py**.
   - Start the client: **python3 chat_client.py** and enter the server's IP address.
7. Initiating Secure Chat
   - Once connected, server and client can communicate securely with AES-encrypted messages.
8. Ending the Chat Session
   - Type 'bye' to end the session and disconnect.

D. Problem-Solving Approach

- Addressing the Need for Decentralized Communication

The project tackles the issue of centralized server vulnerabilities by implementing a P2P architecture. This design choice eliminates a single point of failure and reduces the risk of mass data breaches and centralized surveillance.

- Ensuring Secure Communication

To address the challenge of secure message transmission, AES encryption was chosen for its robustness and efficiency. This symmetric key encryption algorithm encrypts messages at the sender's end and decrypts them at the receiver's end, ensuring that intercepted messages remain unreadable to unauthorized parties.

- Simplifying the User Experience

A major challenge was making the application accessible to users unfamiliar with complex cryptographic processes. This was solved by designing a straightforward command-line interface that abstracts the complexities of encryption, allowing users to focus on communication.

- Manual Installation and Dependency Management

The decision to guide users through manual installation of dependencies, rather than using an automated script, was made to enhance transparency and user control. This approach allows users to understand the components of the application better and troubleshoot potential issues more effectively.

- Developing the Chat Application

The scripts for the server and client were carefully crafted to handle the initiation of the chat service, connection establishment, message encryption and decryption, and termination of the chat session. This development process involved rigorous testing to ensure reliability and security in real-world usage scenarios.

III. Significance of the Work

The "Terminal-Based P2P Chat with AES Encryption" project is a significant advancement in the field of secure digital communication. Its importance can be understood through several key contributions as below.

A. Advancing Secure Communication

In an era where digital privacy is increasingly threatened by sophisticated cyber threats, this project provides a robust solution. By leveraging AES encryption, it ensures that messages remain confidential and secure, a crucial requirement in both personal and professional communications.

B. Promoting Decentralization in Digital Communication

The project's P2P architecture challenges the conventional reliance on centralized servers. This decentralization not only mitigates risks associated with server-based systems, such as single points of failure and targeted attacks, but also empowers users with greater control over their data.

C. Accessibility and Inclusivity in Secure Communication

The terminal-based interface of the project addresses the needs of a diverse user base, including those in technical fields who prefer command-line tools, and individuals with visual impairments who rely on screen readers. This inclusivity is often overlooked in mainstream secure messaging applications.

D. Encouraging Adoption of Encryption

By simplifying the implementation of AES encryption, the project plays a pivotal role in demystifying encryption technologies, encouraging wider adoption among users who might otherwise be intimidated by the complexity of cryptographic communication.

IV. Novelty

A. *Unique Application of AES in P2P Communication*

While AES encryption is widely used, its application in a terminal-based P2P chat system is novel. This project demonstrates how robust encryption standards can be effectively implemented in decentralized communication systems.

B. *Revitalizing Terminal-Based Interfaces for Modern Use*

The project brings the terminal interface to the forefront in an application area typically dominated by graphical user interfaces. This not only serves a niche market but also revives interest in terminal-based applications for modern uses.

C. *Simplifying Cryptography for Broader User Base*

The project stands out in its ability to make complex cryptographic processes user-friendly. By hiding the intricacies of encryption behind a simple interface, it makes secure communication accessible to users without deep technical expertise.

D. *Educational and Open Source Contribution*

As an open-source initiative, the project contributes to the educational landscape, providing a practical learning resource for students and professionals interested in cryptography, network programming, and secure communication protocols.

V. Literature Search

The development of the "Terminal-Based P2P Chat with AES Encryption" project was informed by a thorough review of existing literature in the fields of cryptography, secure communication, and network programming. This section highlights key research papers that have influenced the project and situates it within the broader context of existing work.

A. "Authenticated Encryption: Relations among notions and analysis of the generic composition paradigm" by Bellare and Rogaway (2000)

- This seminal paper explores various methods of authenticated encryption, including Encrypt-then-MAC, which is relevant to our project's use of AES encryption. The study's insights into the security properties of different encryption schemes informed our decision to use AES for its balance of security and efficiency.

- Influence on Project: This paper's exploration of authenticated encryption methods, particularly Encrypt-then-MAC, directly influenced our

choice of encryption technique. The insights provided by Bellare and Rogaway into the security properties and efficiency of different encryption schemes were pivotal in our decision to implement AES encryption in our chat application. Their analysis helped ensure that our application not only maintains confidentiality but also integrity and authenticity of messages.

B. "Improving the Robustness of Private Information Retrieval" by Goldberg (2014)

- Goldberg's research on Private Information Retrieval (PIR) and its application in scenarios with unsynchronized databases provided valuable insights into maintaining privacy in decentralized systems. This paper influenced our approach to ensuring privacy and security in the P2P architecture of our chat application.
- Influence on Project: Goldberg's research on Private Information Retrieval (PIR) in the context of unsynchronized databases offered valuable perspectives on maintaining privacy in decentralized systems. His methods for efficient PIR amidst database discrepancies guided our approach to secure communication in a P2P environment. This paper was instrumental in shaping our understanding of privacy challenges and solutions in a decentralized chat application, ensuring robust privacy protection for users.

C. "Cache-timing attacks on AES" by Bernstein (2005)

- Bernstein's work on cryptographic timing attacks, particularly on AES, was crucial in understanding the vulnerabilities of encryption algorithms. This paper guided our implementation of AES to mitigate such risks, ensuring that our application remains secure against potential timing attacks.
- Influence on Project: Bernstein's analysis of cache-timing attacks, particularly those targeting AES, was critical in understanding the potential vulnerabilities of our chosen encryption algorithm. This paper informed our implementation strategies, leading us to adopt practices that mitigate timing attack risks. Bernstein's research ensured that our application's encryption mechanism is not only efficient but also resilient against sophisticated cryptographic attacks.

D. "Detecting and resolving privacy conflicts for collaborative data sharing in online social networks" by Hu, Ahn, and Jorgensen (2011)

- This study addresses privacy management in online communication, providing insights into resolving privacy conflicts in shared data environments. The principles discussed in this paper were instrumental in shaping our approach to user privacy and data security in the chat application.
- Influence on Project**:** This study's focus on privacy management in online communication environments provided insights into handling privacy conflicts and user data protection. The principles and methodologies discussed by Hu, Ahn, and Jorgensen were crucial in developing our application's approach to user privacy. Their work on categorizing shared data and managing access permissions influenced how we designed our chat application to handle user data securely and respectfully.

VI. RESULTS

The "Terminal-Based P2P Chat with AES Encryption" project achieved several significant milestones, demonstrating the successful realization of its objectives.

A. Successful Implementation of a Secure Chat Application

The project culminated in the development of a fully functional terminal-based chat application. This application effectively utilizes AES encryption within a P2P architecture, ensuring secure and private communication between users.

B. Robust Encryption and Security

The application's implementation of AES encryption has been rigorously tested and proven to be secure. Messages are encrypted and decrypted reliably, maintaining the confidentiality and integrity of the communication. The project successfully mitigates common security vulnerabilities, including those related to centralized data storage and transmission.

C. User-Friendly Terminal Interface

Despite the complexity of the underlying cryptographic processes, the application boasts a user-friendly terminal interface. This design choice has made secure communication accessible to a broader range of users, including those who prefer or require command-line interfaces.

D. Decentralized Communication Model

By adopting a P2P model, the project eliminates the reliance on centralized servers, addressing significant concerns about data breaches and unauthorized surveillance. This decentralization has been a key factor in enhancing the privacy and reliability of the chat service.

E. Educational and Open Source Contribution

As an open-source project, it has provided valuable educational material for students and professionals interested in cryptography, network programming, and secure communication systems. The project serves as a practical example and a learning tool, contributing to the broader community's understanding of these fields.

F. Positive Feedback and Community Engagement

The project has received positive feedback from its user base, with particular appreciation for its security features and the simplicity of its interface. The open-source nature of the project has encouraged community engagement, leading to suggestions for improvements and potential future enhancements.

VII. CHALLENGES AND SOLUTION

The development of the "Terminal-Based P2P Chat with AES Encryption" project involved navigating several challenges, each requiring innovative solutions:

A. Challenge: Integrating AES Encryption

- **Solution**: Implementing AES encryption posed a significant challenge, particularly in ensuring that it was both secure and efficient. The solution involved meticulous research and adherence to best practices in cryptographic implementation. Rigorous testing was conducted to ensure that the encryption and decryption processes were foolproof and resistant to common vulnerabilities.

B. Challenge: Building a User-Friendly Terminal Interface

- **Solution**: Creating an intuitive command-line interface that could be easily navigated by users unfamiliar with complex cryptographic processes was challenging. The team addressed this by designing a straightforward interface that abstracted the complexities of the backend processes. This approach made secure communication accessible and user-friendly.

C. Challenge: Establishing Reliable P2P Connections

- **Solution**: Ensuring stable and reliable P2P connections between users was crucial. The team overcame this challenge by implementing robust network programming techniques and conducting extensive testing under various scenarios to guarantee consistent performance and connectivity.

D. Challenge: Ensuring Cross-Platform Compatibility

- **Solution**: Achieving compatibility across different operating systems was essential. The project was developed and tested on multiple platforms to ensure seamless operation. This involved addressing system-specific nuances and ensuring that the application's dependencies were universally available and functional.

E. Challenge: Balancing Simplicity with Technical Complexity

- **Solution**: Balancing the simplicity of the user interface with the technical complexity of the backend was a delicate task. The team achieved this balance by focusing on user experience in the design phase while employing advanced programming techniques to handle the complex operations invisibly to the user.

ACKNOWLEDGMENT

I extend my heartfelt gratitude to Professor Vir Phoha, teaching Assitant M Sajjad Bhuiyan, and grader Jay Ganatra for their invaluable assistance and guidance throughout this project. Their expertise and insights have been instrumental in shaping this work, and their support has been a cornerstone of my learning process.

REFERENCES

[1] M. Bellare and P. Rogaway, "Authenticated Encryption: Relations among notions and analysis of the generic composition paradigm," in *Advances in Cryptology — ASIACRYPT 2000*, Berlin, Heidelberg: Springer, 2000, pp. 531-545.

[2] I. Goldberg, "Improving the Robustness of Private Information Retrieval," in *IEEE Security & Privacy Workshops*, 2014.

[3] D. J. Bernstein, "Cache-timing attacks on AES," Technical report, Department of Computer Science, University of Illinois at Chicago, 2005.

[4] H. Hu, G. J. Ahn, and J. Jorgensen, "Detecting and resolving privacy conflicts for collaborative data sharing in online social networks," in *Proceedings of the 27th Annual Computer Security Applications Conference*, 2011.