iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** III **Month of publication:** March 2024

DOI: https://doi.org/10.22214/ijraset.2024.58817

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue III Mar 2024- Available at www.ijraset.com

Chat Secure-Messaging Application Based on Secure Encryption Algorithm

Shashank Dabola[1], Vaibhav Tomar[2], Navpreet Singh[3], Dr. Parul Madan[4], Aryan Jhinkwan[5]
[1, 2, 3, 5]*Department of CSE, Graphic Era (Deemed to be University) Dehradun, India*
[4]*Assistant Professor, Department of CSE, Graphic Era (Deemed to be University), Dehradun, India*

Abstract: This study aims to explore the application of cryptography in various chat interfaces. Utilizing a systematic literature review methodology, we examine research conducted across various scientific platforms that bridge cryptography and the chat sector, as well as the intersection of cryptograph and database. The potential for advanced encryption algorithms to enhance the security of the user data is enormous. Implementing cryptography in chat interface presents competitive advantages, as numerous researchers have proposed and validated models that effectively optimize the use of cryptography in sharing data b/w the users.

I. INTRODUCTION

In an age dominated by digital interconnectedness, the exchange of sensitive information through various messaging platforms has become an integral part of daily communication. As individuals and organizations increasingly rely on these digital channels to transmit confidential data, the need to safeguard these exchanges against unauthorized access and interception has never been more critical.

The vulnerability of chat messages to potential eavesdropping, hacking, or unauthorized surveillance presents a substantial risk to privacy, confidentiality, and data integrity. Addressing these concerns necessitates the implementation of robust security measures, with encryption standing as a cornerstone in fortifying the confidentiality of digital conversations. The proliferation of messaging applications, from personal communication tools to enterprise-grade platforms, has led to a surge in the transmission of sensitive data—ranging from personal conversations and financial details to proprietary business information. However, the inherent susceptibility of these communications to cyber threats poses a formidable challenge to the confidentiality and security of such exchanges. Instances of data breaches, privacy infringements, and cyberattacks have underscored the pressing need for adopting stringent security measures to protect digital conversations. Encryption, as a fundamental technology, plays a pivotal role in securing these exchanges by encoding the contents of messages, rendering them unintelligible to unauthorized entities. Encryption standards serve as a framework for ensuring that messaging platforms and communication protocols employ robust cryptographic techniques to protect data from interception and unauthorized access. These standards encompass algorithms, key management practices, and secure protocols that collectively form the bedrock of secure communication.

II. LITERATURE SURVEY

This literature survey aims to examine existing research, studies, and articles pertaining to the implementation and impact of encryption standards in safeguarding chats, ensuring confidentiality, and mitigating potential risks associated with digital communication platforms.

A. Evolution of Chat Security and Encryption:

This section explores the historical evolution of chat security, tracing the progression from unencrypted communication channels to the incorporation of encryption standards in messaging platforms. It examines landmark developments, protocols, and encryption techniques adopted over time, emphasizing their significance in addressing security vulnerabilities in chat systems

B. Importance Of Encryption In Chat Securtiy

Examining the fundamental role of encryption in ensuring secure chats, this section delves into the core principles of encryption and its application in messaging platforms. It discusses how encryption transforms plaintext messages into ciphertext, elucidating the mechanisms behind symmetric and asymmetric encryption algorithms, and their relevance in protecting the confidentiality and integrity of chat data.

C. Encryption Standards and Protocols

This segment analyses the various encryption standards and protocols employed in securing chat communications. It scrutinizes widely utilized standards such as AES (Advanced Encryption Standard), RSA (Rivest-Shamir-Adleman), and others, evaluating their strengths, weaknesses, and applicability in different chat platforms.

Additionally, it explores secure communication protocols like TLS/SSL (Transport Layer Security/Secure Sockets Layer) and their integration into messaging applications.

D. Impact of Encryption Standards on Chat Security

This section investigates the direct impact and effectiveness of implementing encryption standards in enhancing chat security. It reviews case studies, empirical evidence, or industry reports highlighting instances where encryption standards have thwarted potential security breaches or unauthorized access, emphasizing the pivotal role played by encryption in preserving privacy and confidentiality.

E. User Perception and Acceptance of Encrypted Chats

This section focuses on user attitudes, perceptions, and adoption rates of encrypted chat platforms. It explores user motivations for embracing or resisting encryption-enabled messaging apps, addressing factors such as usability, trust, and perceived benefits or drawbacks of encrypted communications from the user's perspective.

F. Legal and Ethical Implications of Chat Encryption:

Delving into the legal and ethical dimensions, this segment examines the regulatory landscape and debates surrounding encryption standards in chat security. It analyzes legal frameworks, government policies, and debates on privacy versus law enforcement concerns, shedding light on the ethical dilemmas and societal implications associated with implementing encryption.

G. Industry Perspectives and Best Practices in Chat Security:

Drawing insights from industry practices, this segment examines how organizations, enterprises, and tech companies implement encryption standards in their messaging platforms. It investigates industry best practices, standards compliance, and the efficacy of security measures implemented by leading chat application providers.

H. Future Trends and Innovations in Chat Encryption

Envisioning the future of chat security, this section explores emerging trends and innovative approaches in encryption technologies. It discusses advancements in quantum cryptography, homomorphic encryption, post-quantum cryptography, and their potential applications in securing future chat systems.

I. Chanlanges and future Direction

Highlighting the challenges and limitations associated with encryption in chat security, this section discusses potential vulnerabilities, key management issues, and regulatory hurdles. It also suggests future research directions, exploring emerging encryption techniques, quantum-resistant cryptography, and strategies to overcome existing challenges in securing chats effectively.

III. METHODOLOGY

A. Research and Background Study

1) *Understanding Encryption Standards:* Conduct an in-depth study of the Double Ratchet Algorithm and AES encryption to grasp their principles, strengths, weaknesses, and compatibility for securing chat communications.

B. Design Phase

1) *System Architecture Design:* Design the architecture for the chat application incorporating the Double Ratchet Algorithm and AES encryption. Plan how messages will be encrypted, decrypted, and securely transmitted between users.
2) *Key Management Strategy:* Develop a strategy for key generation, exchange, and management for both the Double Ratchet and AES encryption. Decide on key rotation policies and procedures for secure handling of cryptographic keys.

C. Implementation

1) *Coding and Integration:* Implement the chat application using a programming language (e.g., Python, JavaScript) and relevant libraries or frameworks (such as Signal Protocol libraries for the Double Ratchet Algorithm and AES implementation libraries).
2) *Integration of Double Ratchet and AES:* Integrate the Double Ratchet Algorithm for secure key exchange and forward secrecy with AES encryption for message encryption/decryption within the chat application.

D. Testing and Validation

1) *Unit Testing:* Conduct unit tests to verify the functionality and correctness of the implemented Double Ratchet Algorithm and AES encryption modules.
2) *Integration Testing:* Test the integration of Double Ratchet and AES within the chat application to ensure proper communication, key exchange, encryption, and decryption.

E. Evaluation

1) *Performance Evaluation:* Measure the performance metrics such as encryption/decryption speed, computational overhead, and system resource utilization to assess the efficiency of the combined Double Ratchet and AES approach.
2) *Security Assessment:* Conduct security assessments and penetration tests to identify vulnerabilities, potential attacks, and overall resilience of the chat application against various threats.

F. User Testing and Feedback

1) *Usability Testing:* Engage real users to test the application's usability, ease of use, and user experience any identified issues or shortcomings in the implemented Double Ratchet and AES encryption.
2) *Gather Feedback:* Collect user feedback to understand their perceptions, concerns, and suggestions regarding the security features implemented using Double Ratchet and AES.

G. Documentation and Reporting

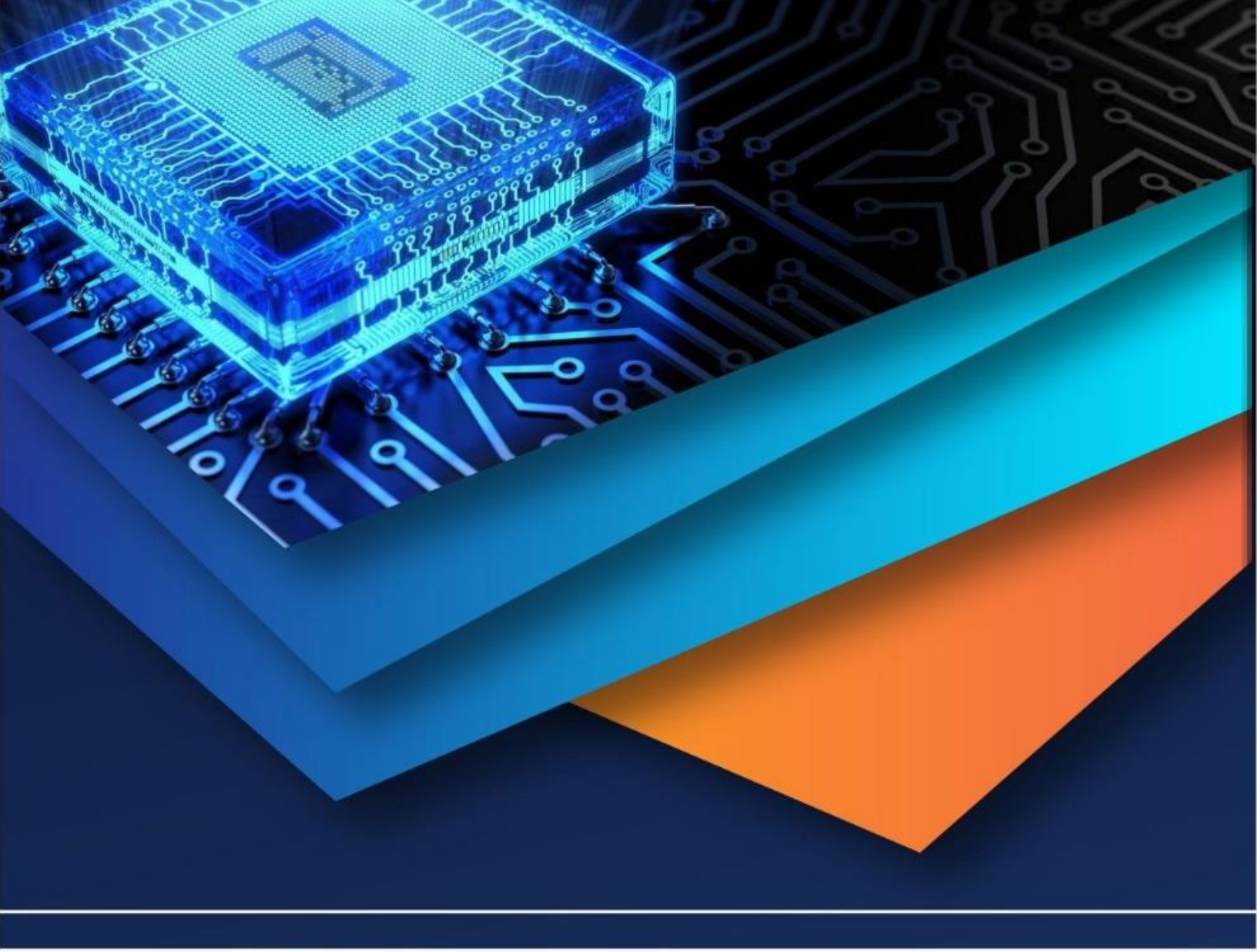
1) *Technical Documentation:* Document the implementation details, key design decisions, challenges faced, and solutions adopted during the development process.
2) *Report Generation:* Compile a comprehensive report summarizing the methodology, findings, results, and recommendations for further improvements or enhancements.

H. Refinement and Iteration

1) *Iterative Improvement:* Based on the evaluation results and user feedback, refine and iterate upon the application to address

REFERENCES

[1] M. Marlinspike and T. Perrin, “The double ratchet algorithm,” 2016. [Online]. Available: https://signal.org/docs/specifications/doubleratchet/doubleratchet.pdf
[2] J. Jaeger and I. Stepanovs, “Optimal channel security against fine grained state compromise: The safety of messaging,” in Advances in Cryptology – CRYPTO 2018, Part I, ser. Lecture Notes in Computer Science, H. Shechem and A. Boldyreva, Eds., vol. 10991. Santa Barbara, CA, USA: Springer, Heidelberg, Germany, Aug. 19–23, 2018, pp. 33–62. 1, 5
[3] B. Pottering and P. Rösler, “Asynchronous ratcheted key exchange,” Cryptology print Archive, Report 2018/296, 2018, https://eprint.iacr.org/2018/296. 1
[4] F. B. Durak and S. Vaud nay, “Bidirectional asynchronous ratcheted key agreement with linear complexity,” in IWSEC 19: 14th International Workshop on Security, Advances in Information and Computer Security, ser. Lecture Notes in Computer Science, N. Attrapadung and T. Yagi, Eds., vol. 11689. Tokyo, Japan: Springer, Heidelberg, Germany, Aug. 28–30, 2019, pp. 343–362. 1



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY