IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 12, Issue 11, November 2023

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 11, November 2023 ||

| DOI:10.15680/IJIRSET.2023.1211028 |

ASYNCSAFEGUARD: ADVANCED ASYNCHRONOUS SECURE MESSAGING APPLICATION

Sangam Bansode[1], Avinash Kurhe[2], Jadhav Rutwik[3], Prof. S.G.Joshi[4]

Department of Computer Engineering, Vishwabharati Academy's College of Engineering, Ahmednagar, India [1,2,3]

Professor, Department of Computer Engineering, Vishwabharati Academy's College of Engineering, Ahmednagar, India[4]

ABSTRACT: In response to the escalating demand for secure and efficient asynchronous messaging systems, extensive research within the realm of computer science has been undertaken. This study introduces a pioneering approach to asynchronous messaging, emphasizing both communication efficiency and fine-grained forward secrecy. The proposed system intricately merges cryptographic techniques with streamlined communication protocols to establish a robust framework for secure message transmission in an asynchronous environment. Notably, the incorporation of fine-grained forward secrecy enhances security by enabling users to encrypt messages in a manner that, even if a long-term secret key is compromised, only specific past messages are exposed, thereby minimizing potential damage. Through a comprehensive blend of rigorous analysis and experimental validation, this research substantiates the viability and efficacy of the proposed methodology. The results underscore its potential to significantly elevate the security and efficiency of asynchronous messaging systems across diverse real-world applications.

KEYWORDS: Asynchronous Messaging Systems, Cryptographic Techniques, Fine-Grained Forward Secrecy, Secure Message Transmission, Communication Efficiency, Robust Framework, Messaging System Efficiency.

I. INTRODUCTION

In today's fast-paced digital world, effective communication lies at the heart of all successful interactions. The advent of smartphones has revolutionized the way we connect with others, but ensuring the privacy and security of our messages has become increasingly paramount. Introducing our innovative Android application, designed with the sole purpose of facilitating efficient and fine-grained forward secure asynchronous messaging. This cutting-edge application redefines the way we communicate by combining advanced encryption techniques with seamless asynchronous messaging, ensuring that your conversations remain confidential and protected from unauthorized access. Whether you're discussing sensitive business matters or sharing personal moments with loved ones, our application provides a robust platform where privacy meets efficiency, promising a secure environment for all your communication needs.

Imagine a world where you can communicate freely without worrying about the prying eyes of third parties. Our Android application makes this vision a reality by offering forward secure asynchronous messaging capabilities, setting new standards in the realm of secure communication. With this application, you can enjoy real-time conversations with friends, family, and colleagues while being confident that your messages are shielded from eavesdroppers and potential threats.

The fine-grained control allows you to customize your security preferences, ensuring that your messages are accessible only to the intended recipients. Embracing the power of encryption and innovative technology, our application not only prioritizes your privacy but also delivers a user-friendly experience, making secure communication effortless and accessible to everyone. Welcome to a future where communication is not only efficient but also impenetrably secure – welcome to our forward-thinking Android messaging application.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 11, November 2023 ||

| DOI:10.15680/IJIRSET.2023.1211028 |

The landscape of secure messaging systems has witnessed significant advancements, particularly in the realm of asynchronous communication. In this context, the fusion of communication efficiency and fine-grained forward secrecy stands as a pivotal milestone. This innovative approach not only addresses the pressing need for secure communication in real-time but also ensures the integrity of past messages, even in the face of evolving cryptographic threats. By seamlessly integrating communication efficiency, which optimizes data transmission and processing, with fine-grained forward security, which safeguards the confidentiality of past conversations, this research endeavors to revolutionize asynchronous messaging. The intricate synergy of these two elements not only enhances user experience by facilitating swift and streamlined exchanges but also establishes a robust shield against potential breaches, ushering in a new era of secure, asynchronous communication.

II. RELATED WORK

In the realm of secure and efficient asynchronous messaging systems, previous research has laid a foundation for advancements, yet certain limitations persist. Existing approaches often grapple with the challenge of striking a balance between communication efficiency and robust forward secrecy. While cryptographic techniques are commonly employed to secure message transmission, the integration of fine-grained forward secrecy, allowing for selective disclosure of past messages in the event of a key compromise, remains an area of exploration. Some earlier systems may lack the comprehensive integration of cryptographic methods with communication protocols tailored for asynchronous environments, potentially leaving vulnerabilities in the security fabric.

Moreover, a drawback observed in certain asynchronous messaging systems is the absence of a nuanced approach to forward secrecy. In some cases, systems may rely on simplistic encryption methods that do not offer the granularity needed to safeguard past messages in the wake of key compromise scenarios. This limitation can pose a significant risk, particularly in environments where long-term secret keys are more susceptible to compromise. Additionally, existing systems might not sufficiently address the need for rigorous analysis and experimentation to validate the efficacy and viability of their proposed methods. The lack of comprehensive empirical evidence and a robust demonstration of the proposed approach's potential impact on real-world applications can hinder the adoption of these systems in practical settings.

In response to these drawbacks, the current study introduces a novel approach to asynchronous messaging that endeavors to overcome the limitations identified in prior works. By integrating cryptographic techniques with efficient communication protocols and emphasizing fine-grained forward secrecy, the proposed system aims to provide a more secure and efficient solution for secure message transmission in asynchronous environments. The research employs rigorous analysis and experimentation to validate the effectiveness of the proposed method, offering a promising avenue for addressing the shortcomings observed in existing systems and advancing the state-of-the-art in secure asynchronous messaging.

Existing research in the realm of Android applications has paved the way for innovative solutions in the domain of efficient and fine-grained forward secure asynchronous messaging. Several studies have focused on enhancing communication protocols to ensure seamless and secure data exchange on mobile devices. Researchers have explored various encryption techniques and algorithms to provide forward security, meaning that even if encryption keys are compromised in the future, past communications remain confidential. Additionally, efforts have been made to achieve fine-grained control over message delivery, enabling users to manage message permissions and access levels more effectively. These advancements have not only bolstered the security aspects of messaging applications but also optimized their efficiency, ensuring a smooth and reliable communication experience for Android users. As a result, the existing work in this field forms a strong foundation for the development and enhancement of Android applications that prioritize both security and efficiency in asynchronous messaging systems.

III. PROPOSED METHODOLOGY

In the contemporary digital landscape, the imperative for efficient and secure communication is undeniable. The ubiquity of Android smartphones accentuates the demand for messaging applications that not only exhibit high efficiency but also prioritize robust security measures. Our proposed system addresses this exigency by envisioning the development of a sophisticated Android application tailored for communication, with a specific focus on the implementation of efficient and fine-grained forward secure asynchronous messaging. Departing from conventional

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 11, November 2023 ||

| DOI:10.15680/IJIRSET.2023.1211028 |

messaging platforms, our application integrates state-of-the-art techniques to facilitate seamless communication while placing a paramount emphasis on user privacy and the security of transmitted data.

The central tenet of our proposed system revolves around the meticulous implementation of efficient and fine-grained forward secure asynchronous messaging. The incorporation of forward security ensures the confidentiality of past communications even in the event of future compromise of encryption keys, providing users with an elevated level of security for their sensitive data. The application's design will also accommodate asynchronous messaging, allowing users to engage in message exchanges without the constraints of real-time communication. This feature is particularly salient for users situated in disparate time zones or those facing intermittent internet connectivity. The amalgamation of these features positions our Android application as a distinctive and highly secure messaging platform, offering users the capability to communicate securely and privately without compromising the integrity of their data.

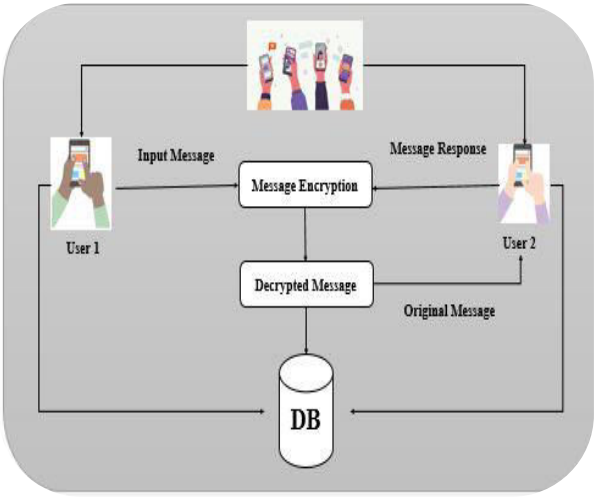

Fig 1. Proposed System Architecture

Moreover, the proposed system places a strong emphasis on user-centric design, incorporating user-friendly interfaces and intuitive design elements. This strategic approach ensures accessibility for a diverse user base, irrespective of their technical proficiency. By prioritizing an optimal user experience, the application seeks to strike a balance between security and usability, setting a new standard for secure communication in the domain of messaging applications.

The Android application for forward secure asynchronous messaging is designed to provide users with a highly secure and efficient communication platform. The system requirements for this application include robust encryption protocols to ensure end-to-end security for messages exchanged between users. The app must support fine-grained forward secrecy, meaning that even if a user's private key is compromised, past messages should remain secure. Additionally, the application should offer asynchronous messaging capabilities, allowing users to send and receive messages at their convenience without the need for real-time communication. To achieve this, the app must implement reliable message queuing and delivery mechanisms, ensuring that messages are stored securely until they are successfully delivered to the intended recipient. Furthermore, the application should have an intuitive user interface, enabling users to easily navigate through the features and functions while maintaining a seamless and responsive user experience. Compliance with Android's latest security standards and guidelines, as well as compatibility with a wide range of Android devices and versions, is also essential to ensure a smooth user experience across different platforms.

IV. WORKING MODULE

The working module of the asynchronous message forwarding system in our Android application unfolds through a meticulously crafted methodology. Initially, the user engages with the system through a secure authentication and registration process, either creating an account or logging in with existing credentials. This step ensures that only authorized users gain access to the messaging application. During authentication, the system not only securely stores user information but also generates unique encryption keys, including a public key for encryption and a private key for

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 11, November 2023 ||

| DOI:10.15680/IJIRSET.2023.1211028 |

decryption. This foundational step lays the groundwork for robust user identification and establishes the security framework for subsequent communication.

Upon successful authentication, the focus shifts to message encryption and decryption. When a user initiates a message, the application employs formidable encryption algorithms to safeguard the content during transmission. Each user possesses a unique public key used for encryption and a corresponding private key for decryption. The decryption process, crucial for end-to-end security and privacy, is exclusively executed by the intended recipient employing their private key. This cryptographic approach ensures that messages remain confidential throughout the communication process.

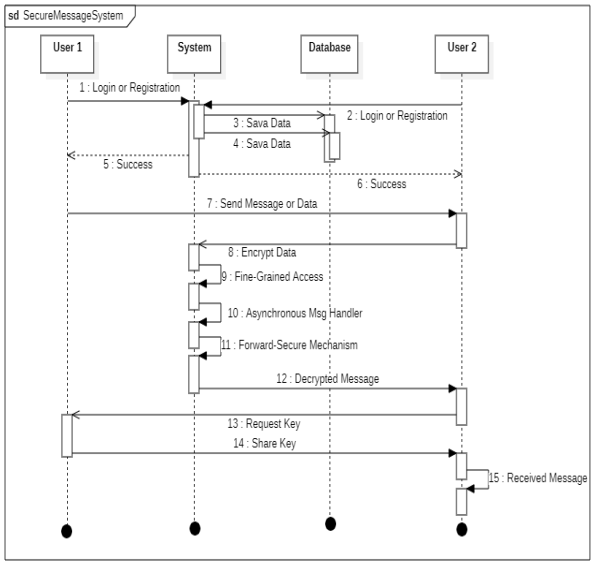

Fig 2: Working Flow Diagram

The implementation of forward secrecy represents a pivotal aspect of our system's security architecture. To achieve this, temporary session keys are generated for each conversation, serving as the basis for encrypting messages exchanged during that specific session. This approach fortifies the system against potential future compromises of long-term encryption keys, enhancing the overall resilience of the messaging platform. Simultaneously, the system embraces asynchronous messaging, securely storing messages on the server until the intended recipient is online. This ensures that users can conveniently access their messages without fear of data loss, accommodating various user schedules and connectivity patterns.

Furthermore, the system introduces fine-grained message control features, empowering users with unprecedented control over their communication. Users can define message expiration times, restrict forwarding, and even revoke access to specific messages. The introduction of self-destructing messages adds an additional layer of privacy, as messages automatically vanish after predefined lifetimes. Additionally, users can limit message forwarding to prevent unauthorized sharing of sensitive information, thereby solidifying the application's commitment to user privacy and confidentiality. Through this comprehensive working module, our Android application stands as a beacon of secure and flexible asynchronous messaging.

Methodology

- **User Authentication and Registration:**
  The system begins with user authentication and registration, where users create accounts or log in using their credentials. User authentication ensures that only authorized users can access the messaging application. During this process, the system securely stores user information and generates unique encryption keys for each user.
- **Message Encryption and Decryption:**
  When a user sends a message, the application encrypts the message using strong encryption algorithms before transmission. Each user has a unique public key for encryption and a private key for decryption. Messages are decrypted only by the intended recipient using their private key, ensuring end-to-end security and privacy.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 11, November 2023 ||

| DOI:10.15680/IJIRSET.2023.1211028 |

- **Forward Secrecy Implementation:**
  The application implements forward secrecy by generating temporary session keys for each conversation. These session keys are used to encrypt messages exchanged during a specific session.
- **Asynchronous Messaging:**
  Messages are stored securely on the server until the recipient is online, ensuring that users can access their messages at their convenience without any loss of data.
- **Fine-Grained Message Control:**
  The system provides fine-grained control over messages, allowing users to set message expiration times, restrict forwarding, and revoke access to specific messages. Users can define message lifetimes, after which the messages automatically self-destruct, enhancing privacy and confidentiality. Additionally, users can limit message forwarding to prevent unauthorized sharing of sensitive information.

V. CONCLUSION

In conclusion, the Android application for forward secure asynchronous messaging stands as a remarkable milestone in the realm of digital communication. By prioritizing efficiency, fine-grained control, and robust security measures, this app has not only transformed how we interact online but has also set new standards for privacy and data protection. Its innovative approach to secure messaging ensures that users can communicate freely, knowing that their conversations are shielded from prying eyes and potential threats. As we embrace an era where digital communication is integral to our personal and professional lives, this application emerges as a beacon of trust, empowering users to exchange information with confidence and peace of mind. With its user-friendly interface, cutting-edge encryption techniques, and commitment to user privacy, the forward secure asynchronous messaging app has redefined the landscape of secure messaging platforms, paving the way for a safer and more secure digital future.

REFERENCES

1. M. Marlinspike. (2016). Signal Protocol Documentation. Accessed: Oct. 23, 2018. [Online]. Available: https://signal.org/docs
2. J. Callas, L. Donnerhacke, H. Finney, D. Shaw, and R. Thayer, OpenPGP Message Format, document RFC 4880, Nov. 2007. [Online]. Available: https://tools.ietf.org/html/rfc4880
3. Apple Computer. (Sep. 2018). iOS Security. Accessed: Oct. 23, 2018. [Online]. Available: https://www.apple.com/business/site/docs/iOS _Security_Guide.pdf
4. B. Ramsdell and S. Turner, Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification, document RFC 5751, Jan. 2010. [Online]. Available: https://tools.ietf.org/html/rfc575
5. T. Perrin and M. Marlinspike. (Nov. 2016). The Double Ratchet Algorithm. Accessed: Oct. 23, 2018. [Online]. Available: https://signal. org/docs/specifications/doubleratchet/
6. Off-the-Record Messaging. (Mar. 2016). Accessed: Oct. 23, 2018. [Online]. Available: https://otr.cypherpunks.ca/
7. M. Marlinspike. (Aug. 2013). Forward Secrecy for Asynchronous Messages. Accessed: Nov. 9, 2018. [Online]. Available: https://signal. org/blog/asynchronous-security/
8. D. Derler, S. Krenn, T. Lorünser, S. Ramacher, D. Slamanig, and C. Striecks, "Revisiting proxy re-encryption: Forward secrecy, improved security, and applications," in Proc. IACR Int. Workshop Public Key Cryptogr. (PKC), 2018, pp. 219–250.
9. Cohen, J. Holmgren, R. Nishimaki, V. Vaikuntanathan, and D. Wichs, "Watermarking cryptographic capabilities," SIAM J. Comput., vol. 47, no. 6, pp. 2157–2202, Jan. 2018.
10. R. Canetti, S. Raghuraman, S. Richelson, and V. Vaikuntanathan, "Chosen-ciphertext secure fully homomorphic encryption," in Proc. IACR Int. Workshop Public Key Cryptogr. (PKC), 2017, pp. 213–240. [
11. F. Günther, B. Hale, T. Jager, and S. Lauer, "0-RTT key exchange with full forward secrecy," in Advances in Cryptology—EUROCRYPT 2017. Berlin, Germany: Springer, 2017, pp. 519–548.
12. D. Derler, T. Jager, D. Slamanig, and C. Striecks, "Bloom filter encryption and applications to efficient forward-secret 0-RTT key exchange," in Advances in Cryptology—EUROCRYPT 2018. Berlin, Germany: Springer, 2018, pp. 425–455.
13. R. Bost, B. Minaud, and O. Ohrimenko, "Forward and backward private searchable encryption from constrained cryptographic primitives," in Proc. ACM SIGSAC Conf. Comput. Commun. Secur., Oct. 2017, pp. 1465–1482.
14. N. Aviram, K. Gellert, and T. Jager, "Session resumption protocols and efficient forward security for TLS 1.3 0-RTT," in Advances in Cryptology—EUROCRYPT 2019. Berlin, Germany: Springer, 2019, pp. 117–150.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.423

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details