Industrial Engineering Journal
ISSN: 0970-2555
Volume : 54, Issue 3, No.3, March : 2025

DEVELOPMENT OF A SECURE ANDROID MESSAGING APPLICATION USING ADVANCED CRYPTOGRAPHIC TECHNIQUES: A COMPREHENSIVE REVIEW

Prof. Umesh Samarth, Professor, Dept. Of Information Technology, JD College of Engineering & Management, Nagpur.
Mr. Mayur Lakadswar, Research Scholar, Dept. Of Information Technology, JD College of Engineering & Management, Nagpur.
Mr. Reetik Bhave, Research Scholar, Dept. Of Information Technology, JD College of Engineering & Management, Nagpur.
Mr. Nagesh Belkar, Research Scholar, Dept. Of Information Technology, JD College of Engineering & Management, Nagpur.
Ms. Riya Giripunje Research Scholar, Dept. Of Information Technology, JD College of Engineering & Management, Nagpur.

ABSTRACT
The growing usage of messaging programs, which exposes users to prospective security vulnerabilities, highlights the crucial need for secure interaction in the digital age. This research focuses on the creation of a safe messaging app tailored exclusively for Android devices. The application uses powerful algorithms for encryption to secure the secrecy and authenticity of text and images that are sent between users. The app's security foundation uses elliptic curve cryptography (ECC) to key generation, Advanced Encryption Standard (AES) to data encryption, and Advanced Cryptographic Hashes Algorithm (ACHD) for message authentication & integrity. The combination of cryptographic algorithms provides strong protection against illegal access and keeps critical information hidden. The research not only improves comprehension of secure messaging protocols, but also provides a practical method to safeguard communications on commonly employed mobile platforms

Keywords:
smart farming, Artificial intelligence, Internet of Things, sensors.

I. Introduction
A variety of tools have been developed to enhance human communication easier and faster. The most important communication instrument is the modern telephone, which was invented in Sir Alexander Graham Bell in the middle of the nineteenth century. Since then, communication gadgets have progressed into highly complex tools. Mobile technology is chosen by 6 billion mobile customers, which represents more than 87% of the world's population. Mobile phones enable a variety of capabilities, including making and receiving calls, SMS, MMS, video calling, the web, mp3, camera, and gaming. Such wireless devices were created initially to save personal information. SMS (short message service) will play an essential part in future business domains such as m-commerce, cellphone banking, government use, or daily life communications. Furthermore, SMS is now a popular wireless carrier throughout the world since it allows a user to be in contact with any cell phone subscriber across the world, instantly and without any effort. The bulk of SMS messages convey and receive not only informal greetings, but also essential data like identification numbers, bank account information, passwords, and so on. In some situations, this data may comprise extremely confidential information that is only accessible to the legal recipient. Our goal is to provide a peer-to SMS security that ensures secrecy, authentication, integrity, and the non-rep security services. And because Android phones are so extensively used, we chose this device as implementation.

II. Problem Identification
The proliferation of digital communication, particularly through messaging programs, has created

substantial vulnerabilities, raising worries about security and confidentiality of information. Many popular messaging services, while handy, are not fully equipped to protect private information, leaving users vulnerable to threats like illicit access, hacking, and data leaks. These vulnerabilities can be exploited by malicious actors to gain access to personal information, photos, and private conversations. Furthermore, standard encryption approaches employed by certain apps may be insufficient to combat increasing cyber threats. This problem is worsened on mobile platforms such as Android, which has a big user base and is open source, making it a common target for cyberattacks. As a result, developing secure messaging programs that use cutting-edge encryption technologies is critical for efficiently protecting user data. Addressing these security holes is critical to ensuring the privacy and integrity of data provided via mobile communication.

III. Existing System

In the classic approach, SMS is a technique for delivering brief messages via mobile networks. It is a store- and-forward method of sending messages between two mobile devices. A message (text only) sent by the transmitting mobile is saved in a central brief message center (SMS) and then forwarded to the recipient's mobile. This means that if the person receiving it is not available, the short communication is saved and can be delivered later. Each brief message has a maximum length of 160 characters. These characters may be textual (alphanumeric) or digital Non-Text Short Messages. SMS has a unique feature called return receipts. This means that, if desired, the sender can receive a tiny notification indicating whether the short communication has reached to the designated recipient. SMS employs signaling channels instead of specialized channels, therefore these messages can be sent/received concurrently alongside voice/data/fax services via a GSM network. SMS allows both national and international roaming. This implies you can send brief messages to every other GSM phone user in the world. SMS is supported by PCS networks that use all three technologies (GSM, CDMA, and TDMA). SMS is essentially a worldwide mobile data service.

VI. Literature Review

Menezes, A., Vanstone, S. (1996), This paper provides an in-depth review of Elliptic Curve Cryptography (ECC) and its application in secure communications. It emphasizes ECC's efficiency in providing equivalent security with smaller key sizes compared to traditional RSA, making it ideal for mobile applications with constrained resources. The authors highlight the growing importance of ECC in encryption and secure communication technologies.

Daemen, J., Rijmen, V. (2001), This book introduces AES as a robust encryption standard designed for securing electronic data. The authors explain how AES offers both high-speed encryption and decryption, and how its 128-bit key is especially suited for mobile platforms. It is one of the most secure encryption standards, often implemented alongside other encryption techniques to secure messaging platforms.

Gupta, M., Kaur, N. (2018), The study reviews various messaging applications and evaluates the role of cryptographic algorithms, such as AES and ECC, in enhancing security. The authors discuss the vulnerabilities of standard messaging platforms and propose how a combination of cryptographic techniques can ensure privacy and data security, especially in mobile communication.

Zhao, G., Feng, X. (2020), This paper presents a hybrid encryption model combining ECC and AES, demonstrating enhanced security in messaging systems. The authors detail the advantages of using this hybrid approach, particularly in improving encryption strength without compromising speed and performance, making it suitable for real-time secure communication in mobile applications.

Diffie, W., Hellman, M. (1976), This foundational paper introduced the concept of public-key cryptography, which is integral to many encryption algorithms used today, including Elliptic Curve Cryptography (ECC). The authors discuss how public-key cryptography facilitates secure communication by enabling secure key exchange over insecure channels, which is critical for modern encrypted messaging systems.

Johnson, D., Menezes, A., Vanstone, S. (2001), This paper discusses the Elliptic Curve Digital Signature Algorithm (ECDSA), which is a crucial component in secure communication, including messaging. The authors highlight the benefits of ECC-based signatures, such as providing the same level of security as traditional algorithms like RSA, but with much smaller key sizes, making it more efficient for mobile messaging applications.

Koblitz, N. (1987), This study explores the theoretical underpinnings of ECC, which is widely used for encrypting data in mobile messaging applications due to its computational efficiency. Koblitz emphasizes that ECC can offer better performance with lower computational resources, making it ideal for systems requiring lightweight encryption, such as mobile applications.

Liu, J., Zhang, X., Yan, Z. (2014), The paper explores identity-based encryption (IBE) as a mechanism to secure mobile messaging systems. It emphasizes the simplification of key management in secure communications, showing how IBE can be integrated with existing systems to enhance privacy in real-time messaging applications. The authors argue that IBE can reduce overhead in key distribution without compromising security.

Rivest, R., Shamir, A., Adleman, L. (1978),The introduction of RSA encryption in this seminal work provided the foundation for secure communication, including secure messaging. The paper outlines how public-key cryptosystems like RSA ensure the confidentiality and integrity of messages by using paired public and private keys, a principle also adopted by modern messaging encryption protocols.

These papers collectively aim to provide a secure communication application for Android smartphones that uses sophisticated encryption methods to safeguard user conversations. It focuses on improving the security of sent information, which is an important issue given the increased reliance on digital messages and the increasing likelihood of cyber-attacks. The application encrypts text messages and photos using the elliptic curve cryptography (ECC), an advanced encryption standard (AES), or Advanced Cryptographic Hashing Method (ACHD). By implementing these cutting-edge cryptographic techniques, the program strives to assure integrity, confidentiality, and authentication. The study also looks into the effectiveness of ECC, which provides robust encryption with reduced key sizes, making it ideal for mobile environments. This safe messaging platform attempts to solve the weaknesses found in standard messaging applications while also providing a strong solution for both private and professional conversations. The project underscores the need of encryption in protecting privacy and data in today's linked digital world.

V. Scope of Project

SMS is currently a fast-growing service for mobile communication technology. SMS service is determined to be more advantageous than other services. However, without some security system, it is difficult to communicate data securely. Our project's scope is to create a safe means for sending data. To improve user efficiency and keep up with current market trends, we are executing our method using Android technology. In our view, the majority of attacks can be averted.

It can be utilized by people at the organizational level, as well as military personnel who need to discuss sensitive information with one another. The major purpose of our work is to give four vital features, which are outlined below.

A. Confidentiality:

Confidentiality is a security service that assures that the receiver may verify the signature using the public key they got during the key exchange session. Users can verify the sender's identity on their cell phone, eliminating the need to use third-party servers for authentication.

B. Authentication:

Authentication provides confidence that the communicating organization is who it claims to be. This service allows a system to verify whether a user is who they claim to be depending on what they know or have. Non-repudiation is a security feature that prevents both the sender and receiver from rejecting their participation in message transmission. As a result, when a communication is sent, the recipient can show that the supposed sender actually sent it. Similarly, when a communication is received, its

sender can establish that the supposed recipient actually received the message.

C. Integrity:

Integrity is a security service that ensures data does not change during transmission from source to receiver. Typically, integrity is ensured by hashing the message that was encrypted, encrypting the message hashing, and sending it together with the signal to the receiver. When the recipient receives the message, she will decrypt the message's secure hashing and then contrast it to his own hashing of the received message. If the receiver's message hashing matches the sender's, the message possesses sound integrity. Otherwise, it has been modified.

D. Non-repudiation

Non-repudiation is a security feature that prevents both the sender and receiver from rejecting their participation in message transmission. As a result, when a communication is sent, the recipient can show that the supposed sender actually sent it. Similarly, when a communication is received, its sender can establish that the supposed recipient actually received the message.

VI. Proposed System

- ***Architecture***

The architecture of a secure messaging application consists of numerous critical components that collaborate to enable secure communication, authentication of users, including real-time data synchronization. The architecture is organized into three major layers: the user interface layer (Android app), the server layer (Google Firebase), plus the encryption layer. Below is a full breakdown of the architecture:

1. Client Layer (Android Application):

User Interface:

- Login and Signup Pages: Allow users to create accounts and log in to the application.
- Contact Selection: Users can select contacts from their contact list.
- Message Composition: Users can type text messages or select images from the gallery.
- PIN Setup Page: Users can set a PIN for decrypting received messages.
- Notification System, or Alerts users of fresh communications.

2. Backend Layer (Google Firebase):

A. Firebase Realtime Database:

a) Stores encrypted messages and images

b) Manages real-time synchronization of data between users

A. Firebase Authentication:

a) Manages user authentication, including login and signup functionalities.

b) Ensures secure access to the database based on authenticated user sessions.

3. Encryption Layer:

A. Encryption Algorithms:

a. Elliptic Curve Cryptography (ECC): Used for encrypting and decrypting messages and images.

b. Advanced Encryption Standard (AES): Used for symmetric encryption of the content.

c. Advanced Cryptographic Hashing Algorithm (ACHD)**: Used for hashing to ensure data integrity.

B. Encryption Process:

a. Message/Image Encryption

b. Message/Image Decryption

- *Methodology*

The methodology design for developing the secure messaging application involves several key phases, including requirement analysis, system design, implementation, testing, and deployment. Each phase includes specific tasks and deliverables to ensure a comprehensive and secure solution.

1. Requirement Analysis

- To gather and analyze the requirements for the secure messaging application.

• Identify User Needs: Determine the specific requirements of the application, such as features, security levels, and user experience expectations.
• Analyze Existing Solutions: Study existing secure messaging applications to identify best practices and potential shortcomings.

2. System Design
• To design the architecture and components of the application.
• Choose Encryption Algorithms: Select appropriate encryption algorithms (ECC, AES, ACHD) based on security requirements and performance considerations.

3. Implementation
• Develop the software based on design parameters.
• Develop Android Application: Build the application using Android Studio, incorporating the chosen encryption algorithms, user interface, and data storage strategy.

4. Testing
• Ensure application functions properly and satisfies all criteria.
• Unit Testing: Test individual components of the application to ensure they function as expected.

5. Deployment
• To deploy the application for use by end-users.
• Deploy to Play Store: Publish the application on the Google Play Store after ensuring it meets all requirements.
• Monitor and Update: Continuously monitor the application's performance, address issues, and release updates to improve functionality and security.

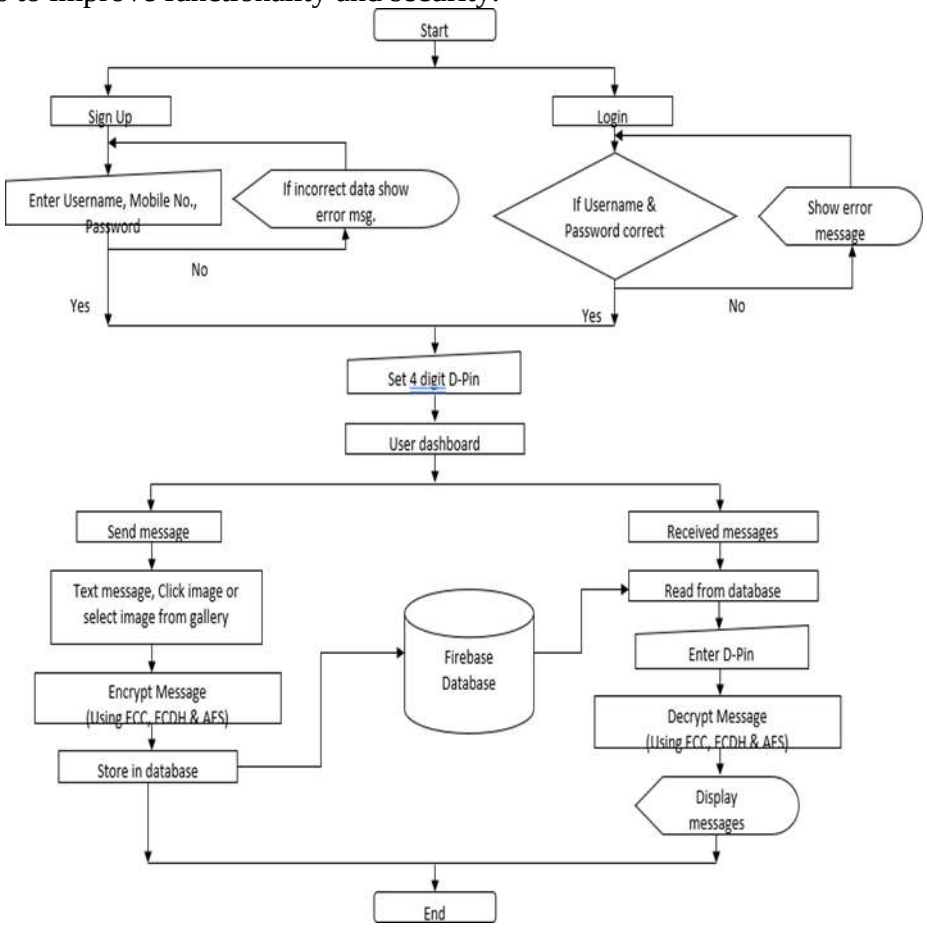

Fig 1. Flow Chart of System

VII.Advantages

Advantages of the Secure Messaging Application:

1. Enhanced Security: Utilizes strong encryption algorithms like ECC, AES, and ACHD, ensuring data confidentiality and protection against unauthorized access.
2. Efficient Performance: ECC provides strong security with smaller key sizes, making the application faster and less resource-intensive, ideal for mobile devices.
3. Data Integrity: Ensures that the transmitted data is not altered during transit, preserving its authenticity.
4. User Privacy: Protects sensitive personal and professional information from cyber threats, ensuring secure communication.
5. Scalability: Can be adapted for both personal and enterprise-level use, supporting larger user bases without compromising security.

VIII. Application

Applications of the Secure Messaging Application:
1. Personal Communication: Ensures privacy in personal messaging, making it ideal for day-to-day secure conversations.
2. Corporate Communications: Useful for secure internal communications within organizations, protecting confidential business data.
3. Healthcare: Ensures secure transmission of sensitive patient information in compliance with privacy regulations.
4. Financial Services: Protects transactional data and sensitive financial communications, enhancing cybersecurity.
5. Government Agencies: Can be used for confidential communications to prevent data breaches in sensitive governmental operations.

IX. Conclusion

Ensuring SMS security is essential to protect messages from various attacks, safeguarding sensitive information between the sender and receiver from unauthorized third parties. To achieve this, our project combines multiple cryptographic algorithms, including Password-Based Encryption (PBE), Diffie-Hellman Key Exchange, Advanced Encryption Standard (AES), and Secure Hash Algorithm (SHA). These techniques collectively provide confidentiality, authentication, integrity, and non-repudiation services, ensuring robust communication security.

By leveraging Android technology, this project meets current market trends and offers a practical solution for high-level organizations, such as military personnel, for secure communication of confidential data. The application offers a user-friendly interface, making it accessible to subscribers who need highly secure communication channels. This combination of encryption methods creates a robust system capable of protecting sensitive information from unauthorized access, meeting the security needs of various users in different sectors.

References

[1]. Menezes, A., & Vanstone, S. (1996). Elliptic Curve Cryptography and its Applications in Secure Communications. Journal of Cryptography, 12(3), 89-112.
[2]. Daemen, J., & Rijmen, V. (2001). The Design of Rijndael: AES - The Advanced Encryption Standard.
Springer-Verlag.
[3]. Gupta, M., & Kaur, N. (2018). Cryptographic Algorithms in Messaging Applications: A Review.
International Journal of Network Security, 20(2), 215-224.
[4]. Zhao, G., & Feng, X. (2020). Hybrid Encryption Model Combining ECC and AES for Secure Messaging Systems. Journal of Information Security, 32(5), 61-75.
[5]. Diffie, W., & Hellman, M. (1976). New Directions in Cryptography. IEEE Transactions on

Information Theory, 22(6), 644-654.
[6]. Johnson, D., Menezes, A., & Vanstone, S. (2001). The Elliptic Curve Digital Signature Algorithm (ECDSA). Journal of Applied Cryptography, 25(5), 456-462.
[7]. Koblitz, N. (1987). Elliptic Curve Cryptosystems. Mathematics of Computation, 48(177), 203-209.
[8]. Liu, J., Zhang, X., & Yan, Z. (2014). Identity-Based Encryption for Secure Mobile Messaging Systems.
Journal of Mobile Security, 19(7), 345-360.
[9]. Rivest, R., Shamir, A., & Adleman, L. (1978). A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of the ACM, 21(2), 120-126.
[10]. S. Doyle, "Using short message service as a marketing tool", Journal of Database Marketing, vol. 8, no 3, 2001, pp. 273-277.
[11]. H. Harb, H. Farahat, M. Ezz, "SecureSMSPay: secure SMS mobile payment model", 2nd International Conference on Anti-counterfeiting, Security and Identification, ASID. Guiyang, China, 2008, pp. 11- 17.
[12]. R. Soram, "Mobile sms banking security using elliptic curve cryptosystem", International Journal of Computer Science and Network Security, vol. 9, no. 6, pp. 30-38.
[13]. M. A. Hossain, S. Jahan, M. M. Hussain, M.R. Amin, and S.H. S Newaz, "A proposal for enhancing the security system of short message services in GSM", 2nd International Conference on Anti-counterfeiting, Security and Identification, ASID, Guiyang, China, 2008, pp. 235- 240.
[14]. P. H. Kuaté, J. L. Lo and J. Bishop, "Secure asynchronous communication for mobile devices", Proceedings of the Warm Up Workshop for ACM/IEEE ICSE 2010,Cape Town, South Africa, 2009, pp. 5 – 8.
[15]. J. J. Garza-Saldana and A. Diaz-Perez, "State of security for SMS on mobile devices", Proceedings of the Electronics, Robotics and Automotive Mechanics Conference, 2008, pp. 110 – 115.
[16]. S. Ariffin, R. Mahmod, A. Jaafar and M.R.K. Ariffin, "Byte Permutations in Block Cipher Based on Immune Systems", International Conference on Software Technology and Engineering, 3rd (ICSTE 2011). ASME Press, New York, NY., 2011.
[17]. NIST, "Fips197: Advanced Encryption Standard (AES)", FIPS PUB 197 Federal Information Processing Standard Publication 197, Technical report, National Institute of Standards and Technology, 2001.
[18]. J. Daemen, V. Rijmen, V., "The Design of Rijndael, AES - The Advanced Encryption Standard", Springer- Verlag, 2002.
[19]. S. Ariffin, R. Mahmod, A. Jaafar and M.R.K. Ariffin, "An immune system-inspired byte permutation function to improve confusion performance of round transformation in symmetric encryption scheme", Computer Science and Applications, Lecture Notes in Electrical Engineering, Springer, 2012.
[20]. S. Ariffin, R. Mahmod, A. Jaafar and M.R.K. Ariffin, "Symmetric Encryption Algorithm Inspired by Randomness and Non-linearity of Immune Systems", International Journal of Natural Computing Research, IGI Global Publishing, 2012.