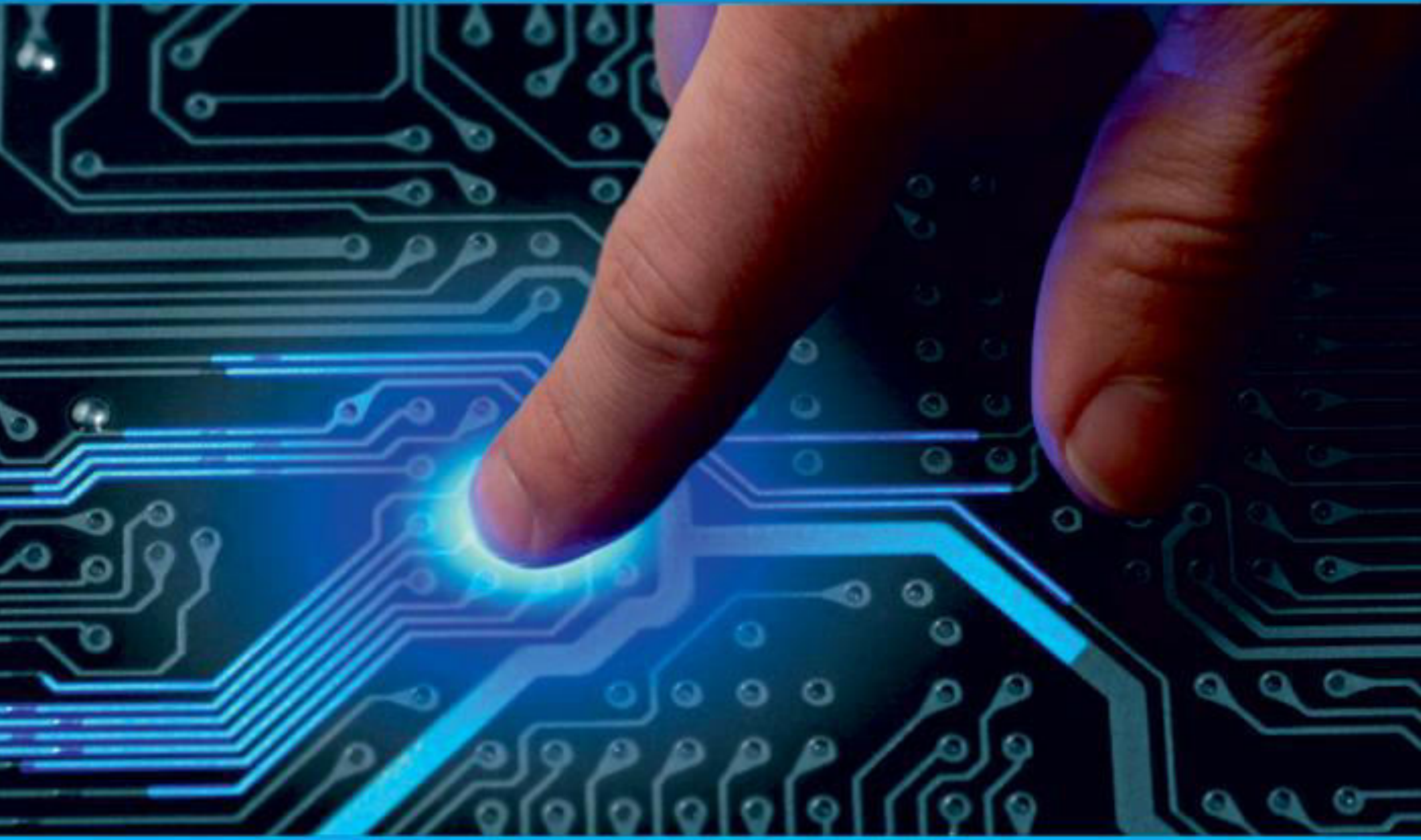
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 4, April 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

9940 572 462 6381 907 438 ijircce@gmail.com www.ijircce.com

| DOI: 10.15680/IJIRCCE.2024.1204014 |

Android Based Encrypted SMS System

Dr.R.Nagarajan[1], Bavanya M[2]

[1]Assistant Professor, PG & Research Department of Computer Science, Sri Ramakrishna College of Arts & Science, Coimbatore, India

[2]UG Student, PG & Research Department of Computer Science, Sri Ramakrishna College of Arts & Science, Coimbatore, India

ABSTRACT: The rapid development of telecommunications technology has brought enormous benefits. Thanks to this technology, geographical distance and time are no longer a significant obstacle. One important result of this success is the Short Message Service (SMS). Android SMS, a built-in feature that allows users to receive and send messages on their mobile devices.In this project, we are developing a mobile application whose purpose is to encrypt text messages and ensure the confidentiality of message content. The SMS system encrypts the messages into encrypted text using the key provided by the sender before sending them to the number of the intended addressee. In contrast, the system receiving the text message decrypts these encrypted text messages, ensuring that only the recipient has access to the original content. Our system uses standardized communication protocols that facilitate the exchange of short text messages between mobile devices. To ensure data confidentiality, we use converged encryption, which encrypts and decrypts data with a converged key derived from the cryptographic hash value of the contents of the data copy. After generating the key and encrypting the data, users store the keys and send the encryption to the recipient. A message proxy or unauthorized person or third party cannot read fully encrypted messages because they do not have the necessary key. We implement this model with a modified Blowfish cipher and ensure code integrity with the MD5 hashing algorithm..

KEYWORDS: Telecom Secure SMS, message encryption,MD5 hashing algorithm

I.INTRODUCTION

In the midst of the continuous development of telecommunication technology, the mobile communication is witnessing the profound impact of innovation. Short message service (SMS), a ubiquitous aspect of modern communication, transcends time and space barriers, but raises privacy and security concerns. In response, we present Secures, an innovative mobile application designed to enhance the confidentiality of text messages through advanced encryption techniques. Using the native text messaging service on Android devices, Secure SMS allows users to convert plain text messages into encrypted text, hiding. the content for unauthorized access. celebrate By integrating modern encryption methods and cryptographic protocols, Secure SMS provides complete protection and creates confidence in the privacy of sensitive communications. Secure SMS uses a complex encryption framework at its core, anchored by a modified Blowfish algorithm that is highly rated. effectiveness and reliability of data protection. Using encryption keys derived from approximation of message content, SecureSMS creates a strong barrier against unauthorized access and strengthens the integrity of the data exchanged. In addition, SecureSMS adheres to end-to-end encryption principles and issues decryption keys as intended. . only to the sender. recipient, which prevents eavesdropping or eavesdropping attempts by malicious parties. Using standardized communication protocols and cryptographic methods, SecureSMS overcomes the limitations of traditional SMS services and ushers in a new era of secure mobile communication. In addition to encryption capabilities, SecureSMS offers a smooth user experience with an intuitive user interface that makes encryption and decryption easy. of messages. decryption Users can create unique encryption keys that provide a custom level of data security. In addition, SecureSMS includes robust error handling mechanisms to ensure reliable delivery of encrypted messages under various network conditions.

II. RELATED WORK

A Study of Collection Methods and Cross Collections Comparison of Android Unlock Patterns" is a research project conducted by Aviv, A.J. and Dürmuth, M., published in arXiv preprint November 2018 (arXiv:1811.10548). This project analyzes different methods for collecting data on Android unlock patterns and compares them across different datasets. It assesses the impact on security and privacy, taking into account factors such as ease of collection, pattern strength and potential vulnerabilities. Ultimately, the study aims to improve our understanding of the security of Android unlock patterns and guide the development of more effective authentication methods..

Analyzing the Impact of Collection Methods and Demographics for Android's Pattern Unlock was presented at the Workshop on Usable Security (USEC) in 2016. It is a research project conducted by Aviv, A.J., and Dürmuth, M. This study analyzes various methods for collecting data on Android unlock patterns and compares them across different datasets. It assesses their impact on security and privacy, considering factors such as ease of collection, pattern strength, and potential vulnerabilities. Ultimately, the study aims to enhance our understanding of the security of Android unlock patterns and inform the development of more effective authentication methods.

Chaitanya, G.K. and Raja Sekhar, K.,Verification of Pattern Unlock and Gait Behavioral Authentication through a Machine Learning Approach" published in the International Journal of Intelligent Unmanned Systems in 2021, likely delves into using machine learning to authenticate users via pattern unlock and gait behavior. It explores the efficacy of machine learning in accurately identifying users based on unique patterns and traits. This study could advance biometric authentication methods for enhanced security in unmanned systems and other applications. Under the Table Tap Authentication for Smartphones" explores tap authentication as a new method for smartphone security. Authored by Marques, D., Guerreiro, T., Duarte, L., and Carriço, L., the study investigates using tapping gestures for user authentication, using smartphone sensors. It aims to evaluate the effectiveness, usability, and security of tap authentication compared to traditional methods like PINs or passwords. This research contributes to improving smartphone security and user authentication.

III.PROPOSED METHODOLOGY

Our approach to building an encrypted SMS system for Android is all about putting users first. We start by really understanding what people need and making sure our system meets the highest security standards. Our interface is designed to be super easy to use, and we use really strong encryption methods to keep messages safe and private. Security is a big deal for us, so we make sure that only the right people can access messages by managing encryption keys carefully and verifying user identities. We're also super serious about following all the rules and regulations to protect user data and privacy. Before we let anyone use our system, we test everything thoroughly to make sure it's working perfectly. And if anyone needs help or guidance along the way, we're here to support them every step of the way. Plus, we believe in keeping things transparent and empowering users with knowledge about why encrypted communication matters. We're always listening to feedback and looking for ways to make our system even better to meet the needs of our users in today's digital world

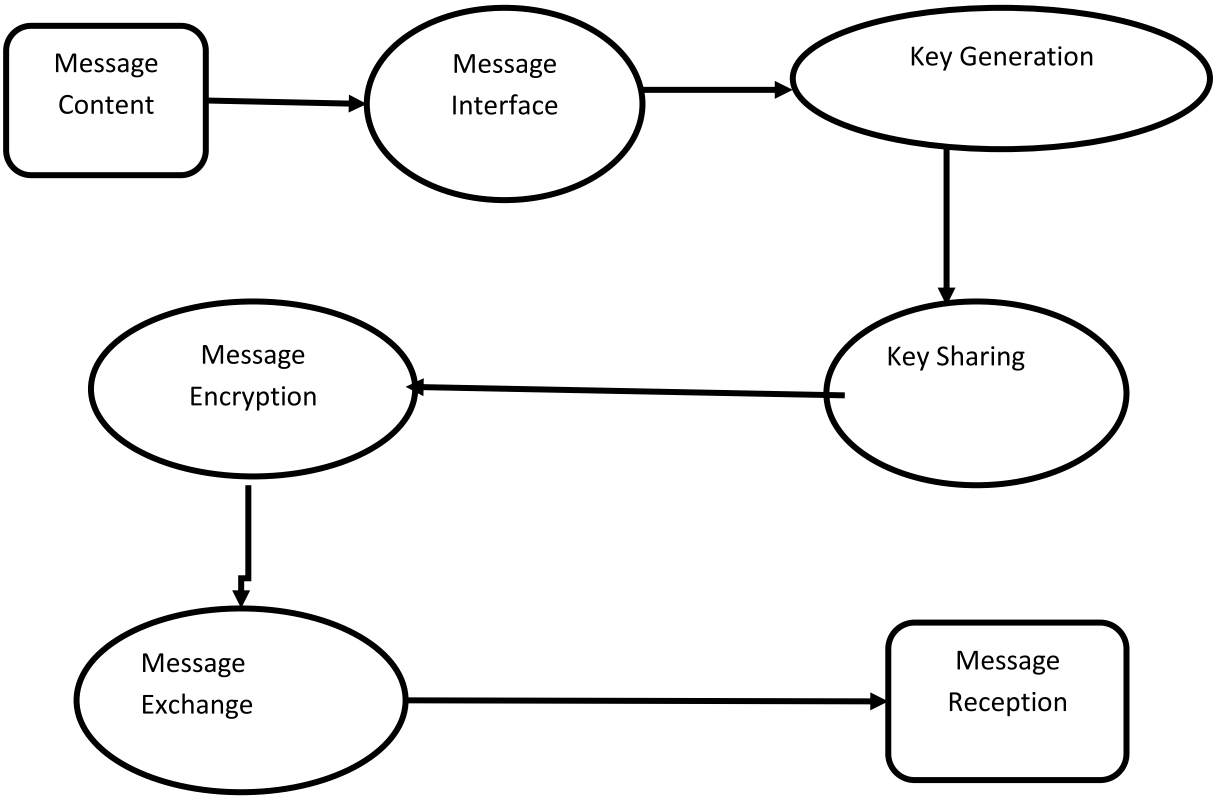


Fig-1 System Architecture

Configure SMS Gateway

Deploying mobile apps to end users can be complex due to manufacturers requiring distribution through specific digital platforms (e.g., iOS's App Store). Approval processes for inclusion in these platforms are time-consuming, and additional data updates often require separate approval. These restrictions complicate distribution and management. Many individuals lack the expertise to navigate these challenges, despite attempts to simplify app development for a wider audience.

KEY GENERATION

The system is engineered to establish both dedicated and shared keys between senders and receivers. Uploaded file content undergoes encryption using the shared public key, which receivers decrypt using their private key. An elliptic curve key generation algorithm is employed to create the shared key between users. This shared key is utilized for encrypting and decrypting the file content. Input parameters such as device ID, session information, and plaintext data of the video content are utilized to generate dedicated and shared keys, facilitating encrypted video content transmission between devices.

SMS ENCRYPTION AND TRANSMISSION

Content based encryption is applied to encrypt the text data. The contents are subdivided into number of encodes for the Encode processing model. Encode based encryption with the handling of macro blocks of text data is applied by differentiating the encode type content. The system sub divides the macro block structure and to provide the ease of encryption modeling of text data. Text content in terms of content and encode content of text data are taken as input and the Encrypted text content with successful decryption are obtained as output and signature generated for validating the decryption of data.

RECEIVE SMS AND DECRYPTION

The innovation improves scrolling on electronic displays, allowing users to navigate data effortlessly. It introduces a touch-responsive mechanism translating finger movements into scrolling actions, with speed and direction determining movement. Users can control scrolling by adjusting gestures. Implemented via microprocessor programming, it provides a natural scrolling experience. Mobile devices featuring this innovation have a user-friendly interface with multiple desktop screens, some password protected, and use touch-sensitive displays. This description guides practitioners in implementing the invention effectively within the defined scope.

IV. RESULTS AND DISCUSSIONS

The development of an Android-based encrypted SMS system meets the urgent need for secure communication in today's digital environment. Using encryption techniques, such a system can protect sensitive information exchanged via text messages from unauthorized access and interception. The system includes strong encryption protocols to ensure message confidentiality and integrity, while an intuitive and user-friendly interface seamlessly integrated with the default messaging app on Android devices improves user experience and facilitates widespread adoption. Secure mechanisms are created, shared and stored in keys to prevent unauthorized access to encryption keys, thus improving the overall security of the system. Ensuring compatibility with many Android devices and versions and compatibility with existing SMS infrastructure enables seamless communication between different devices and networks. System optimization for efficient performance minimizes latency and resource consumption while maintaining strong encryption standards, ensuring Android devices run smoothly without compromising performance. The adoption of an Android-based encrypted text messaging system will improve security, better privacy, ease of use, widespread adoption and reliability among users, an important step forward in secure communication technology.

V. CONCLUSION

A mobile device comprising: a secure element; a touch sensitive display device thatallows a user to navigate between desktop screens using swipe gestures. In this work an application is developed on the mobile phone to modify the SMS message into ciphertext so that the information content of the SMS is not known by others. SMS delivery system for encrypting messages into ciphertext using a key that is entered by the sender then sends to the destination number. SMS reception system to decrypt it to others via SMS without the fear of information from these messages will be known by others

REFERENCES

1.Sun, C., Wang, Y. and Zheng, J., 2014. Dissecting pattern unlock: The effect of pattern strength meter on pattern selection. *Journal of Information Security and Applications*, *19*(4-5), pp.308-320. Aviv, A.J., Budzitowski, D. and Kuber, R., 2015, December. Is bigger better? Comparing user-generated passwords on 3x3 vs. 4x4 grid sizes for android's pattern unlock. In *Proceedings of the 31st Annual Computer Security Applications Conference* (pp. 301-310) Kunda, D. and Chishimba, M., 2018. A survey of android mobile phone authentication schemes. Mobile Networks and Applications, pp.1-9.
2.Tsai, Y.C. and Yang, C.H., 2013. Physical forensic acquisition and pattern unlock on Android smart phones. In Future information communication technology and applications (pp. 871-881). Springer, Dordrecht.
3.Tsai, Y.C. and Yang, C.H., 2013. Physical forensic acquisition and pattern unlock on Android smart phones. In Future information communication technology and applications (pp. 871-881). Springer, Dordrecht.
4.Chaitanya, G.K. and Raja Sekhar, K., 2021. Verification of pattern unlock and gait behavioural authentication through a machine learning approach. International Journal of Intelligent Unmanned Systems.
5.Saxena, N., Uddin, M.B., Voris, J. and Asokan, N., 2011, March. Vibrate-to-unlock: Mobile phone assisted user authentication to multiple personal RFID tags. In 2011 IEEE International Conference on Pervasive Computing and Communications (PerCom) (pp. 181-188). IEEE.
6.Hintze, D., Hintze, P., Findling, R.D. and Mayrhofer, R., 2017. A large-scale, long-term analysis of mobile device usage characteristics. Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies, 1(2), pp.1-21.
7.Ibrahim, N. and Sellahewa, H., 2017, February. Touch gesture-based authentication: A security analysis of pattern unlock. In 2017 IEEE International Conference on Identity, Security and Behavior Analysis (ISBA) (pp. 1-8). IEEE.
8.Marques, D., Guerreiro, T., Duarte, L. and Carriço, L., 2013, September. Under the table: tap authentication for smartphones. In 27th International BCS Human Computer Interaction Conference (HCI 2013) 27 (pp. 1-6).
9.Løge, M.D., 2015. Tell me who you are and i will tell you your unlock pattern (Master's thesis, NTNU).
10.Aviv, A.J., Maguire, J. and Prak, J.L., 2016. Analyzing the impact of collection methods and demographics for android's pattern unlock. In Proc. Workshop on Usable Security (USEC). Internet Society.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE
SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

📱 9940 572 462 🟩 6381 907 438 ✉ ijircce@gmail.com

www.ijircce.com

Scan to save the contact details