Available online at https://asric.africa/natural-sciences
ASRIC Journal on Natural Sciences Vol 4(1) (2024) 1-9

Development of An Encrypted Messaging Service Within A Multimedia Virtual Learning System For Tertiary Institutions: Utilizing Hybrid Encryption Approaches

Emmanuel, Victoria Nkemjika[1], Enyinnaya Chibunna Victor[2] and Ezeoha Bright Uzoma[3]

[1]Imo State University, emmanuelvictoriankem@gmail.com
[2]Abia State College of Health Sciences and Management Technology, victorenyinnaya2016@gmail.com
[3]Abia State Polytechnic, bright.ezeoha@abiastatepolytechnic.edu.ng

Corresponding Author Email: emmanuelvictoriankem@gmail.com
Received 10 April 2024; revised 06 May 2024; accepted 03 June 2024

Abstract

The study on design and development of end-to-end encrypted Short Message Service (SMS) using hybrid encryption algorithm was motivated by high rate of insecurity of data observed during Short Message Service (SMS) on Mobile devices. The aim of this study is to develop end to end encrypted Short Message Service (SMS) using hybrid encryption algorithm. This work discusses various encryption algorithms. Secondary sources of data were used for gathering of relevant literatures from internet search of published journals on security and mobile technologies. In this thesis two methodologies were employed – Structured systems Analysis Design Methodology (SSADM) and Object-Oriented Analysis and Design Methodology (OOADM). With the help of the two techniques (RSA and DES algorithm) employed; integrity, confidentiality, authentication and security of messages were achieved. The implementing programs were coded in Java. At the end of the thesis, security of data during Short Message Service (SMS) on mobile devices and also confidentiality, integrity and authentication in SMS were achieved.

Keywords:

Introduction

Mobile communication devices have become common place during the past few years, integrating multiple wireless networking technologies to support additional functionality and services. One of the most important developments that have emerged from communications technology is SMS. They are designed as part of Global System for Mobile communications (GSM). Banks worldwide are using SMS to conduct some of their banking services. For example, clients are able to query their bank balances via SMS or conduct mobile payments. In addition, people sometimes exchange confidential information such as passwords or sensitive data amongst each other. SMS technology suffers from some risks such as vulnerabilities, eavesdroppers and unauthorized access. Therefore, one need to secure SMS messages and keep their contents private, without increasing their size.

Short Message Service (SMS) has become one of the fastest and strong communication channels to transmit the information across the Worldwide (Marko, 2008). SMS is the most popular mobile data

service. Due to its wide popularity SMS technology is used in various field applications. This also include security sensitive fields such as e-banking and e-government. Messages are transmitted as plaintext between mobile user (MS) and the SMS center (SMSC), using wireless network. SMS contents are stored in the systems of network operators and can be read by their personnel (Chin-Der and Yi-Ming, 2016).SMS is sent as plaintext; unfortunately, SMS does not offer a secure environment for confidential data during transmission. So the traditional SMS service offered by various mobile operators surprisingly does not provide information security it is strongly required to provide end to-end secure communication between end users. Security to the SMS is the main problem. Encryption is the process of encoding information to prevent anyone other than its intended recipient from viewing it (Nithya and Sripriya, 2016). Encrypted messaging (also known as secure messaging) provides end-to-end encryption for user-to-user text messaging. Encrypted messaging prevents anyone from monitoring your text conversations. Hybrid encryption is a mode of encryption that merges two or more encryption systems. It incorporates a combination of asymmetric and symmetric encryption to benefit from the strengths of each form of encryption. These strengths are respectively defined as speed and security. Cipher (or cypher) is an algorithm for performing encryption or decryption—a series of well-defined steps that can be followed as a procedure (Medani *et al*., 2018). To encipher or encode is to convert information into cipher or code. When using a cipher, the original information is known as plaintext, and the encrypted form as ciphertext. The ciphertext message contains all the information of the plaintext message, but is not in a format readable by a human or computer without the proper mechanism to decrypt it. The aim of the study is to develop an end-to-end encrypted Short Message Service (SMS) using hybrid encryption algorithm.

Literature Review

Theoretical Framework

The theoretical framework is a summary of the theory regarding a particular problem that is developed through a review of previous research on the variables involved.

Information Theory

Information theory studies the transmission, processing, extraction, and utilization of information. Abstractly, information can be thought of as the resolution of uncertainty. In the case of communication of information over a noisy channel, this abstract concept was made concrete in 1948 by Claude Shannon in his paper “A Mathematical Theory of Communication”, in which "information" is thought of as a set of possible messages, where the goal is to send these messages over a noisy channel, and then to have the receiver reconstruct the message with low probability of error, in spite of the channel noise. Shannon's main result, the noisy channel coding theorem showed that, in the limit of many channel uses, the rate of information that is asymptotically achievable is equal to the channel capacity, a quantity dependent merely on the statistics of the channel over which the messages are sent.

Cryptographic Theorems, Principles and Concepts.

The foundational theory for cryptography was based on three core theories namely Fermat theory, Number theory and Chinese Remainder theory stated below. Modeling this theories and concept from William’s prime number series in Mathematical algebra, William (2018) opined that “a prime number is an integer that can only be divided without remainder by positive and negative values of itself and 1. Prime number plays a critical role both in number theory and in cryptography”, in furtherance of this argument scholars have stated distinctively “two theorems that play important roles in public-key cryptography to be Fermat’s theorem and Euler’s theorem.

Conceptual Framework

Short Message Service (SMS)

Short message service (SMS) is a text messaging service component of most telephone, internet and mobile device systems (Ahonlu *et al*., 2018). It is a mobile phone application that allows digital phone

users to receive text message on their digital phones. Each message may be a maximum of 160 characters long. SMS message are supported by GSM, TDMA and CDMA based mobile phone networks currently in use today. It uses standardized communication protocols to enable mobile devices to exchange short text messages.

Encryption

Encryption has a long history dating back to when the ancient Greeks and Romans sent secret messages by substituting letters only decipherable with a secret key. Encryption is the process of using an algorithm to transform information to make it unreadable for unauthorized users.

Sharba *et al*., (2017) defined encryption as the process of making files or data unreadable with an encryption key or pass phrase so that even if somebody gains access to the files – it doesn't matter because the only thing an intruder sees is gibberish. Only with the right key can one access the encrypted file(s). As a result, it helps protect sensitive data such as credit card numbers by encoding and transforming information into unreadable cipher text. This encoded data may only be decrypted or made readable with a key. Symmetric-key and asymmetric-key are the two primary types of encryption. Encryption is essential for ensured and trusted delivery of sensitive information.

Cellular Systems Generations

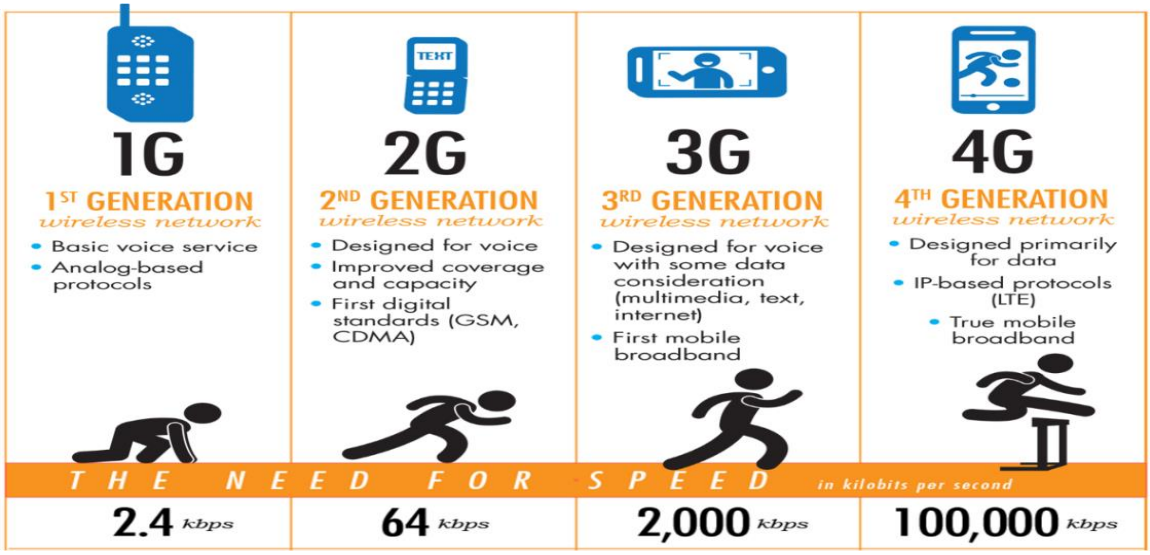
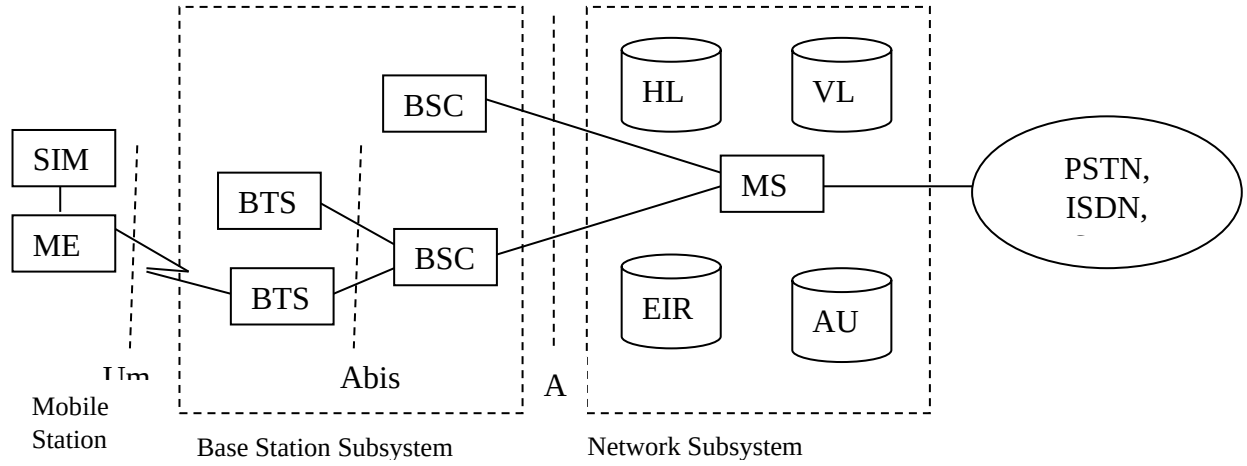


Fig 1: Evolution of Mobile network (Prema, 2017).

The diagram above showcases the evolution of mobile network from first generation to fourth generation. It also highlights some of the features of each generation and its speed per second. The functionality of the above diagram includes – flexible enough to use the features and functions of almost all public and private networks, has increased capacity, consumes less power, can be distributed to larger coverage area and reduces interference from other signals. Further explanation can be seen on IG to 4G below.

GSM Network Architecture



SIM Subscriber Identity Module
ME Mobile Equipment
BTS Base Transceiver Station
BSC Base Station Controller
HLR Home Location Register
VLR Visitor Location Register
MSC Mobile Service Switching Center
EIR Equipment Identity Register
AuC Authentication Center

Fig. 2: GSM Network Architecture. Source (Singh and Pratap, 2012)

The diagram above showcases the GSM network architecture. It consists of different elements including Network & Switching Subsystem (NSS), Base Station Subsystem (BSS), Mobile Station (MS) Operation & Support Subsystem (OSS) as well as elements including- MSC, AuC, HLR, VLR, etc. Suffice it to say that the different elements of the GSM network operate together and the user is not aware of the different entities within the system.

Architecture of Android Operating System

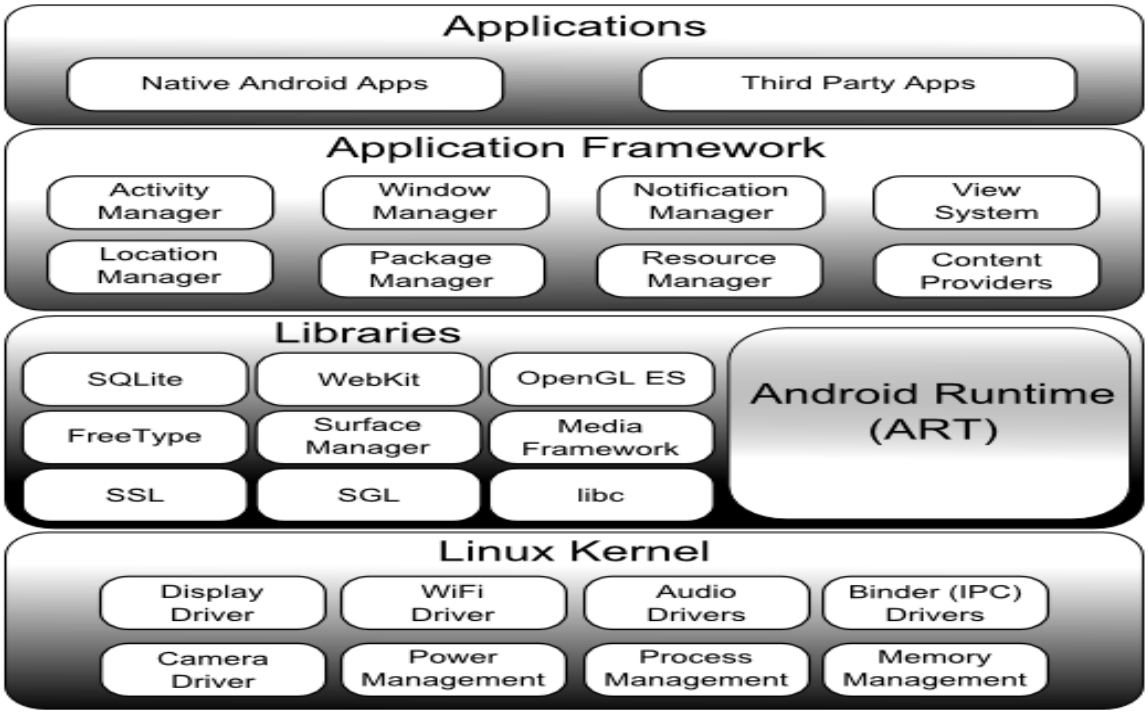


Fig. 3: Architecture of Android O/S (android.com)

The above diagram shows the architecture of android operating system. Android operating system is a stack of software components. From the above diagram, the main components of Android Operating System Architecture or Software Stack are Linux kernel, native libraries, Android Runtime, Application Framework and Applications. Android uses the Dalvik virtual machine with just-in-time compilation to run Dalvik dex-code (Dalvik Executable), which is usually translated from Java bytecode. The main hardware platform for Android is the ARM architecture. There is support for x86 from the Android x86 project, and Google TV uses a special x86 version of Android. Having carried out this research work, it is important to note that End to End Encrypted Short Message Service (SMS) app using Hybrid Cipher Algorithm can be applying in the following areas, Banking Sector, Health Sector, Department of Defense Agencies, some Companies/Organization.

Empirical Review

Literatures related to this study are acquired from libraries and online journals. The literature consisting of books, journals and other scholarly works were highly informative on the previous related works on security, Short Message Service and encryption. However, all review was based on the work that are related to research scope.

Sharbaf, (201) carried out a comparative study on cryptographic algorithms. In this paper, the authors said that MD5 algorithm takes largest encryption time whereas RSA takes least encryption time. They also found that decryption of DES algorithm is better than other algorithms, while hashing based algorithms does not require decryption. The source of data for the study is secondary gotten from online journals. Singh and Pratap (2018) carried out a study on enhancing the security of DES, Blowfish, AES algorithm using transposition cryptography techniques. In this paper, it was observed that after applying transposition cryptography technique, the security of DES algorithm was improved, while others were not. It was further observed that transposition cryptography technique is better in DES than any other algorithm. Mohsen and Shirazi (2016), provided the introduction of new secure SMS messaging protocol (SSMS) for the mobile banking. The authors use different keys for encryption and decryption. The data used for this study were collected from online journals and books. Agoyi and Devrim (2019), evaluated encryption and decryption time for three algorithms Blowfish, Elliptic curve and ELGamal to which plaintext of different sizes is provided. In this paper, the result shows that key generation, encryption and decryption time increases with an increase in key size. Mohsen *et al*., (2016), presented a survey on WEP protocol types, weaknesses and enhancements. Their paper accepted that the third generation of wireless security protocol would be WPA2/802.11i. The source of data for the study is secondary gotten from journals and books.

Research Methodologies

Object Oriented Analysis Design Methodology (OOADM)

Object-oriented analysis and design (OOAD) is a technical approach for analyzing and designing an application, system, or business by applying object oriented programming, as well as using visual modeling throughout the software development process to guide stakeholder communication and product quality. Object Oriented Analysis Design Methodology (OOADM) which comprises of the procedure of identifying software engineering requirements and developing software specifications in terms of a software system's object model and implementation of the conceptual model produced during object oriented analysis. In OOADM the researcher uses graphic symbols, Data Flow Diagrams (DFDs), Use case diagram, Collaboration diagram, Class diagram, State chart diagram, Activity diagram to represent the system. The Structured Systems Analysis and Design Methodology (SSADM) which is a systems approach to the analysis and design of information systems. SSADM provides a set of techniques and graphical tools. They allow the researcher to develop a new kind of system specifications that are easily understandable to the user. In SSADM the researcher uses graphic symbols, Data Flow Diagrams (DFDs) and Data Dictionaries (DDs) to represent the system.

Overall Use Case Diagram

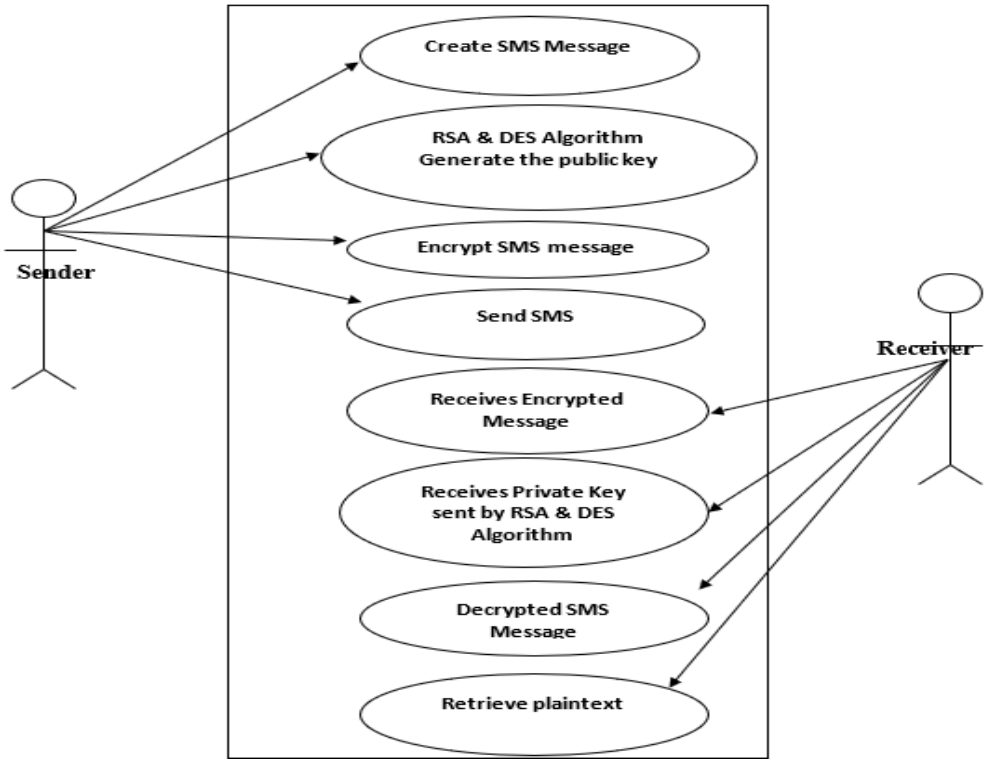


Fig. 4: Overall Use Case Diagram of SecMS App. (Field Study, 2023)

The above diagram illustrates the overall Use Case diagram, which comprises of Sender Use Case diagram and Receivers Use Case diagram. In the Sender Use Case diagram, the sender creates short message service (SMS). After that it generate the public key for the encryption process. Then encrypt the short message service (SMS) message and finally send the message. While in the Receivers Use Case diagram, the receiver receives encrypted message sent by the sender, then receives the private key after that it decrypt the SMS and finally retrieve plaintext.

Results

Architecture of the New System

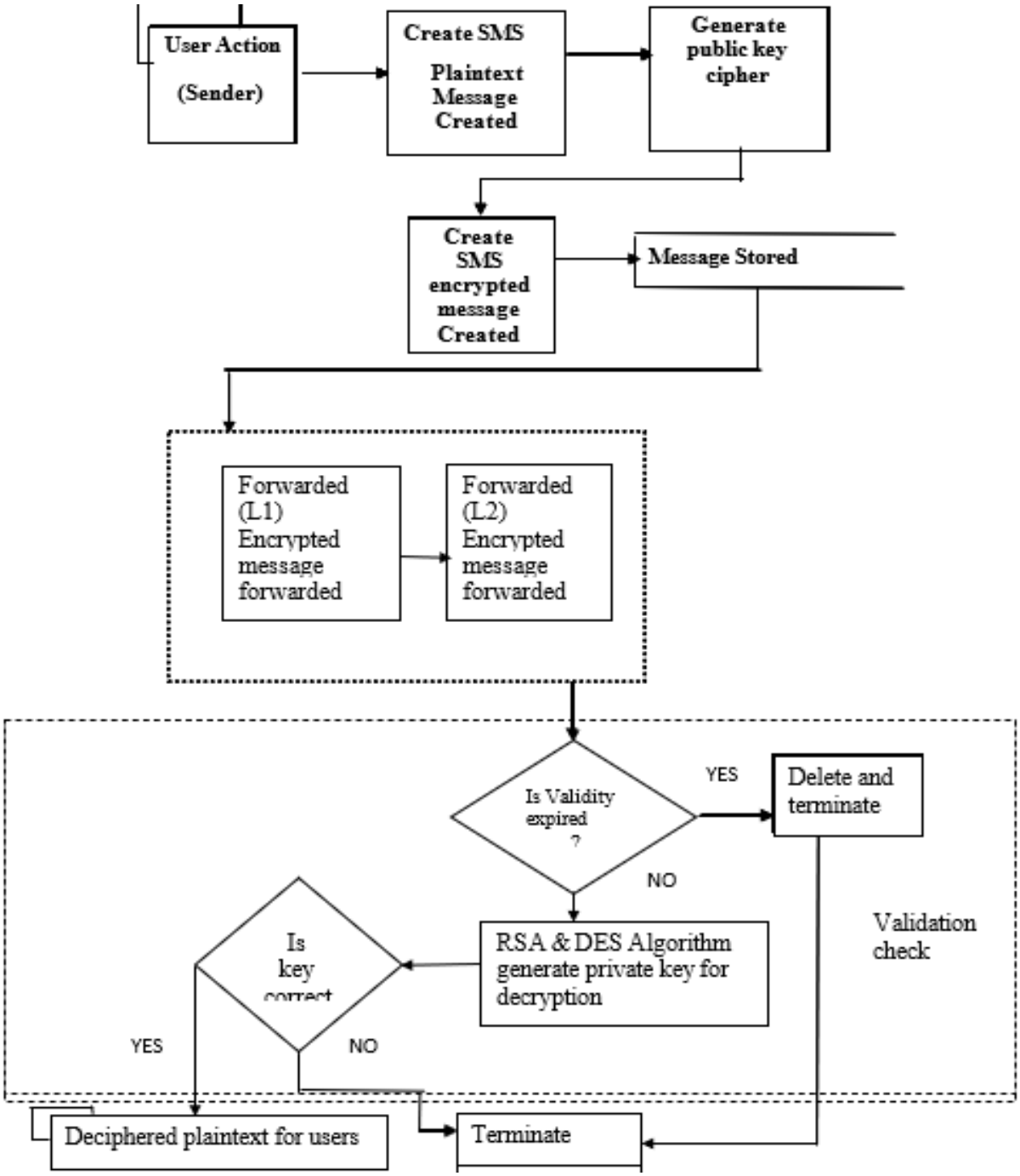
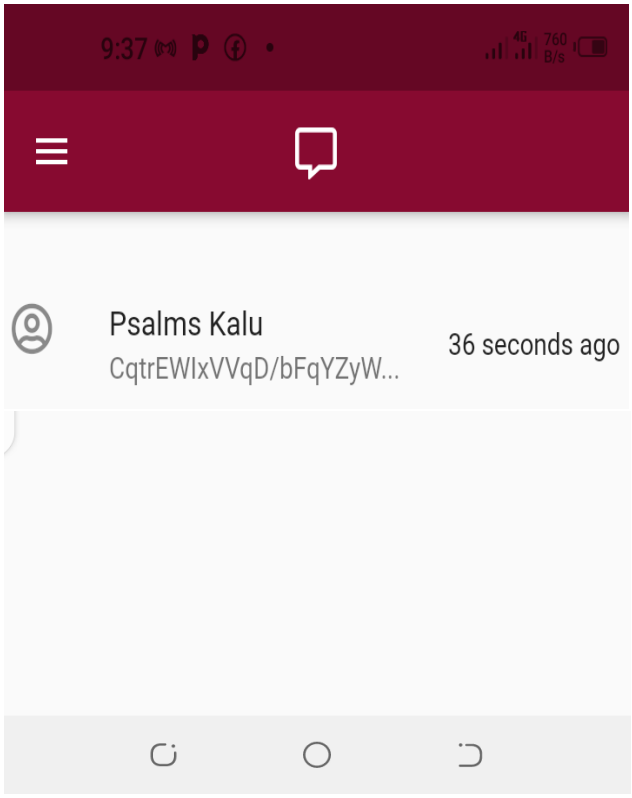
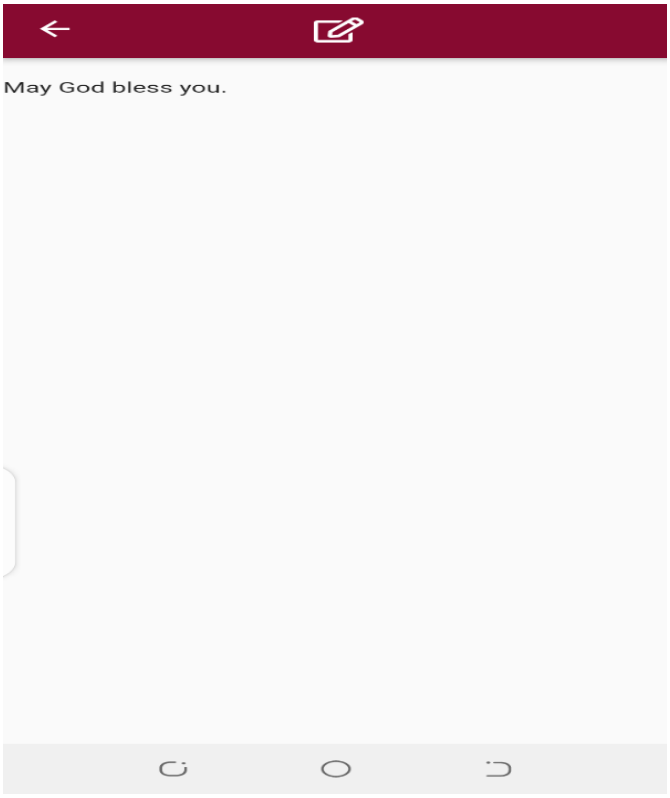


Fig 5: Showing Architecture of the New System. (Field Study, 2023)



Shows encrypted message after been sent. (Field Study, 2023)



Decrypted message been received. (Field Study, 2023)

From the above diagram, the user creates the message and the public key for encryption is automatically generated. Then the message is sent as encrypted SMS which is also retained in the short message service center (SMSC) as encrypted SMS. Validity period is checked and message is either delivered or deleted as encrypted. On delivery, the private key for decryption will automatically decrypt the message.

Conclusion

Short Message Service (SMS) is getting more popular now adays since its experimental stage by Neil Papworth. Mobile phones provide us not only communication services, but also multimedia and other functions useful for human being. Mobile phone contains private or personal data. This data is saved in a form of phone contacts, SMS notices in a calendar, photos etc. The majority of experts on information security admit that end-to-end encryption is one of the most reliable methods to secure data exchange. Based on this, the messages that are transmitted between end-to-end encryption applications can be read only by users of these apps but not by any third party. Such functionality can be achieved by using unique keys for data encryption and decryption. Only the end users can generate and store these keys.

This work presents the study on design and development of end-to-end encryption SMS using Hybrid Encryption Algorithm. It deals with providing security to data using Hybrid Encryption Algorithm. Hybrid encryption incorporates a combination of asymmetric and symmetric encryption to benefit from the strenghts of each form of encryption. It is a known fact that messages that are transmitted between end-to-end encryption applications can be read only by users of these apps but not by any third party. Also, with the help of the two cryptographic algorithms employed- Rivest Shamir Adleman (RSA) and

Data Encryption Standard; integrity, confidentiality, authentication and security of messages were achieved.

Recommendation

It is highly recommended that software developers and organizations adopt and implement encrypted end-to-end SMS using Hybrid Encryption Algorithm when designing SMS security system for mobile devices.

References

Agoyi, M. and Devrim S. (2019). *SMS Security: An Asymmetric Encryption Approach*, IEEE-20 I 0, 978-0-7695-4 182-211 0 University Science.

Chin-Der W., and Yi-Ming C., (2016). *Position tracking and velocity estimation for mobile positioning systems*, Wireless Personal Multimedia Communications 2016. The 5th

International Symposium on, vol. 1, pp. 310-314 vol.1.

Marko H. (2008), "SafeSMS - End-to-End Encryption for SMS Messages", *IEEE International Conference on Telecommunications*, 359-365.

Medani A., Gani A., Zakaria O., and Zaidan A.A (2018) "Review of Mobile Short Message Service Security Issues and Techniques Towards the Solution". *Scientific Research and Essays* Vol.6(6) pp. 1147- 1165

Menezes, A. J.; Van-Oorschot, P. C.; and Vanstone, S.A. (2016). *Handbook of Applied Cryptography*. ISBN978-0-8493-8523-0 Archived from the original on 7 March 2016.

Mohsen E., and Shirazi, C. (2016). "SSMS-A secure SMS messaging protocol for the m-payment systems," IEEE ISCC, pp. 700–705.

Nithya B. and Sripriya P, (2016) Comparative Analysis of Symmetric Cryptographic Algorithms on .Net Platform. *Indian Journal of Science and Technology*, Vol 9 (27)

Prema M. (2017). A Study of Encryption Algorithms AES, DES and RSA for Security. *Global Journal of Computer Science and Technology Network*, Web & Security Vol. 13 Issue 15

Sharbaf, M. S. (2017). Quantum Cryptography: An Emerging Technology in Network Security. *2011 IEEE International Conference on Technologies for Homeland Security (HST)*. pp. 13–19.

Singh, S., and Pratap S., (2012) "Key Concepts and Network Architecture for 5G Mobile Technology.", *International Journal of Scientific Research Engineering & Technology*, 15

Singh, S., Maakar, S. K., & Kumar, D. S. (2018). Enhancing the security of DES algorithm using transposition cryptography techniques. *International Journal of Advanced Research in Computer Science and Software Engineering*, 3(6), 464-471.

Sri R. and Sai R. (2018). Securing SMS using Cryptography. *International Journal of Computer Science and Information Technologies*, Vol.4.