Scientific Research Publishing

Journal of Software Engineering and Applications, 2020, 13, 25-40
https://www.scirp.org/journal/jsea
ISSN Online: 1945-3124
ISSN Print: 1945-3116

Design and Implementation of End to End Encrypted Short Message Service (SMS) Using Hybrid Cipher Algorithm

Emmanuel Nwabueze Ekwonwune[1], Victor Chibunna Enyinnaya[2]

[1]Department of Computer Science, Imo State University, Owerri, Nigeria
[2]Department of Computer Science, Abia State College of Health Sciences and Management Technology, Aba, Abia State, Nigeria
Email: ekwonwuneemmanuel@yahoo.com

How to cite this paper: Ekwonwune, E.N. and Enyinnaya, V.C. (2020) Design and Implementation of End to End Encrypted Short Message Service (SMS) Using Hybrid Cipher Algorithm. *Journal of Software Engineering and Applications*, **13**, 25-40.
https://doi.org/10.4236/jsea.2020.133003

Received: August 14, 2019
Accepted: March 28, 2020
Published: March 31, 2020

Abstract

The study on design and implementation of end to end encrypted Short Message Service (SMS) using hybrid cipher algorithm is motivated by high rate of insecurity of data observed during Short Message Service (SMS) on Mobile devices. SMS messages are one of the popular ways of communication. The aim therefore is to design a software for end to end encryption short message service (SMS) that can conceal message while on transit to another mobile device using Hybrid Cipher Algorithm on Android Operating System and implement it for security of mobile SMS. Hybrid encryption incorporates a combination of asymmetric and symmetric encryption to benefit from the strengths of each form of encryption. Various encryption algorithms have been discussed. Secondary sources were employed in gathering useful data. In this research work three methodologies are employed—Structured System Analysis Design Methodology (SSADM), Object Oriented Analysis Design Methodology (OOADM) and prototyping. With the help of the three cryptographic algorithms employed—Message digest 5 (MD5), Blowfish and Rivest-Shamir Adleman (RSA); integrity, confidentiality, authentication and security of messages were achieved. The messages encrypted by developed application are also resistant to brute force attack. The implementing programs were coded in Java.

Keywords

Encryption, Hybrid, Security, Integrity, Authentication, Vulnerability, Cryptography, Short Message Service (SMS), Global System for Mobile Communication (GSM), Message Digest 5 (MD5), Blowfish and Rivest-Shamir Adleman (RSA)

1. Introduction

Information security is the process of protecting information. It protects its availability, privacy and integrity. Access to stored information on computer databases has increased greatly.

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 Short Message Service (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 Short Message Service (SMS) or conduct mobile payments. In addition, people sometimes exchange confidential information such as passwords or sensitive data amongst each other. Short Message Service (SMS) technology suffers from some risks such as vulnerabilities, eavesdroppers and unauthorized access. Therefore, we need to secure SMS messages and keep their contents private, without increasing their size.

Short Message Service (SMS) is a standard communication service in the Global System for Mobile Communications. It is a technology that enables text messages to be sent and received as same as voice calls. The short message is transmitted over the radio channel using the signaling path. The first appearance of Short Message Service (SMS) is in Europe in 1992. The maximum size of Short Message Service (SMS) is (160 characters if 7-bit character encoding) or (70-character if 16-bit Unicode character) is used. Short Message Service (SMS) contains some meta-data—sender number and Service center number, Data coding scheme and Protocol identifier and Time stamp.

Short Message Service (SMS) has become one of the fastest and strong communication channels to transmit the information across the Worldwide. SMS is the most popular mobile data service. Due to its wide popularity, Short Message Service (SMS) technology is used in various field applications. This also includes security sensitive fields such as e-banking and e-government. Messages are transmitted as plaintext between mobile user (MS) and the Short Message Service Center (SMSC), using wireless network. Short Message Service (SMS) contents are stored in the systems of network operators and can be read by their personnel. Short Message Service (SMS) is sent as plaintext; unfortunately Short Message Service (SMS) does not offer an secure environment for confidential data during transmission. So the traditional Short Message Service (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 Short Message Service (SMS) is the main problem.

Encryption is the process of encoding information to prevent anyone other than its intended recipient from viewing it. 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.

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. Cipher is an algorithm for performing encryption or decryption.

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.

Hybrid encryption is considered a highly secure type of encryption as long as the public and private keys are fully secure.

1.1. Statement of Problem

Short Message Service (SMS) has become one of the fastest and strong communication channels to transmit the information across the worldwide. The Short Message Service (SMS) business being on such a great rise is vulnerable to attacks. Accordingly it has now turned out to be more basic to encode Short Message Service (SMS) before sending. Encrypted messaging isn't generally vital, but it can still be a welcome safeguard for whenever you, your family, or business partners need to communicate sensitive information from one side of the globe to the next. Smart phones have become an essential part in the life of the individuals and their priorities at the present time. The most prominent uses are in chatting and conversation applications. Some of the problems encountered in these applications include:

1) No required protection and privacy of the data exchange between users.

2) Easily hacked Short Message Service (SMS).

3) Lack of Authentication Assurance: SMS messages lacks authentication of sender source, made possible by encryption and communication of decryption key to the receiver.

4) Problem of developing and deploying an end-to-end encryption application for the SMS mobile technology application.

5) Continuous compromise on data transmitted over the internet as it is always insecure, which provide great danger for end users and mobile phone users.

6) Lack of locally developed and deployed applications for secure mobile SMS transmission using existing encryption concepts.

1.2. Aim and Objectives of Study

The aim of the study is to design a software for end-to-end encryption short message service (SMS) that can conceal message while on transit to another mobile device using Hybrid Cipher Algorithm on android operating system and implement it for security of mobile Short Message Service (SMS). The objectives for achieving this are shown below:

i) To develop a software that will ensure the encryption of every message transmitted within the network of an organization. This software will provide security measures whenever information is transmitted from one mobile device to another because it is important to protect the information while it is on transit.

ii) To determine the best security encryption algorithm for mobile devices with consideration of Smartphone capabilities.

iii) To develop a new cryptography algorithm for end-to-end encrypted Short Message Service (SMS) that will be better than conventional cryptographic algorithm and highly effective against brute force attack.

1.3. Scope and Limitations of Study

This research work on design and implementation of encrypted end-to-end Short Message Service (SMS) using Hybrid Cipher Algorithm focuses on security of Short Message Service (SMS) with much concentration on confidentiality, integrity and privacy of message on transit. Considering the time frame and large scope of security in computing we will not be able to study all aspects. However, the scope will rely fully on Short Message Service (SMS) security and use of Hybrid Cipher Algorithm to achieve end-to-end communication. Furthermore, the research work does not cover voice call, video or stored files in the mobile device. As such the encryption requirements of voice traffic and other data traffic were not discussed. But a review of characteristics of different encryption schemes and their performance on modern mobile devices was presented. A total comparison of Short Message Service (SMS) properties were assessed with respect to their impact on encryption scheme selected.

Based on its merits, a suitable encryption scheme for Short Message Service (SMS) was selected and deployed. A typical application that runs on android was developed and used to validate the selection. Several mobile development platforms exist but this research work centered on Android mobile phone Operating system. More so, the concentration was on Short Message Service (SMS) for communication and all development requirement concepts are based on android standards.

The application can be deployed in industries for secured data transfer and by extension can be used for business and non-commercial use. The main purpose was to develop encrypted end-to-end Short Message Service (SMS) using hybrid cipher algorithm on android operating system and implement it for security of mobile short message service (SMS).

1.4. Significance of the Study

This research work will be beneficial to the following:

1) Software developers: This research work will help to give a prototype and information on how to develop an application for encrypted end-to-end SMS using hybrid cipher algorithm.

2) Trainee Programmers: It would provide real information that will fill the knowledge gaps which exists in the security and cryptography body of knowledge.

3) Financial Institution: It will provide security strategy application for financial transactions that relies heavily on Short Message Service platform. This is because it will conceal Short Message Service on transit and ensure security of the channel, message and sender.

4) Researchers: It will serve as a reference material to any researcher who intends to embark on a similar research work.

2. Review of Empirical Literatures

Literatures related to this study are gotten 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 reviews were based on the works that are related to research scope.

[1] proposed "*A comparative study of Cryptographic Algorithms*". Their study showed the performance of existing cryptographic methods like RSA, AES, Blowfish, DES, Elliptic Curve, MD5, SHA, and RSA algorithms. Based on their experimental result it was affirmed that MD5 algorithm takes least encryption time whereas, RSA takes largest encryption time. They also found out that Decryption of Blowfish algorithm is better than other algorithms. While, hashing based algorithms does not require decryption.

[2] used their research to propose a new project "*Enhancing the Security of DES Algorithm Using Transposition Cryptography Techniques*" to improve the security of DES algorithm by addition of transposition techniques before the process performance of DES algorithm. By using an Enhanced DES algorithm the security was improved. When the transposition technique was used before the original DES, the intruder is required first to break the original DES algorithm and then transposition technique. Hence, the security was approximately double as compared to simple DES algorithm. In contrast to the proposal and implementation of the specific algorithm, several other aspects of their works focused on comparison to ascertain the best algorithm for use in securing data.

These works are pointers to the direction for further research, In 2013 Malhotra and Singh proposed "*Study of Various Cryptographic Algorithms*". Their proposal took study of AES, DES, RSA, Diffie-Hellman, RC4, Blow Fish, ElGamal, MD5, and Miller-Rabin and provided a summary study of works done in various cryptography field and various cryptographic algorithms being used through a literature survey of between 2008 and 2013. Their study provided a direction to the naïve users and allows many new future applications.

[3] provided the introduction of new Secure SMS Messaging Protocol (SSMS) for the M-payment. It being an application layer protocol and is intended for GSM users as a secure bearer in the M-payment system. It uses elliptic curve based public key solution which uses public key as secret key for symmetric encryption. Also it uses different keys for encryption and Decryption.

[4] compared the performance analysis of evolving wireless 802.11 security

architecture. Their work explained, wireless network security methods with emphasis on security layers like WEP shared key authentication and 40 bit encryption, WEP shared key authentication and 104 bit encryption, WPA with PSK authentication and RC4 encryption, WPA with EAP-TLS authentication and RC4 encryption, WPA2 with PSK authentication and AES encryption and WPA2 with EAP-TLS authentication and AES encryption plus effects on the throughput [4].

[5] proposed accost effective scheme which uses a concept called Cheating Text. The original message is embedded in a meaningful text called cheating text. Here, index table called (Real Message Index File) RIF file is hashed and sent to the receiver along with the cheating text in which the original message is embedded. Authentication is achieved by verifying the hash value of the plain text.

2.1. Short Message Service (SMS) Overview

Short message service (SMS) is a text messaging service component of most telephone, internet and mobile device systems [6]. It is a mobile phone application that allows digital phone users to receive text message on their digital phones [7]. Each message may be a maximum of 160 characters long. Short Message Service (SMS) message are supported by GSM, TDMA and CDMA based mobile phone networks currently in use today [8]. It uses standardized communication protocols to enable mobile devices to exchange short text messages. An intermediary service can facilitate a text-to-voice conversion to be sent to landlines. Short Message Service (SMS) was the most widely used data application at the end of 2010, with an estimated 3.5 billion active users or about 80% of all mobile subscribers [6] The benefits of Short Message Service (SMS) to subscriber center on convenience, flexibility and seamless integration of messaging services and data access provided by mobile platforms. These benefits depend on the application the service provider offers. The advancement of mobile technology has revolutionalized the way peoples use mobile devices in their day to day activities [8]. Short Message Service (SMS) as used on modern devices originated from radio telegraphy in radio memo pagers that used standardized phone protocols. These were defined in 1985 as part of the Global system for mobile communications (GSM) series of standards [9]. The first Short Message Service (SMS) message was sent in 1992 [10].

Short Message Service (SMS) is also employed in mobile marketing a type of direct marketing [11]. According to one market research report as of 2014 the global Short Message Service (SMS) messaging business was estimated to be worth over $100 billion, accounting for almost 50 percent of all the revenue generated by mobile messaging [12]. While Short Message Service (SMS) is still a growing market, it is being increasingly challenged by internet protocol based messaging services such as apples, massage, face book Messenger Whats App, Viber Wechat (in china) and line (in Japan) available on smart phones with data connections. It has been reported that over 97% of smart phone owners use alternative messaging services at least one a day (**Figure 1**).

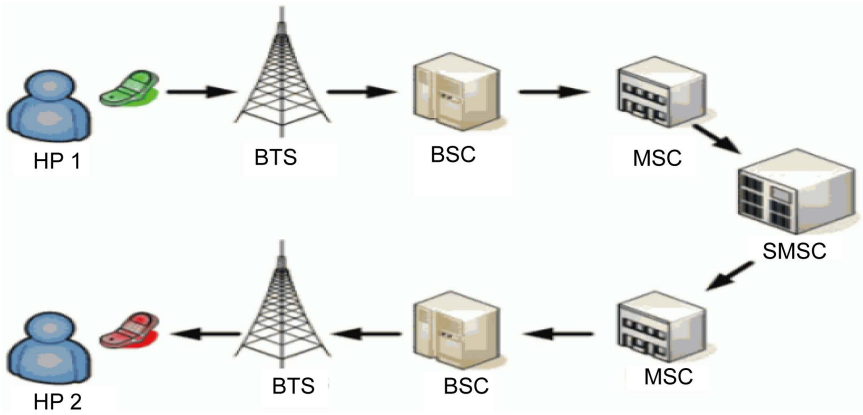

Figure 1. Transmission Path of SMS: Source (Rohan, Sanket and Priyanka, 2012).

Short Message Service centers (SMSC) is used to store the Short Message Service messages before they are forwarded to the mobile users service provider or another SMSC. Although the network connections between the SMSC and nodes in a GSM network are usually protected by virtual private network (VPN) tunnels, the Short Message Service (SMS) messages are stored unencrypted at the SMSC. This means that employees of SMSC operators or others who can hack into can view all the SMS messages passing through the SMSC. Many Short Message Service Centre (SMSCs) also retain a copy of the SMS messages for audit, billing and dispute resolution purpose. If an attacker manages to compromise the SMSC, the attacker can also read the SMS traffic.

Some of the features of Short Message Service (SMS) that have led to its popularity are:

1) Short Message Service (SMS) supports confirmation of message delivery. The sender of the message can choose to receive a return message back to indicate whether the Short Message Service (SMS) has been delivered or not.

2) Short Message Service (SMS) can be sent and received simultaneously with other traffic. SMS uses the control channel as a transport mechanism, unlike voice, data and fax calls which use dedicated radio channels for the duration of the call.

3) Short Message Service (SMS) compression and concatenation have been defined and incorporated into the GSM SMS standards. As such, the original 160 character limitation has been overcome.

However, [13] state that Short Message Service (SMS) is a mobile technology that enables sending and receiving of messages between text-enabled Smartphone's. It was included in the GSM standards right at the beginning and later ported to wireless technologies like Code Division Multiple Access (CDMA) and Time Division Multiple Access (TDMA). As implied by its name "Short Message Service", the data value that can be held by an SMS message is very limited. For instance one SMS message can contain at most 160 bytes of data when 8 bit character encoding is used or 80 characters if 16-bit Unicode character encoding is used [13]. SMS text messaging supports languages internationally and works fine with all languages supported by Unicode including Arabic, Chinese, Japanese and Korean.

Short Message Service (SMS) application has become successful and a massive revenue earner worldwide among all wireless carrier. Besides text, SMS messaging can also carry binary data; send ringtones, pictures, wallpapers, animations and business secrets and other Wireless Application Protocols (WAP) configurations to a mobile phone. The wide varieties of application of Short Message Service (SMS) stem from one major advantage, which is its compatibility and support for all GSM mobile phones, while others merits are inexpensive nature and old mobile phone acceptance.

2.2. Security Overview

Information security is seen as the act of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information [14]. Encryption is the best approach to accomplish information security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it. Unencrypted data is called plain text encrypted data is referred to as cipher text [14]. Keeping up security in our personal communication is something everybody wants. The objectives of online security include protection of information and property from theft, corruption or threats attack while allowing the information and property to remain accessible and productive to its intended users. This affirms that "Security is the collective processes and mechanisms by which sensitive and valuable information and services are protected from publication, tampering or collapse by unauthorized activities or untrustworthy individuals and unplanned events respectively.

As short message service (SMS) is currently broadly utilized as a business tool, its security has turned into a noteworthy worry for business organization and customers [15]. Encryption is the coding or scrambling of information so that it can only be decoded and read by someone who has the correct decoding key [16]. In [17] cryptography algorithm was defined as the techniques used for concealing the content of message from all users except the sender and the receiver and to authenticate the correctness of the message to the recipient. The most common of these are encryption algorithms. A study by [18] On encryption time and algorithms AES, DES, and RSA for security showed that advanced encryption standard (AES) consume least encryption time and generates better output on decryption of message.

[18] Opines that in a symmetric key algorithm (e.g. DES and AES) the sender and receiver must have a shared key set up in advance and kept secret from all other parties, the sender uses this key for encryption and the receiver uses the same key for decryption. He said that in an asymmetric key algorithm (e.g. RSA) there are two separate key; a public key is published and enables any sender to perform encryption while a private key is kept secret by the receiver and enables only him to perform correct decryption. There are examples of symmetric cryptographic algorithms like AES and DES. AES uses various 128,192,256 bit keys while DES uses one 64-bit key [18]. All these algorithms can provide authentication, integrity, confidentiality and authorization to data travel from one point to anoth-

er point. The RSA algorithm is the most widely known asymmetric key cryptographic algorithm. The entire RSA algorithm can be performed using three step-key generation, encryption, decryption.

Deploying RSA with object oriented modeling technique yields a better SMS encryption app on android/S [19]. Cipher is an algorithm for performing encryption or decryption [20]. The operation of a cipher usually depends on a piece of auxiliary information called a key [20]. A series of well defined steps that can be followed as a procedure. An alternative, less common term is encipherment. To encipher or encode is to convert information into cipher or code. He said that cipher is synonymous with code, as they are both a set of steps that encrypt a message codes generally substitute different length string of characters in the output while ciphers generally substitute the same number of characters as are input [21]. When using a cipher, the original information is known as plaintext and the encrypted form as cipher text. The cipher text message contains all the information of 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 encrypting procedure is varied depending on the key which changes the detailed operation of the algorithm.

A key must be selected before using a cipher to encrypt a message. Without knowledge of the key, it should, be extremely difficult if not impossible to decrypt the resulting cipher text into readable plaintext. Modern encryption methods can be divided by two criteria by type of key used and by type of input data. By type of key used ciphers are divided into symmetric key algorithms (private key cryptography) where the same key is used for encryption and decryption and asymmetric key algorithms (public key cryptography) where two different keys are used for encryption and decryption. He added that ciphers can be distinguished into two types by the type of input data—block ciphers which encrypt block of data of fixed size and stream ciphers which encrypt continuous streams of data.

2.3. Global System for Mobile Communication (GSM) and Security

The Global System for Mobile Communications (GSM) is a standard developed by the European Telecommunications Standards Institute (ETSI) to describe the protocols for second-generation (2G) digital cellular networks used by mobile devices such as mobile phones and tablets. It was first deployed in Finland in December 1991 [22]. By the mid-2010s, it became a global standard for mobile communications achieving over 90% market share, and operating in over 193 countries and territories [23].

2G networks developed as a replacement for first generation (1G) analog cellular networks. The GSM standard originally described a digital, circuit-switched network optimized for full duplex voice telephony. This expanded over time to include data communications, first by circuit-switched transport, then by packet data transport via General Packet Radio Service (GPRS), and Enhanced Data Rates for GSM Evolution (EDGE). Subsequently, the 3GPP developed third-generation

(3G) UMTS standards, followed by fourth-generation (4G) LTE Advanced standards, which do not form part of the ETSI GSM standard.

GSM was intended to be a secure wireless system. It has considered the user authentication using a pre-shared key and challenge-response, and over-the-air encryption. However, GSM is vulnerable to different types of attack, each of them aimed at a different part of the network [24].

The development of UMTS introduced an optional Universal Subscriber Identity Module (USIM), that uses a longer authentication key to give greater security, as well as mutually authenticating the network and the user, whereas GSM only authenticates the user to the network (and not vice versa). The security model therefore offers confidentiality and authentication, but limited authorization capabilities, and no non-repudiation.

GSM uses several cryptographic algorithms for security. The A5/1, A5/2, and A5/3 stream ciphers are used for ensuring over-the-air voice privacy. A5/1 was developed first and is a stronger algorithm used within Europe and the United States; A5/2 is weaker and used in other countries. Serious weaknesses have been found in both algorithms: it is possible to break A5/2 in real-time with a ciphertext-only attack, and in January 2007, The Hacker's Choice started the A5/1 cracking project with plans to use FPGAs that allow A5/1 to be broken with a rainbow table attack [25]. The system supports multiple algorithms so operators may replace that cipher with a stronger one.

Since 2000 different efforts have been made in order to crack the A5 encryption algorithms. Both A5/1 and A5/2 algorithms have been broken, and their cryptanalysis has been revealed in the literature. As an example, Karsten Nohl developed a number of rainbow tables (static values which reduce the time needed to carry out an attack) and have found new sources for known plaintext attacks. GSM uses General Packet Radio Service (GPRS) for data transmissions like browsing the web.

3. Methodology

Research methodology can be defined as a scientific method of enquiry involving formal process of verifying knowledge. It entails the plan and systematic collection, analysis and presentation of data. It compasses sources of data collected, method, analysis and interpretation of data collected. Research methodology therefore contains information on how data was collected, while design referred to planned structure and strategy of investigation though in order to get responses to research question and control variance. It can be said to be general program of study. It defines how the objects of the study will be accomplished and how problems encountered will be treated.

However, the researcher will employ three methodologies—The Structured Systems Analysis and Design Methodology (SSADM) which is a systems approach to the analysis and design of information systems, Object Oriented Analysis design Methodology which comprises of the procedure of identifying software engineering requirements and developing software specifications in terms of a software sys-

tem's object model and implementation of the conceptual model produced during object oriented analysis and Prototyping. 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. Furthermore, the SSADM which was adopted in this research work has the following components which are contextually presented below:

i) Problem Identification
ii) Feasibility Study
iii) Analysis
iv) Design
v) Implementation
vi) Post Implementation Maintenance

Finally, three cryptographic algorithms were also used—Message digest 5 (MD5), Blowfish and Rivest-Shamir Adleman (RSA).

3.1. High Level Model of Mobile SMS Encryption App

The high level model shows the starting of the application with either encryption process or decryption process as it deems fit by the user. The high level model is breakdown into two phases—The sender's system phase and the receiver's system phase. In the sender's system phase, the user opt to login and create or compose the message, then initialize Rivest Shamir Adleman (RSA) for key generation and finally apply Blowfish with RSA or MD5 with Twofish for message encryption. This is illustrated in Figure 2.

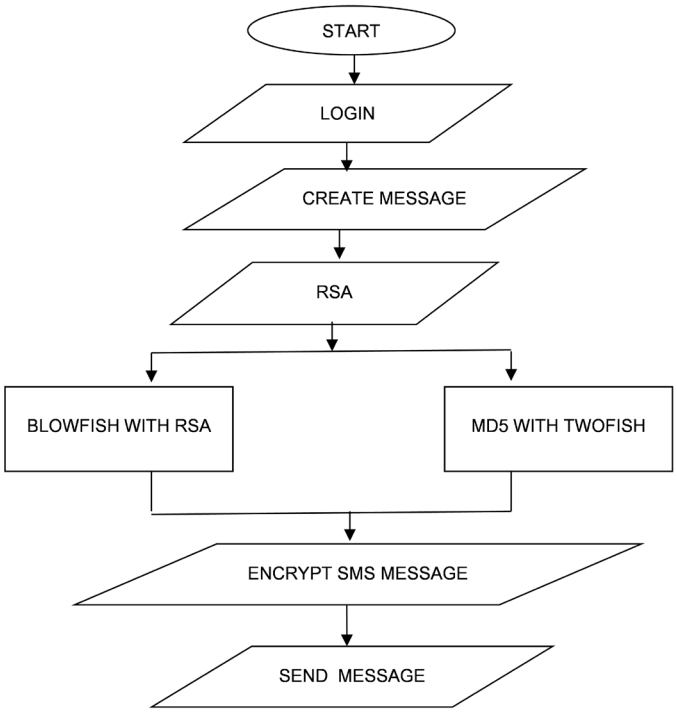

Figure 2. Shows sender's system phase.

At the receiver's system phase, the user select login, received the encrypted message, enter the correct key, if the key is correct the user will now select Blowfish with RSA or MD5 with Twofish to decrypt the SMS message and finally retrieve the plaintext but where the key entered is not correct then access denied. This is also illustrated in Figure 3.

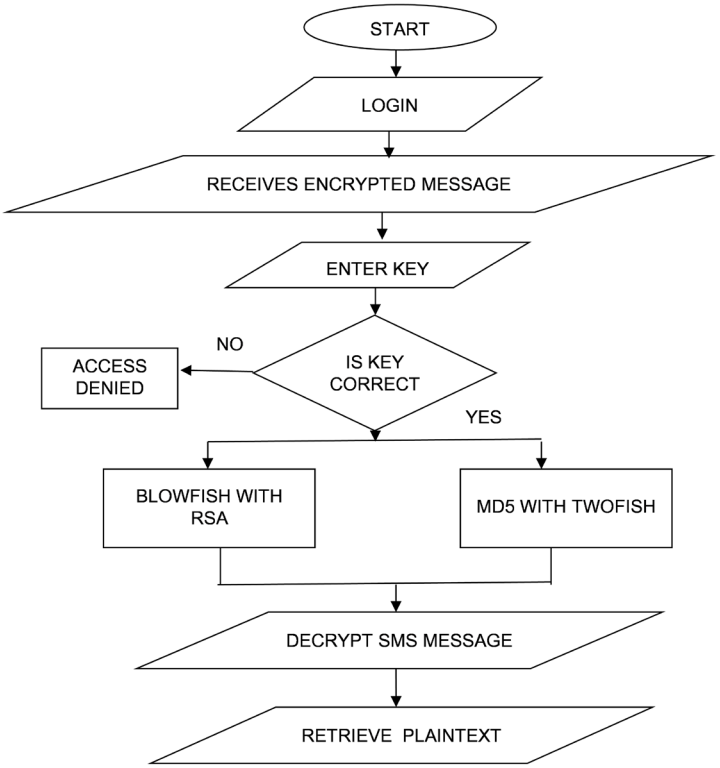

Figure 3. Shows receiver's system phase.

3.2. Application Screen

3.2.1. Splash Screen

The splash screen create room for the user to compose messages, view the inbox and search for contact numbers (see Figure 4).

3.2.2. Compose Message

In this interface, the user type in the message, select the receipient phone number and click on send button. It also has provision for the user to view the recent messages and also access its contact. There is also provision for attachment of short messages (see Figure 5).

3.2.3. Encrypted and Decrypted Messages

The screen shows the encrypted and decrypted messages. Once the message enters the receiver's phone. The receiver will only see the encrypted message. The receiver will now click on Decrypt button to convert the encrypted messge to plaintext. The Delete button is use to delete the message if the receiver want to do so (see Figure 6).

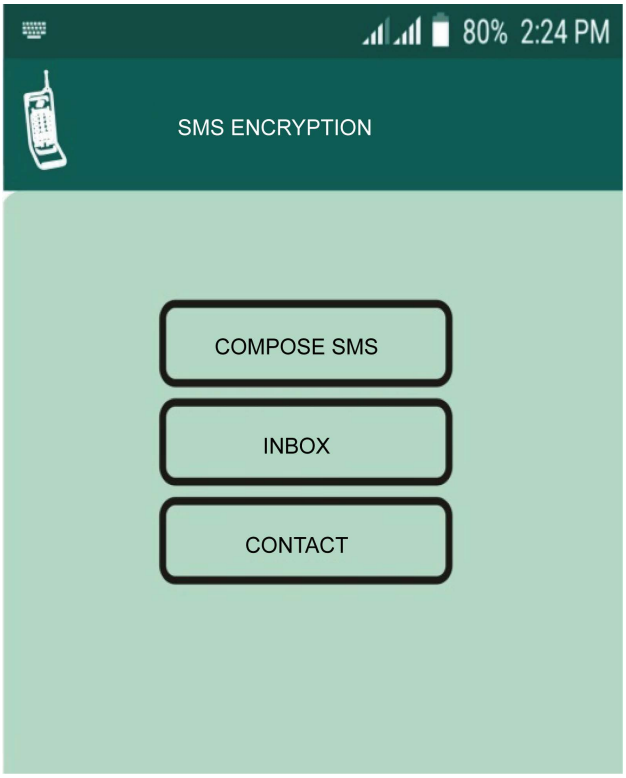

Figure 4. Shows the splash screen.

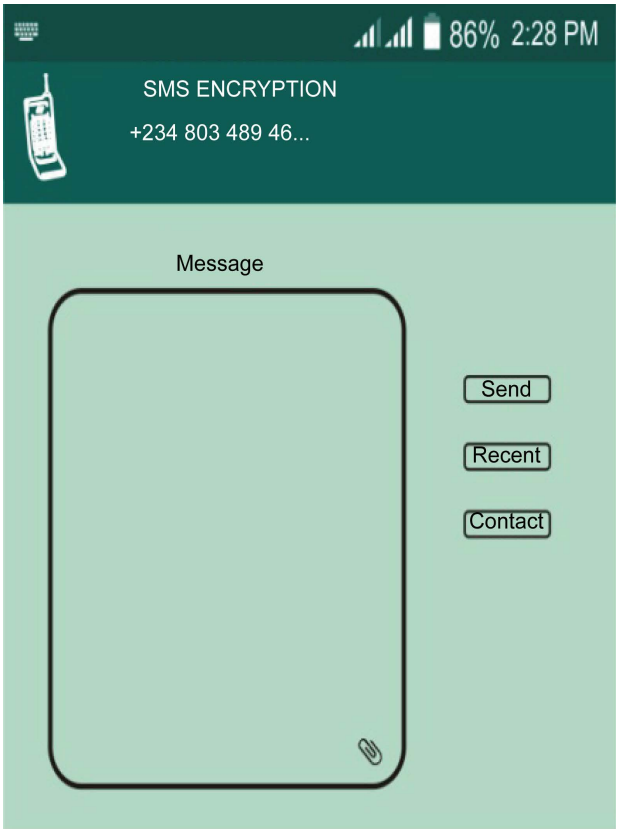

Figure 5. Shows the compose message.

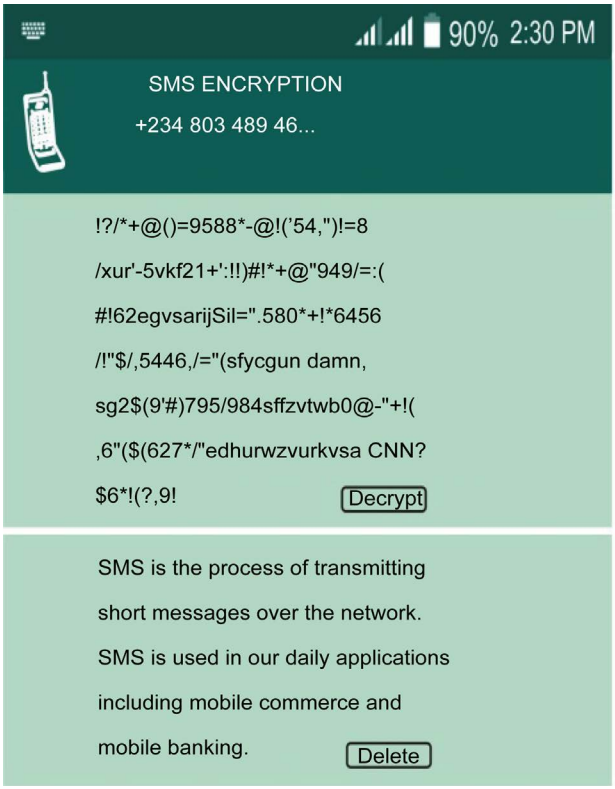

Figure 6. Shows encrypted and decrypted message.

4. Results and Discussion

The software developed—Design and Implementation of End to End Encrypted SMS using Hybrid Cipher Algorithm is designed in Java. The software developed was tested with two android phones in order to ascertain the transmission of SMS messages across platforms. Result proves that transmission of SMS is based on availability of wireless network service by network providers. The messages sent without service will be delivered even if the receiving device cannot be contacted, if a wireless recipient is switched off, out of range, the SMS message will be stored in the network and delivered when the recipient becomes available again. Message digest 5 (MD5) algorithm helps to achieve integrity of the message while Blowfish and Rivest Shamir Adleman (RSA) help to achieve confidentiality and authentication and also provide more security when messages are sent over the network.

5. Conclusions

This paper presents the study on design and implementation of end to end encryption SMS using Hybrid Cipher Algorithm. It deals with providing security to data using Hybrid Cipher Algorithm. Hybrid encryption incorporates a combination of asymmetric and symmetric encryption to benefit from the strengths 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 thethree cryptographic algorithms employed—Message digest 5 (MD5), Blowfish and Rivest-Shamir Adleman (RSA), integrity, confidentiality, authentication and security of messages were achieved.

6. Recommendation

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

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Shaza, D.R., Ahmed, K., *et al*. (2012) A Performance Comparison of Encryption Algorithms AES and DES. *International Journal of Engineering Research and Technology*, **4**, 151-154.

[2] Singh, S., Maakar, S.K. and Kumar, D.S. (2013) Enhancing the Security of DES Algorithm Using Transposition Cryptography Techniques. *International Journal of Advanced Research in Computer Science and Software Engineering*, **3**, 464-471.

[3] Toorani, M. and Beheshti, S.A.A. (2008) A Secure SMS Messaging Protocol for the M-Payment Systems. *IEEE Symposium on Computers and Communications*, Marrakech, 6-9 July 2008, 12-15. https://doi.org/10.1109/ISCC.2008.4625610

[4] Gin, A. and Hunt, R. (2008) Performance Analysis of Evolving Wireless IEEE 802.11 Security Architecture. *Proceedings of the* 5*th International Conference on Mobile Technology, Applications and Systems*, *Mobility Conference* 2008, Yilan, September 2008, 50-57. https://doi.org/10.1145/1506270.1506393

[5] Rupa, Ch. and Avadhani, P.S. (2009) Message Encryption Scheme Using Cheating Text. 6*th International Conference on Information Technology*: *New Generations*, Las Vegas, 27-29 April 2009, 470-474. https://doi.org/10.1109/ITNG.2009.232

[6] Ahonlu, T.T. (2011) Time to Confirm Some Mobile User Numbers: SMS, MMS, Mobile Internet, M-News. Communities Dominate Brands.

[7] ESTI (2006) Analysis of the Short Menage Service (SMS) and Call Broadcast Service (CBS) for Emergency Menaging Application; SMS and CBS.

[8] Sharad, K.V. and Ojha, D.B. (2014) An Approach to Enhance the Mobile SMS Security. *Journal of Global Research in Computer Science*, **5**, 25-30.

[9] Han, E. (2015) Cheaper Mobile Calls and Text as ACCC Moves to Slash Wholesale Fees.

[10] Wiley, H. (2010) SMS the Creation of Personal Global Text Menaging.

[11] Black, K. (2016) What Is SMS Marketing? WiseGEEK.

[12] Portio Research (2014) Portio Research Mobile Menaging Futures 2014-2018.

[13] Sagheer, A.M., Abdulhameed, A.A. and Abduljabbar, M.A. (2013) SMS Security for Smartphone. 6*th International Conference on Developments in eSystems Engineering*, Abu Dhabi, 16-18 December 2013, 32-35. https://doi.org/10.1109/DeSE.2013.57

[14] Biggs, N. (2008) Codes: An Introduction to Information Communication and Cryptography. Springer, Berlin, 171. https://doi.org/10.1007/978-1-84800-273-9

[15] Loon Ng (2016) Short Message Service (SMS) Security Solution for Mobile Devices. Master's Thesis, Naval Postgraduate School, Monterey.

[16] Lisoněk, D. and Drahanský, M. (2008) SMS Encryption for Mobile Communication. *IEEE International Conference on Security Technology*, Hainan Island, 13-15 December 2008, 198-201. https://doi.org/10.1109/SecTech.2008.48

[17] Sharbaf, M.S. (2011) Quantum Cryptography: An Emerging Technology in Network Security. *IEEE International Conference on Technologies for Homeland Security*, Waltham, 15-17 November 2011, 13-19. https://doi.org/10.1109/THS.2011.6107841

[18] Mahayam, P. and Shachdera, A. (2013) A Study of Algorithms AES, DES and RSA for Security. *Global Journal of Computer Science and Technology*, *Web and Security*, **13**, 140.

[19] Ashioba, N.C. and Yoro, R.E. (2014) RSA Cryptosystem Using Object Oriental Modeling Technique. *International Journal of Information and Communication Technology Research*, **4**, 57-61.

[20] King, D.A. (2001) The Ciphers of the Monks—A Forgotten Number Notation of the Middle Ages. Frdriz Steiner, Stuttgart.

[21] Ibrahim, A. (1991) Cryptography and Data Security: Cryptographic Properties of Arabic. *Proceeding of the third Saudi Engineering Conference*, Riyadh, 24-27 November 1991, Vol. 2, 910-921.

[22] Huurdeman, A.A. (2003) The Worldwide History of Telecommunications. John Wiley & Sons, Hoboken, 529. https://doi.org/10.1002/0471722243

[23] Sauter, M. (2014) From GSM to LTE-Advanced: An Introduction to Mobile Networks and Mobile Broadband. Second Edition, John Wiley & Sons, Hoboken.

[24] Owano, N. (2011) GSM Phones—Call Them Unsafe: Says Security Expert.

[25] NGMAST (2008) Solutions to the GSM Security Weakness. *Proceedings of the* 2*nd IEEE International Conference on Next Generation Mobile Applications*, *Services*, *and Technologies*, Cardiff, September 2008, 576-581.