International Journal of Electronics Communication and Computer Engineering
Volume 12, Issue 6, ISSN (Online): 2249–071X

Applications of End-to-End Encrypted Short Message Service (SMS) using Hybrid Encryption Algorithm

Victor Chibunna Enyinnaya[1*], Emmanuel Nwabueze Ekwonwune[2], Oliver E. Osuagwu[3], Alphonsus Onyekachi Agbakuru[4] and Bethran Chibuike Amanze[5]

[1]Department of Computer Science, Abia State College of Health Sciences and Management Technology, Aba, Abia State, Nigeria.
[2]Department of Computer Science, Imo State University, Owerri, Nigeria.
[3]Department of Computer Science, Imo State University, Owerri, Nigeria.
[4]Department of Computer Science, Imo State University, Owerri, Nigeria.
[5]Department of Computer Science, Imo State University, Owerri, Nigeria.
*Corresponding author email id: enyinnayachibunnavictor@gmail.com

Date of publication (dd/mm/yyyy): 15/12/2021

***Abstract* – This research focuses on applications of end-to-end encrypted Short Message Service (SMS) using hybrid encryption algorithm. In end-to-end encrypted short message service (SMS), messages are encrypted as the message or data travel between devices. The unreadable message can only be decrypted with a secret key on the recipient's device. Hybrid encryption is a mode of encryption that merges two or more encryption system. The research methodologies used are Structured System Analysis and Design Methodology (SSADM) and Object Oriented Analysis and Design Methodology (OOADM). With the help of the two techniques-Rivest-Shamir Adleman (RSA) and Data Encryption Standard (DES) Algorithm employed; integrity, confidentiality, authentication and security of messages were achieved. The software was developed using Java programming language.**

***Keywords* – Authentication, Encryption, Hybrid, Integrity, Security, Short Message Service (SMS).**

I. INTRODUCTION

Short message service (SMS) is a text messaging service component of most telephone, internet and mobile device systems. It is a mobile phone application that allows digital phone users to receive text message on their digital phones [1]. 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. An intermediary service can facilitate a text – to – voice conversion to be sent to landlines. 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 [2]. The benefits of SMS to subscriber center on convenience, flexibility and seamless integration of messaging services and data access provided by mobile platforms. These benefits depends on the application the service provider offers. The advancement of mobile technology has revolutionized the way peoples use mobile devices in their day to day activities [3]. 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. The first SMS message was sent in 1992 [4]. SMS is also employed in mobile marketing a type of direct marketing [5]. According to one market research report as of 2014 the global SMS messaging business was estimated to be worth over $100 billion, accounting for almost 50 percent of all the revenue generated by mobile messaging.

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 transf-

-orm information to make it unreadable for unauthorized users.

Encryption is 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 [6].

Encryption algorithms assist in the process of transforming plain text into encrypted text, and then back to plain text for the purpose of securing electronic data when it is transported over networks. By coding or encrypting data, hackers or other unauthorized users are generally unable to access such information. Some encryption algorithms are considered faster than others, but as long as algorithm developers, many of whom have math backgrounds, stay on top of advancements in this technology, this type of encryption should continue to flourish as hackers continue to be more sophisticated [7].

Decryption is the process of transforming data that has been rendered unreadable through encryption back to its unencrypted form. In decryption, the system extracts and converts the garbled data and transforms it to texts and images that are easily understandable not only by the reader but also by the system. Decryption may be accomplished manually or automatically. It may also be performed with a set of keys or passwords [8].

One of the foremost reasons for implementing an encryption-decryption system is privacy. As information travels over the communication channel, it becomes subject to scrutiny and access from unauthorized individuals or organizations. As a result, data is encrypted to reduce data loss and theft. Some of the common items that are encrypted include email messages, text files, images, user data and directories. The person in charge of decryption receives a prompt or window in which a password may be entered to access encrypted information [7, 8].

II. Review of Empirical Literature

Literature related to this research work are gotten from internet search of published journals on security, Short Message Service, encryption and mobile technologies which was based on the works that are related to the research scope.

Proposed an algorithm to send message through GSM using an asymmetric Rivest, Shamir and Adleman (RSA) cipher [9]. This application prevents tapping and substituting techniques to secure SMS. It is achieved by storing the public key in a certificate which can be signed by the certification authority.

Developed an application on Android platform which allows the user to encrypt the messages before it is transmitted over the network [10]. In this paper, Advanced Encryption Standards algorithm for encryption and decryption of the data was used. The application can run on any device which works on Android platform. This application provides a secure, fast, and strong encryption of the data. However, messages encrypted by the developed application are not resistant to Brute-Force and pattern attacks.

Proposed accost effective scheme which uses a concept called Cheating Text [11]. The original message is e-

-mbedded 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.

Carried out a study on enhancing the security of DES, Blowfish, AES algorithm using transposition cryptography techniques [12]. 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.

III. METHODOLOGIES

The methodologies employed in this research are the Structured System Analysis and Design Methodology (SSADM) and Object Oriented Analysis and Design Methodology (OOADM). In Structured System Analysis and Design Methodology, problems were identified, a feasibility study was undertaken, the present system was analyzed and the proposed system designed based on the problems identified in the present system. The program was coded and tested and the system was implemented. In Object Oriented Analysis and Design Methodology, the researcher used data flow diagram, Use case diagrams, Class diagram etc to represents the system.

IV. CONTROL CENTRE (MAIN MENU)

Control centre is the engine of the software. It comprises of the House keeping, sending security details, get report and exit. The House keeping is made up of; Edit, Delete and Exit while the Sending security details is made of Send, Received and Feedback.

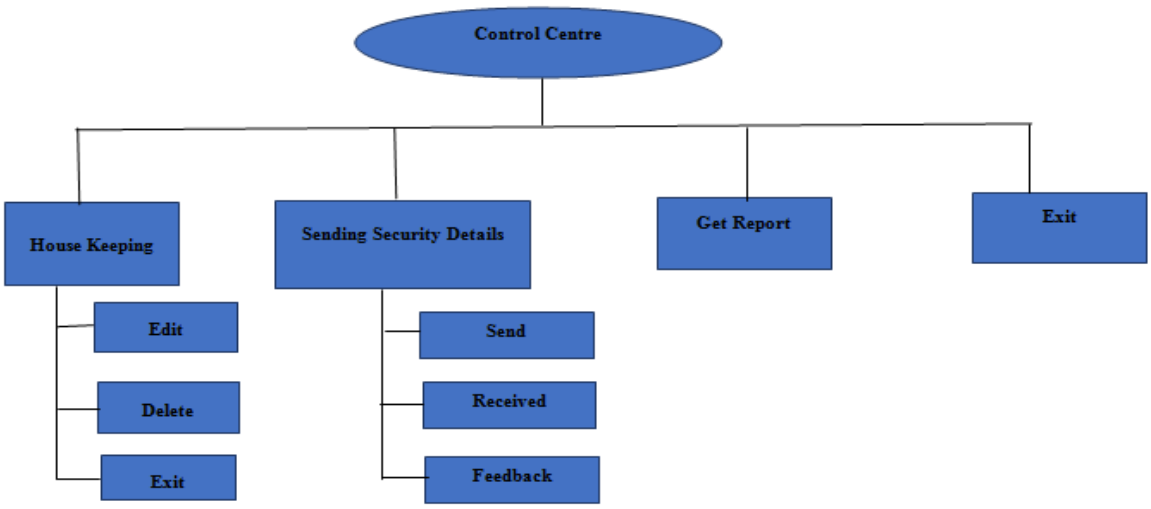

Fig. 1. Control Centre.

V. RESULT AND DISCUSSION

The application was tested at close range and wider range using two android phones to ascertain the communicability of short message service across platform. It was observed that message passes through encryption process which encrypts the message using public key and produce a cipher text to be transmitted. The cipher text is passed through the decryption process which decrypts the cipher text using private key. However, result also showed that transmission of short message service relies on availiability of wireless network service by the network providers. Furthermore, messages sent without service or network will be

delivered even if the receipient device is switched off, it will be stored in the network and later delivered immediately the receipient device is avaliable. Finally, Data Encryption Standard (DES) algorithm helps to achieve integrity of the message while Rivest Shamir Adleman (RSA) helps to achieve authentication, confidentiality and security of messages.

VI. SAMPLE OUTPUT

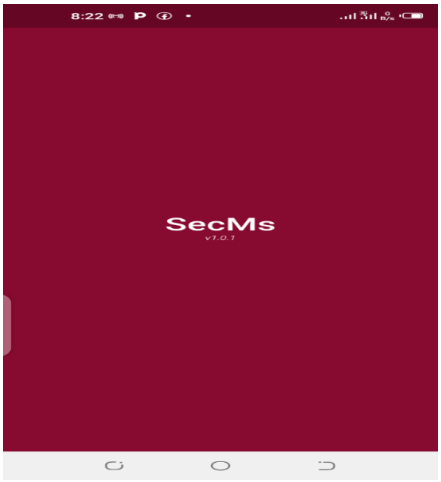

Fig. 2. Shows the Splash Screen of SecMS App.

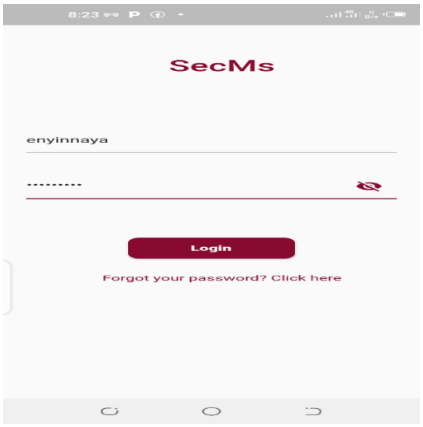

Fig. 3. Shows the Login Screen.

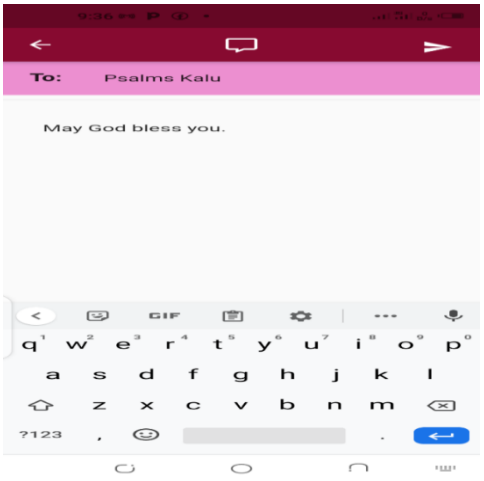

Fig. 4. Shows compose message Interface.

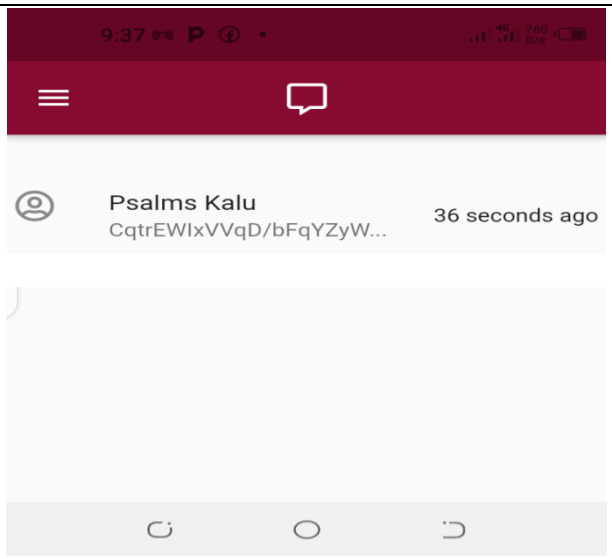

Fig. 5. Shows encrypted message after been sent.

VII. Applications Areas

Having carried out this research work, it is important to note that End-to-End Encrypted Short Message Service (SMS) app using Hybrid Encryption Algorithm can be apply in the following areas:

- *Banking Sector*

Since transmission of SMS is not secure in the network using global system for mobile communications or general packet radio service, the Secret Message *(SecMs)* app developed in this research work will address or arrest security threats observed in the use SMS in Mobile banking and Mobile payments. Also bankers can also use this *SecMs* app to send end of month account statement to their customers.

- *Health Sector*

The *SecMs* app developed in this research work will go a long way in providing a high level security and privacy of patient information. It will also create room for SMS messages interactions between health care professionals and patient using mobile phones. Doctors can use the app to securely communicate critical information to their nurses, midwives and other medical personnel's without exposing the secrecy within the medical profession and without others understanding the SMS.

- *Department of Defense Agencies*

The *SecMs* app developed in this research work will provide private communication with utmost secure communication and collaboration tools for department of Defense Agencies via-Army, Air force, Navy etc.

VIII. Conclusion

The applications of end-to-end encrypted short message service using hybrid encryption algorithm has been stated, the software is developed using Java programming language. The software developed can be applied in Banking Sector, Health Sector, Department of Defense Agencies and Companies. With the help of the two techniques – Rivest-Shamir Adleman (RSA) and Data Encryption Standard (DES) Algorithm employed; integrity, confidentiality, authentication and security of messages were achieved.

REFERENCES

[1] N.G. Loon, Short Message Service (SMS) Security Solution for Mobile Devices. Master's Thesis, Naval Postgraduate School, Monterey, 2016.
[2] M. Sauter, From GSM to LTE-Advanced: An Introduction to Mobile Net-works and Mobile Broadband. Second Edition, John Wiley & Sons, Hoboken, 2014.
[3] A.M. Sagheer, A.A. Abdulhameed, and M.A. Abduljabbar, SMS Security for Smartphone. 6th International Conference on Developments in eSystems Engineering, Abu Dhabi, 16-18 December 2013, 32-35. https://doi.org/10.1109/DeSE.2013.57 . 2013.
[4] S. Neetesh, and S.C Narendra "EasySMS: A Protocol for End-to-End Secure Transmission of SMS", *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 7, July 2014.
[5] K. Black, What Is SMS Marketing? WiseGEEK. 2016
[6] A. Monika, "A Comparative Survey on Symmetric Key Encryption Techniques", *International Journal on Computer Science and Engineering (IJCSE)*, vol. 4, no. 05, May 2012.
[7] A.K. Najib , A. Turki, and A. Khalid, *Performance Evaluation of Three Encryption/Decryption Algorithms IEEE*, 2010.
[8] L. David, . and D. Martin, SMS Encryption for Mobile Communication, IEEE International Conference on Security Technology, 2019.
[9] David Lisoněk and Martin Drahanský, SMS Encryption for Mobile Communication, IEEE International Conference on Security Technology, 2013, 198 – 2011.
[10] Rohan Rayariker, Sanket Upadhyay, Priyanka Pimpale "SMS Encryption using AES Algorithm on Android", International Journal of Computer Applications. 2012, Volume 50 No.19.
[11] Rupa, Ch. and Avadhani, P.S. Message Encryption Scheme Using Cheating Text. 6th International Conference on Information Technology: New Generations, Las Vegas, 27-29 April 2009, 470-474. https://doi.org/10.1109/ITNG.2009.232
[12] Singh, S., Maakar, S.K. and Kumar, D.S. Enhancing the Security of DES Al-gorithm Using Transposition Cryptography Techniques. International Journal of Advanced Research in Computer Science and Software Engineering, 2013, 464-471.

AUTHOR'S PROFILE

First Author
Mr. Enyinnaya, Chibunna Victor, holds a Bachelor of Science (B.Sc Second Class Upper Division) in Computer Science, Master of Science (M.Sc) in Information Technology and currently at the verge of finishing his Doctorate Degree (Ph.D) in Computer Science (Cyber Security), Imo State University, Owerri, Nigeria. He has been teaching Computer Science since 2012 and had published in a variety of local and international journals. He is a member of International Association of Computer Science and information Technology (IACSIT), Nigeria Computer Society (NCS) and Computer Professionals (Registration Council) of Nigeria (CPN).

Second Author
Emmanuel Nwabueze Ekwonwune, Department of Computer Science, Imo State University, Owerri, Nigeria.

Third Author
Oliver E. Osuagwu, Department of Computer Science, Imo State University, Owerri, Nigeria.

Forth Author
Alphonsus Onyekachi Agbakuru, Department of Computer Science, Imo State University, Owerri, Nigeria.

Fifth Author
Bethran Chibuike Amanze, Department of Computer Science, Imo State University, Owerri, Nigeria.