ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 6, Issue 2, pp: (67-75), Month: April - June 2018, Available at: www.researchpublish.com

Mobile SMS Application Security: Problems, Prospects and Mitigating Techniques

[1]Chike David N., [2]Prof. Gloria Chukwudebe A., [3]Dr.Emma Ekwonwunne

[1]Imo State University, Owerri
[2]Federal University, Owerri
[3]Imo State University, Owerri

Abstract: **Mobile technologies are everywhere these days from home to large enterprise corporate networks due to the portability and flexibility of use, user's convenience, avoidance of wiring cost and constant mobility support. However, the greater availability of mobile phone and proliferation of its application means increased danger of attacks and increased challenges to all concerned users, manufacturers and mobile software developers, and IT security professionals. This paper discusses the various security issues and vulnerabilities related to the Mobile Technology with emphasis on Mobile Smartphone SMS and proffer encryption standard apps design as possible mitigating techniques/ measures against common threats/attacks. This also identified the some user's attitude that subjects them to attacks. Finally, it provided an SMS app with overall guidelines and recommendation to users.The methodology used is survey of literature on related works as it relates to mobile SMS and artifact design of an encryption software application useful for securing mobile SMS messages in an android operating system. The research artifact was tested on android phone using two compatible phones engaged in sending and receiving of SMS messages using symmetric encryption "Advanced Encryption Standard) with earlier agreed secret keys between the sender and the receiver and the result showed a successful concealed SMS communication between the platforms that required decryption key to read.**

Keywords: **Mobile, Technologies, Applications, Vulnerabilities, Security, SMS, Mitigation.**

1. INTRODUCTION

The earth is now under a newest revolution of mobile communication and is gradually rushing into another level of communication arena, where machines can talk to machines without human interference. Mobile smart phones have become a common mobility tool of the time, which houses flexible applications like Short Message Services (SMS), Multimedia Service (MMS) and voice/voice mail service (VMS). Mobile Technology Applications are proliferating to the extent of replacing conventional desktop applications [1]. Today the bulk of our technology applications have gone electronics ('E's), due to deployment of and Mobile Wireless Technologies. The convenience of using mobile device like phones have created a new shift in portability of documents files. Nowadays, it is common for subscribers to store their financial details, personal reminders, special days and times, wedding and anniversaries without thoughtful thinking of vulnerabilities and security breaches [32]. Mobile Wireless Devices (MWDs) interfacing and communicating in multi-protocol signal directions have made mobile devices accessible from several radio platforms making security issue of multiple- devices and multiple techniques considerations [1,6].

Users are battling with control of their respective cells, protection of their data within the cells, protection of physical devices used for signal receptions. More user attacks are recorded on daily basis, and this shows increase in user's vulnerabilities, cases of financial fraud [4, 7, 6] and other related crime on ignorant or incompetent users of the technology is on the increase. Personal Information and Databases are now synced into mobile devices without consideration of theft, loss or damage of the mobile device cum other attendant risk of hijacking or sniffing personal files from it for potential attack on the user [9,7].

The voice calls, the Short message services (SMS), the Multimedia Services (MMS), the Radio Frequency Identifications (RFIDs), the sensor interactivities are all offshoot of Mobile Technology [20]. The risk factor associated with these technologies borders on Security, which also posses as a major challenge faced by the mobile Smartphone manufacturers and users. This security risk affects three major parties namely the manufacturer (Device maker), the Software App makers and the end-users or device owner [19,9].

Security issues as it relates to mobile technologies applications consider the problems in relation to users on technicalities of the system and proffers approaches to mitigating the problems on evaluation of the techniques deployed. This research work was motivated by increasing growth in the mobile sector and its deployment speed on to virtually every activities of man that was once formerly done on a desktop. Because, there is big prospect for continuous Mobile Technology Applications growth and use, propelled by wireless and portable platform that gives convenience and flexibility than desktop applications then security issues must reoccur from time to time.

1.1 Background of Study:

Mobile Technologies Application is a geometrically growing system, a revolutionary trend of our time. With increase in mobile handheld devices subscription in 2006 and continuous unprecedented growth on daily basis, the system has challenged and surpassed the growth of Industrial Revolution. One attendant problem that still faces the creators and users of these common devices is security of the *Container* (the mobile device) and the *Content* (the data file) and the *Software apps and Operating system*. The container is a major concern of the manufacturers, the content major headache of the end users, while attackers are so much interested in vulnerable holes within the software apps to exploit for attacks physically or remotely.

The protocols of mobile communication systems are built in a way to provide protective security for the device and its channels of communication, without due considerations to the end users safety. Protective strategy for the device includes encryption securities, which ensures that the message got delivered to the recipient irrespective of distance and location without trace or compromise.

1.2 Statement of Problem:

There is no-gainsaying that we are living in a safe world with advent of handheld devices (mobile devices) because the challenges facing mankind has gradually increased day by day with additional mobile devices introduction, protocols multiplicities and vulnerable platforms that exposes us to unforeseen dangers. Mobility is good by its application is a problems to mankind. But in the long run, man has remain unsecured, unsafe and exposed to more risk of attack by his own activities while online or on the move. The problems remain how we can secure ourselves.

i. How can we protect possible snooping and interception on GSM communications?

ii. How can we Protect unauthorized traffic interception by unauthorized masqueraders.

iii. How can we develop and deploy an end-to-end encryption application for the SMS mobile technology application.

1.3 Aim and Objectives:

The aim of this work is firstly to design a Short Message Service (SMS) encryption application that can conceal the message, while on transit to another mobile device using Advanced Encryption Standard (AES) algorithm on android operating system and implement it for security of mobile SMS. The other objectives that will be achieved in line with this work are isolation of several security risks associated with Mobile Technologies Applications with a view to identify the problems and highlight prospective approaches to mitigating the identified risks and to proffer relevant techniques/ solutions for using mobile devices as to avert possible mobile problems and attacks of any kind.

2. LITERATURE REVIEW AND RELATED WORKS

Both security and wireless communication will remain an interesting subject for years to come [1]. Security in computer world determines the ability of the system to manage, protect and distribute sensitive information [1,2]. Every security system must provide a bundle of security functions that can assure the secrecy of the system and these functions are the goals of security system. According to [30] categorical goals of security are subdivided into five main subheadings: Authentication, which means that before sending and receiving data, the receiver and the sender identity should be verified; Secrecy or Confidentiality, which implies how most people identify a secure system; Integrity, that means

content of the communication data is assured to be free from any type of modification between the end points; Non-Repudiation, that implies neither the sender nor the receiver can falsely deny they have sent a certain message and Service Reliability and Availability, that entails granting the users the quality of service they expected[12, 13].

Short Message service is a mobile phone application that allows digital phone users to receive text messages on their digital phones [5]. Each message may be a maximum of 160 characters long. SMS messages are supported by GSM, TDMA and CDMA based mobile phone networks currently in use today [2]. The benefits of SMS to subscribers center on convenience, flexibility and seamless integration of messaging services and data access provided by mobile platforms. These benefits depends on the applications the service providers offers. The advancement of mobile technology has revolutionalized the way people use mobile devices in their day to day activities [3,2]; while mobile computing offers a computing environment over physical mobility, it means the users will be able to access data, information or other logical objects from any device in any network while on the move [3].

There are some security shortcomings identified in GSM such include no possibility of encrypting International Mobile Subscribers Number (IMSI) with A5, recall that unless the IMSI is transmitted in plaintext a subscriber is rejected[3,4]. Security has significant consequences or difference considering theoretical and effective security technique applied. In theory smart cards and PKI for authentication are always proffered, but these measures are so painful to deploy and use that they are almost never employed [4]. Security experts tend to focus exclusively on the measures that provide the best (theoretical) security, but often these measures provide very little effective security because they end up being misused, turned off or bypassed. Worst still when they focus only in the theoretically perfect measures they do not even try to get lesser security measures right [4]. Attackers are always smarter in exploiting the non-implementation of lesser security measures to achieve mobile phone attacks like traffic analysis, passive eavesdropping, active eavesdropping, unauthorized access, man in the middle attacks, session high-jacking, replay attacks, rough AP, flooding attacks and Denial of service (DoS) attack[1, 3, 6]. Today mobile wireless market is increasing by leaps and bounds and the success of mobile lies in the ability to provide high speed data services to the mobile users as well as secured platform. A mobile device plays a key role in the realization of payment as mobile phone is used by payer in one or more steps during banking or financial transactions [3] so the vulnerabilities posses potential risk or attack surface to the users.

Mobile phone SMS application is preferred by many because it has the following service oriented characteristics and applicability's:- Alert SC, Retry Schedules, Concatenation, Message duplications, priority messaging, short code messaging, smart cards, man-machine interfaces, roaming, viruses [13], Spam, malicious emergency short messaging, charging, fixed network connectivity capabilities, prepaid mobile phone billing, performance evaluations and location tracking[5]. Security breaches often occur more easily by concentrating on people rather than on technology and SMS technology is not truly a secure environment application [7], which informs the need for an end-to-end encryption in order to provide a secured medium of communication [8].

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 [9]. In [10] 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 [7, 8, 10]. A study by [14] on encryption 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 [13,12,14]. Deploying AES with object oriented modeling techniques yields a better SMS encryption app on android O/S[15]. Because AES require very low RAM space and is very fast [16], our research design adopted AES for the demonstration application development and it result proved a very successful project.

AES is a symmetric encryption algorithm [18] that allows the sender and receiver to agree on key exchange medium for transmission with single key for encryption and decryption of the messages before transmission process [17].

In recent years network security has become an important issue [18], because data which is to be transmitted from sender to receiver in network must be encrypted using encryption algorithms in cryptography [20,6]. Mobile Technology Applications are numerous these days, with Short Message Service (SMS) and Multimedia services (MMS) as the two most common. While voice calls can be interrupted and snooped on, mobile SMS can be intercepted or fabricated to the detriment of the users of such applications. Consequent upon that [23] opine that hacking mobile network via Signaling System No 7(SS7) allows interception, shadowing and thus has become the bad guys platform for tracking mobile

phones, inflicting Denial of service (DoS), interception and even a threat to Internet of Things (IoT) and financial transactions[24]. Against this backdrop, [1, 23] suggested an encryption and decryption algorithm as solution to use on the protocol to ensure confidentiality, integrity and non-repudiation of messages. Encryption is the process of transforming information (referred to as plaintext) using an algorithm (called cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key [29,1]. Tracking is a violation of personal data protection laws and have proved hard to stop Any Time Interrogation, provide subscribers information and location. For some radio signal interceptors are used when subscribers are nearby. An advanced Encryption Standard (AES) algorithm is not

only for security, but also for speed with hardware and software faster implementations [20]. AES is a symmetric encryption standard, which entails use of one key to encrypt and decrypt data[20], a techniques used to secure the SMS transmitted over mobile network via an end-to-end encryption application (Mobicrypt). [7,6,5]. Advanced Encryption Standard algorithm plays very important role in communication security and its decryption patterns is better than other algorithms.

Computer security also known as cyber security or IT security is the protection of information systems from theft or damage to the hardware, the software and to the information on them, as well as from disruption or misdirection of the services they provide [30]. It includes controlling physical access to the hardware, as well as protecting against harm that may come via network access, data and code injection, [6,3,18] and due to malpractice by operators, whether intentional, accidental, or due to them being tricked into deviating from secure procedures. Computer security covers all the processes and mechanisms by which digital equipment, information and services are protected from unintended or unauthorized access, change or destruction and the process of applying security measures to ensure confidentiality, integrity, and availability of data both in transit and at rest [19]. Security counter measures help ensure the confidentiality, availability, and integrity of information systems by preventing or mitigating asset losses from Cyber security attacks [31]. Sometimes, they arises a security issue for an unauthorized access to the message, hence a secured communication protocol is needed which can provide an authentication and integrity protection [32] in a wireless network like that of mobile.

Mobile Technology Applications is a sub branch of Wireless Technology. Mobile Technology in general is any technology of mobility such technology as in cars, industry, notebooks, PDAs and cellular phones [21]. According to Oxford Dictionary of Computing “Mobile Computing generally is any application in which the computing system used in not assigned a specific location. Technology is used in a specific as the communication technology using unguided media transmission such as radio wave, microwave, infra-red and Bluetooth so one can transfer any type of data with mobile technology such as voice, video and text etc [21, 34].

Mobile application stem from Wireless Network Connectivity (WNC). Wireless communication is the exchange of data between two or more points that are not joined by an electrical transmitter. The most well known wireless technologies are electromagnetic wireless communications for instance radio; television etc. with radio waves distances as short as TV Remote Control or to the extent of thousand or even huge number of kilometers from profound space radio communications. It includes different sorts of Fixed, Mobile and Portable applications including two-way radios, cell phones, individual PDAs and wireless networking [36].

According to the latest statistics released by the International Telecommunication Union (ITU) in 2013, the number of mobile subscribers has reached 6.8 billion worldwide. Meanwhile it has been reported in that an increasing number of wireless devices are abused for illicit cyber-criminal activities including malicious attacks, computer hacking, data forging, financial information theft, online bullying/stalking and so on[10]. Hence it is paramount to improve wireless communication security to fight against cyber-criminal activities, especially because more and more people are using wireless networks (e.g. Smartphone and Wi-Fi) for online banking, personal emails, owing to the widespread use of same. The study in [7] shows that mobile device security has become more critical as businesses have began to rely on these devices for everyday processes. Nonetheless, the security for these devices has been established as nonexistent. This ITU study showed that on average, only 10% of the approximately 86 million devices in use today are secured [5]. Looking at security [6] affirms that security as a counter measure helps ensure the confidentiality, availability and integrity of information systems by preventing or militating against asset losses from cyber security attacks. With Smartphone development, social media connectivity and cloud computing a whole new sets of security problems that required new regulations and new thinking has emerged [12].

According to [11] mobile phones share many of the vulnerabilities of PCs, the attributes of easy to carry, use and modify open then to a range of attacks because many seemingly legitimate software apps are malicious, even the legitimate Smartphone software can be exploited. Phishing attack use electronic communication to trick users into installing malicious software or even give away sensitive information. In addition, [11] suggested the following as mitigating measures for users:

i. When choosing mobile phone, users/subscribers should consider its security features by asking the service providers, if the device offers file encryption, ability to find and wipe devices remotely, and ability to delete known malicious apps remotely.

ii. Subscribers should configure the device to be secured by enabling the password features with complex password and encryption, remote wipe capabilities and antivirus activation.

iii. Users should configure web or social media accounts to use secure connections and ensure to set accounts to use secured, encrypted connections because enabling these features deters attackers from eavesdropping on the web session.

iv. User should avoid links sent in suspicious email or SMS messages because it may lead to malicious sites of attackers.

v. Subscribers should limit exposure to mobile phone number and think before posting mobile phone number to a public website as attackers often use software to collect mobile phone numbers from web and then use them to target attacks.

vi. Subscribers should selectively consider what information to store on the device, because with enough time and sophisticated software access to the device, any attacker could obtain stored information from the device physically or remotely.

vii. Users should be selective in apps download / installation, but should always do a little research on apps to check what permissions it requires before installing them, when permission seem beyond what the app should require, it should be avoided.

viii. Subscribers should maintain physical control of their device especially in public or semi-public place to avoid theft or loss.

ix. Users should always set Bluetooth-enabled devices to non-discoverable as to prevent them from being visible to nearby devices which can alert an attacker or expose them to compromise.

x. Users should avoid joining unknown Wi-Fi networks or using public Wi-Fi hotspots as attackers sometimes create phony dedicated Wi-Fi hotspots designed to attack mobile phones.

xi. When possible users should delete all information stored in a device prior to discarding it to avoid traces to previous files once manipulated on the device.

xii. Finally users should be careful using social networking applications, because these apps may reveal more personal information than intended to unintended parties and also be careful when using services that track locations or power on GPS services unknowingly.

The techniques proffered for mobile security issues include according to [8] implementation of the three mobile security capabilities to address the challenges, it infers that current mobile devices lack the hardware-based Roots of trust (RoT) that are increasingly built into laptops and other types of hosts. Unfortunately, many mobile devices are not capable of providing strong security assurances to end users and organizations. But a hardware technique necessary for achieving safe mobile device is the use of hardware root of trust (RoT) applicable in laptops and other host devices [8].

Meanwhile, Mobile devices are also vulnerable to “jailbreaking” and “rooting,” which provide device owners with greater flexibility and control over the devices, but also bypass important security features which may introduce new vulnerabilities. Security components are foundational elements that can be leveraged by the device, the operating system (OS), and applications. The three required security components are *Roots of Trust (RoTs)*, an *Application Programming Interface (API)* to expose the RoTs to the platform, and a *Policy Enforcement Engine (PEnE)*[8].

Root of Trust (RoT) is categorically security primitives composed of hardware, firmware and/or software that provide a set of trusted, security-critical functions. Hardware RoTs are preferred over software RoTs due to their immutability, smaller attack surface, and more reliable behavior. To support device integrity, isolation, and protected storage, devices should implement the following RoTs [8]

- Root of Trust for Storage (RTS)- provides a protected repository and a protected interface to store and manage keying material.
- **Root of Trust for Verification (RTV)-** provides a protected engine and interface to verify digital signatures associated with software/firmware and create assertions based on the results.
- **Root of Trust for Integrity (RTI)-** provides protected storage, integrity protection, and a protected interface to store and manage assertions.
- **Root of Trust for Reporting (RTR)-** provides a protected environment and interface to manage identities and sign assertions.
- **Root of Trust for Measurement (RTM)-** provides measurement used by assertions protected via the RTI and attested to with the RTR.

Consequently, application of RoT ensures the device integrity, which is the absence of corruption in the hardware, firmware and software of a device. A mobile device can provide evidence that it has maintained device integrity, when the software, firmware and hardware configurations can be shown to be in a state that is trusted by a relying party [8]. In the same vein, *isolation* and *Policy Enforcement Engine (PEnE)* contributes to the reliability on the hardware (mobile device). While Isolation prevents unintended interaction between applications and information contexts on the same device and PEnE enables the processing, maintenance, and management of policies on the mobile device. The PEnE allows Information Owners to express the control they require over their information; thus it translates the desired requirements for storing and sharing their information into the appropriate device and network configurations and policy [8].

For software issues ultimately cryptographic encryption of applications should be the approach to several challenges faced by software vendors. Encryption according to [1, 5] is the concealment of data using a set of keys necessary for securing the message and rendering it meaningless to the attacker or unintended recipient, while at the same time rendering it meaningful to the intended recipient via the decryption process by deployment of the known key.

3. METHODOLOGY

The design of the secured SMS application named Mobicrypt, involves the design of external and internal components of the app on android operating system, open source software). The internal architecture depicts the internal communication diagram of the app, while the external architecture shows the physical framework of the app on an android mobile device. The methodology adopted for this work is a literature survey of the different security scholarly works and the literature extracted from the thesis presented on Development of security system for SMS encryption. The main goal was the design and implementation of the app on a real life device and deployment of software testing paradigm in ensuring its successful use. However, this work proved helpful in the study of categories of mobile parties: Users (device owners), the Manufacturers (Makers) and Service or Application Service providers. Secondary source was used for gathering the relevant literatures from internet search of published Journals on security and mobile technologies. Analysis was quantitative as no calculation was necessary in this work. Graphical representations were Mobicrypt Interface design used to showcase the app for clarity of issues and concepts.

4. CONCLUSION

The research has shown that mobile SMS technology is a porous one that does not guarantee security of data and files due to its mobile nature and architectural framework. Securing the wireless network and mobile hi-tech devices is an ongoing process. Realistically, there is no single true security measure in place. When a new technology is first introduced, attackers and hackers study the protocol, look for vulnerabilities and then cobble together some program and scripts to try to exploit those vulnerabilities. Overtime those tools become more focused, more automated and readily available and

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 6, Issue 2, pp: (67-75), Month: April - June 2018, Available at: www.researchpublish.com

published on the open source network. Hence, they can be easily downloaded and run by anyone. So, we can never eliminate all threats and vulnerabilities and even if we do, we will probably end up wasting money by defeating some low probability and low impact attack. On the other hand, if we start eliminating the biggest security loopholes, attackers may turn to easier targets. So therefore using encryption app can ameliorate problems of mobile security.

The following modules in fig 1.1 below shows the Mobicrypt SMS App Interface developed and deployed in mitigation of the challenges raised including careful guideline reeled out for handling of mobile devices like deployment of multiple security strategies such as encryption and password. Finally It is our recommended that for all mobile phone users should for the seek of SMS communications security use Mobicrypt App.

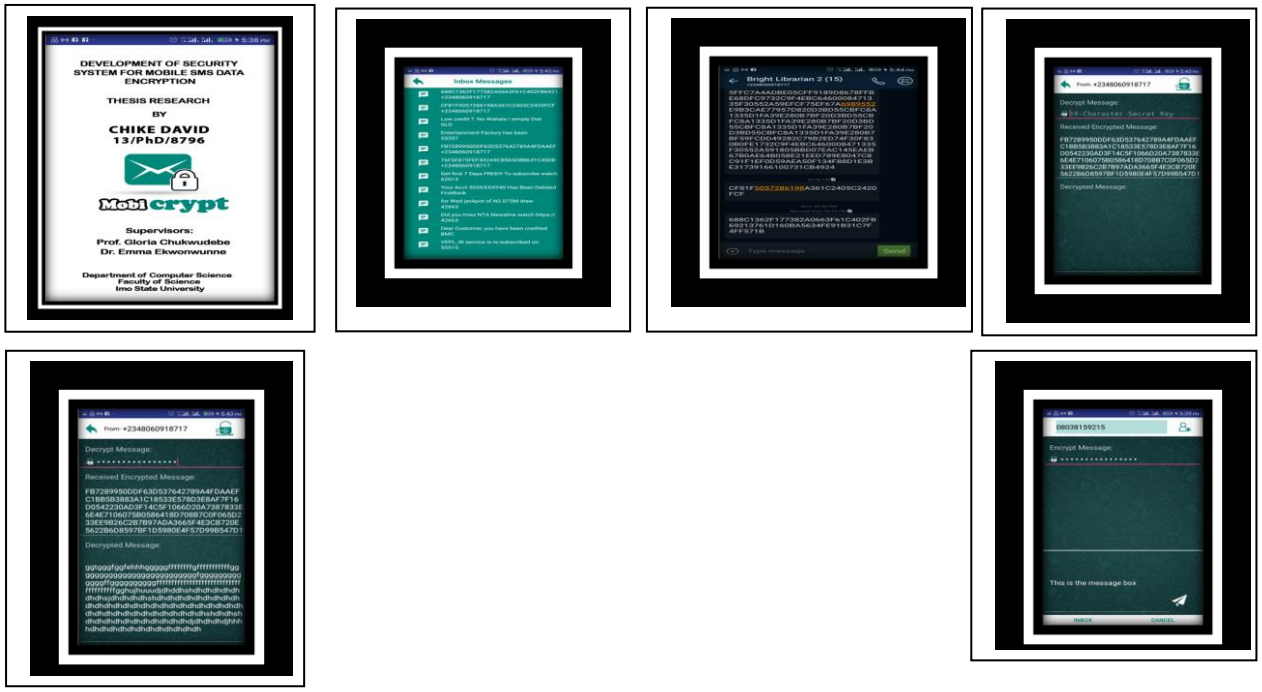

Fig 1.1 Mobicrypt Application Interfaces

REFERENCES

[1] Adel-Karim R.AI (2016) Security in Wireless Data Networks: A survey paper.

[2] California Software Laboratories Software development service section.

[3] Krishna Prakash et al (2015), Security issues & challenges in mobile computing & M. commerce, International journal of computer science & engineering survey (IJCSES) vol. 6.NO.2 APRIL 2015.

[4] Peter Gutmann (2014) Engineering Security, Book Draft, April 2014

[5] ETSI(2006) Analysis of the Short Message Service (SMS) and call Broadcast Service (CBS) for Emergency Messaging Application; Emergency Messaging; SMS and CBS.

[6] UmeshKumar and Sapna Gambhil (2004) A Literature Review of Security Threats to Wireless Networks, International Journal of Future Generation Communication and Networking Vol.7, No.4 pp 25-34.

[7] Sharad K.V. and D.B.Ojha(2014) An Approach to Enhance the Mobile SMS Security, Journal of Global Research in Computer Science. Volume 5, No.5 May, 2014.

[8] B. Nithya and P. Sripriya(2016) Comparative Analysis of Symmetric Cryptographic Algorithms on. NET Platform. Indian Journal of Science and Technology Vol.9 (27), DOI: 10.17485.

[9] Manisha M, Kavyashree C.V. et al (2012) Cryptography on Android Message Application Using Look Up Table and Dynamic Key (CAMA). IOSR Journal of Computer Engineering.

[10] Shaza D.R, Ahmed K, et al(2015) A Performance Comparison of Encryption Algorithms AES and DES. International Journal of Engineering Research and Technology, Vol.4, Issue 12.

[11] Chao W. Chang, Heng Pan et al(2008) A Secure Short Message Communication Protocol. International Journal of Information and Computing.

[12] Rufai Y. Zakari and Najib Abdulrazan (2016) Computer Security: A Literature Review and Classification. International Journal of Computer Science and Control Engineering, Vol.4, No.2, 2016 pp 6-13.

[13] K. Suresh Babu and Alraddadl F. Saleems (2013) SMS Encryption for Mobile Communication. International Journal of Scientific Engineering and Technology Research, Vol.02, Issue 17.

[14] P. Mahayam and Abhishek Shachdera (2013) A Study of Encryption Algorithms AES, DES and RSA for Security, Global Journal of Computer Science and Technology, Web and Security, vol.13 Issue.15 version.

[15] N.C Ashioba and R.E Yoro (2014) RSA Cryptosystem using Object Oriented Modeling Technology, International Journal of Information and Communication Technology Research.Vol.4

[16] Rohan Rayariskar, et al(2012) SMS Encryption Using AES Algorithm on Android International Journal of computer Applications Vol.50.

[17] Nimmyer U. and Divjan K.V.(2015) Cipher SMS Protocol: A Secure SMS Transmission for Confidential Data.International Journal of Scientific Engineering and Applied Science (IJSEAS) . Vol.7

[18] Sri Rargaranjam, N. Sai Ram et al(2013) Securing SMS using Cryptography. International journal of computer science and Information Technology Vol.4 (2)

[19] Sandip Thitme and Vijay Kumar Verma (2016) A Recent Study of Various Encryption and Decryption Techniques. International Research Journal of Advanced Engineering and Science. Vol. 1,Issue 3,pp 92-94.

[20] www.answer.com/Q/what is mobile technology?# slide=2

[21] Oxford University Press (2008) Oxford Dictionary of Computing sixth edition London

[22] Yulong Z. Jia Z, Xianbin W, and Lajos Henso (2018) A Survey on Wireless Security: Technical Challenges, Recent Advances and Future Trends, Proceedings of IEEE.

[23] T.Blitz ‘ Decoding Mobile device security’. Security Vol.5 no 42, pp 46-47, 2005

[24] Atul M.T, Suraj S.K and Surbhi, R.C (2013) Cyber Security: Challenges for society –Literature Review .

[25] Cassandra Beyer (2014) Mobile Security: A Literature Review ….

[26] NIST (2013) Guidelines for Managing the security of Mobile Devices in the Enterprise, NIST Special publication.

[27] CIO(2012) Government use of Mobile Technology: Barriers, Opportunities and Gap Analysis, CIO council publication.

[28] Kaspersky (2012) Security Technologies for Mobile and BYOD, A whitepaper that assesses the security technologies. Forrester Research Inc.

[29] Paul Ruggiero and Jon Foote (2011) Cyber Threats to Mobile phones, US-CERT, Carnegie Mellon University, U.S.A

[30] Rajinda A, Deborah R, and Karen S (2014) Security and Privacy Issues Related to the Use of Mobile Health app, Australasian Conference on Information Systems.

[31] Hazam M.E, Ali E.T, and Ahmed H.A(2013) A New Mobile Application for Encrypting SMS/Multimedia Messages on Android, International Journal of scientific &Engineering Research, Vol.4 Issue 12 Dec, 2013.

[32] Marzie A, Kathy R, and Mussie T(2013) BYOD Issues and Strategies in Organizations: Issues in information systems vol. 14, Issue 2, pp 195-201, 2013

[33] Poonam M, Gauri P, Chetna S and Vishal P(2014) SMS Security for Android Mobile Using Combine Cryptographic Algorithms, International Journal of Advanced Research in computer and communication Engineering Vol.3, Issue 4 April 2014.

[34] TISN (2012) Mobile Device Security Information for IT Managers.

[35] D. ayetal Israeli, "the Linux kernel as a case study in software evolution," journal of system and software, pp. 485-501, 2011.

[36] Ahmed I. Sallam, E.-S.E.-R (2012, 6). Encryption- based multilevel model for DBMS. Computers & security, 31(4),437-446.

[37] Prerna Mahajan et al(2013) A Study of Encryption Algorithms AES, DES and RSA for Security. Global Journal of Computer Science and Technology Network, Web & Security Volume 13 Issue 15 Versions 1.0 Year 2013.