MODEL FOR CONFIDENTIAL DATA TRANSFER ONANDROID

*Adebayo, A. O., Ojo, F., Olayinka, Y., Uchendu, P.

*adebayoa@babcock.edu.ng
Department of Computer Science, School of Computing and Engineering Sciences, Babcock University

Abstract

Connectivity provides a means to communicate and learn. However, information in transit isexposed to abuse. Implementationof Advanced Encryption Standardalgorithm grossly reduces information confidentiality abuse, but it is unpopular for mobile devices. Android is a common Operating System for mobile devices. This study, therefore, focused on proposing a model, and prototype, for confidentiality secure data transfer by mobile devicesusing Android. The Waterfall system development life cycle model was adopted. The software development environment includes Android Studio, PHPMyAdmin and XAMPP packages. A model for secure data transfer on mobile device, which could be used as a guide for developing similar systems, was developed.An application for confidential data transfer for android, which smartphone users could use securely among themselves, was created.

Keywords: Key Distribution Centre, Encryption, Android,Security Model, Smartphone Security Software

1.0 INTRODUCTION

Business and social models, among others, have changed dramatically with connectivity, the Internet and several other technologies. The world has become a 'global village'. What is transmitted or exchanged is data or information. Data is the core asset of any information system,created to provide users with reliable information on which to base their decisions (Hardcastle, 2011). With various methods of information exchange comes a need for information security.All organizations, including government, private, and other institutions, must realize these problems, as loss of information can have undesirable impact on quality of services and operations management (Zukime, Mat, Abdullah, Mohd and Mohd, 2014).Information security refers to the mechanisms that protect information systems and ensure they operate, meeting or exceeding expectations.The truth is hundred percent information security cannot be guaranteed. However, it is much better to implement some security mechanisms than leaving systems purely exposed to threat(s) (Privacy Technical Assistance Center, 2011).

An effective approach in ensuring confidentiality of information, which is an aspect of information security, is cryptography and encryption. These are concepts which have been used successfully for thousands of years. Encryption is one specific element of cryptography in which information or data is obfuscated by transformationinto an undecipherable code or meaningless form. The Advanced Encryption Standard (AES) encryption algorithm had been proven reliable (TechTarget, 2014). AES has been adopted by the U.S government and is now been used worldwide. It was announced by the US National Institute of Standards and Technology (NIST) to be reliable (United States National Institute of Standards and Technology, 2001). AES is a symmetric key algorithm, which comes with a key management and distribution problem, especially when many individuals are physically involved in the key distribution. In an educational environment, which consist of students, staff, and other individuals, this problem is obvious. It is visibly unrealistic for individuals to store those keys by themselves and use them for their various communications purposes at will.

In recent years, mobile devices have become rampant.Documents on the laptop or desktop computer are transferred or duplicatedon phones and tablets for mobility. Information is constantly travelling in the air from device to device. However, data in transit is vulnerable to security threats of various kinds, especially its confidentiality, and AES algorithm implementation is not popular with these smart devices. A large number of the smart devices run on Android.Thisstudy, therefore, focused upon proposing a modelfor confidential data transfer on mobile device, and creating a prototype application for secure data transfer for Android.

The Waterfall system development life cycle model was adopted.The actors of the system were identified and their requirements and expectations noted. The essential reasons for the system were subsequently derived, and Use Case diagrams were used to compliment thedocumentation. A wide study of literature on components and system that are similar and relevant to the current focus was done, and enlightenment derived utilized.The model and application adopted a Client-Server architecture. The illustrations of the model were constructed with Unified modelling languages. The interfaces of the application were benched marked with other popular applications, and ensured to follow standard practices in designing Android applications. Several test cases were run to debug the application. Test techniques include White Box, Unit testing, and System Testing.

This study contributes towards enabling confidential data or information transfer by mobile devices by proposing a model and implementing a prototype for Android platform of the AES encryption standard. Encryption key exchange is securely automated, making it transparent and easy to use. The model could be used as a guide for developing similar systems. The application ensures confidential data transmission among smartphones users on Android.

2.0 OUTCOMES

2.1 The Model

2.1.1 Functional and Non-Functional Requirements

The functional requirements of different users are as follows: The System Administrator should be able to login, logout, manage users' profiles, add/delete users, and search through users, among others. A User should be able to login, logout, view messages, and search for messages.

Some of the non-functional requirements include that the system should be easy to operate, the target Operating System platform Android, the application should not be more than about 20 Megabytes, and the system should be robust enough to withstand faults or errors by restarting immediately as well as recovering data.

A Use Case diagram is used to show the functionality provided by a system in terms of actors, their goals represented as use cases, and any dependencies between them. It also depicts every functionality that any user can carry out on the system. Figures 1 and 2 show a standard user and the system administrator requirements of the system, respectively.

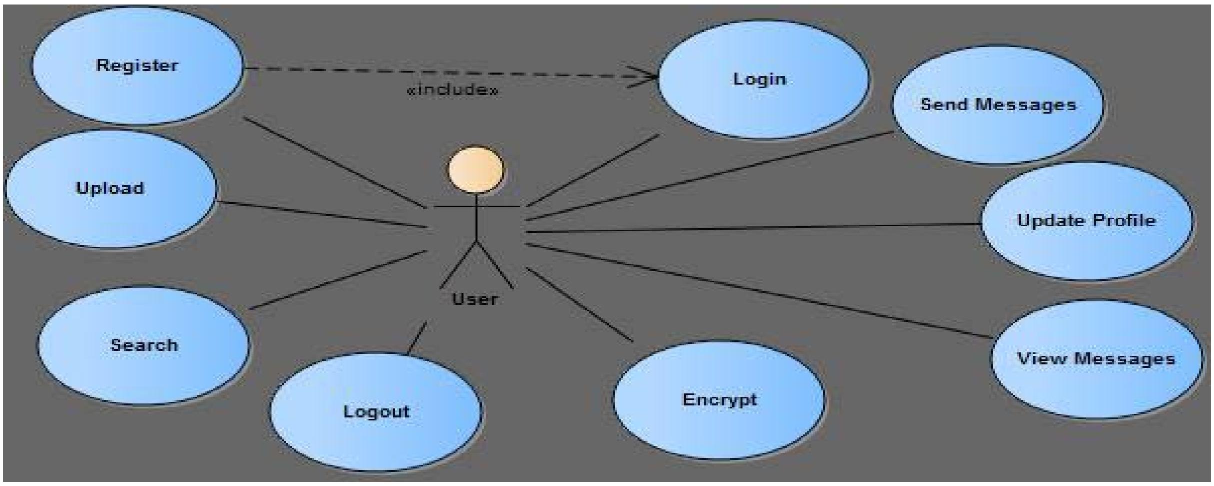


Figure 1 – Standard User Use Case

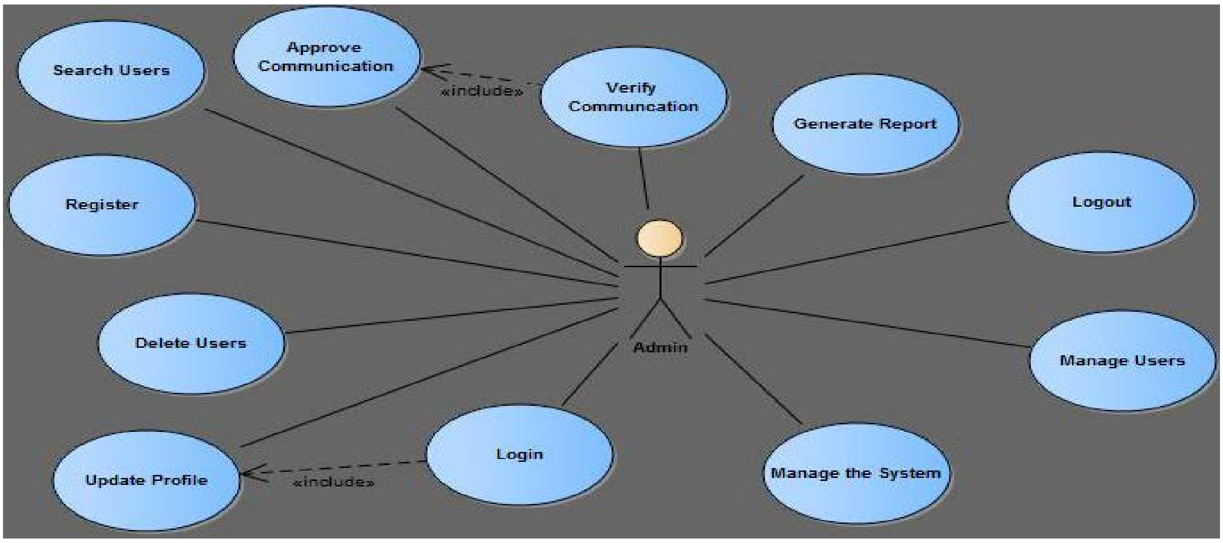


Figure 2 – The Administrator Use Case

2.1.2 System Architectural Layout

Figure 3 depicts the architectural layout of the proposed system. It shows a server and two model devices, the requirements needed for each component to work as well their main functionalities. This representation cuts across all forms of devices as well as all forms of servers. The server basically represents the backend functionalities and the devices show the frontend functionalities.

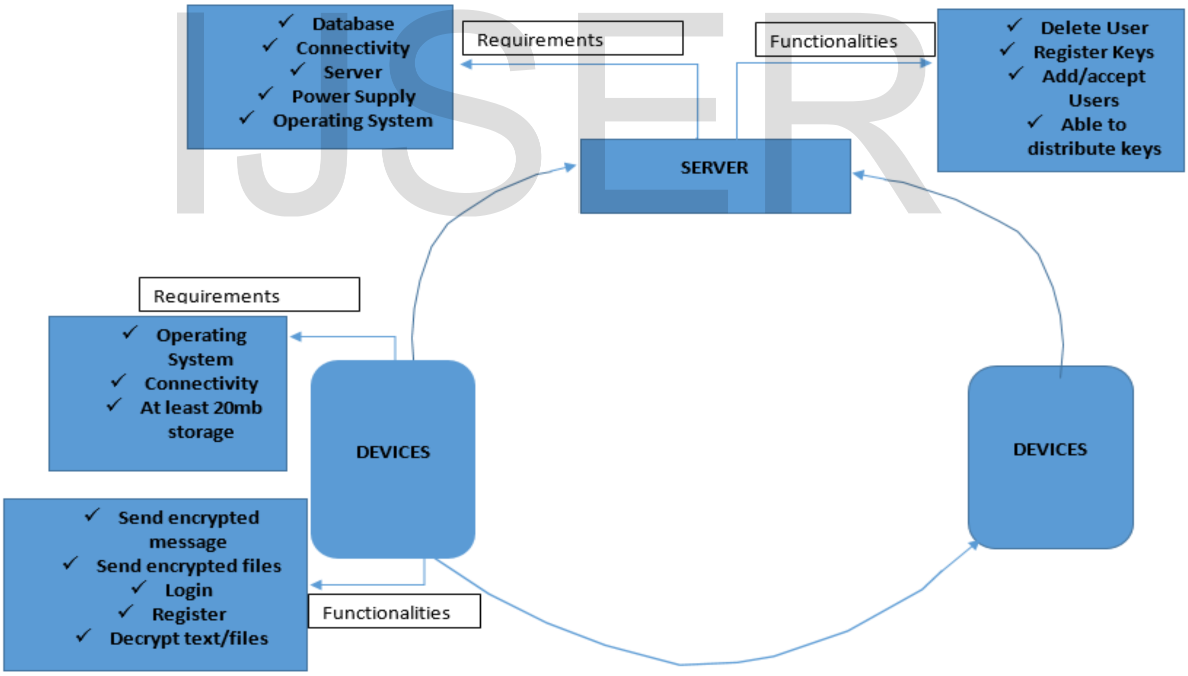


Figure 3 – Proposed System Layout

2.1.3 Database Design

Figure 4 presents the Entity Relationship Diagram (ERD). The ERD helps to capture application semantics, and is very good for conceptual designs. There are three entities, two weak entities, twenty two attributes, two weak attributes and two relationships.

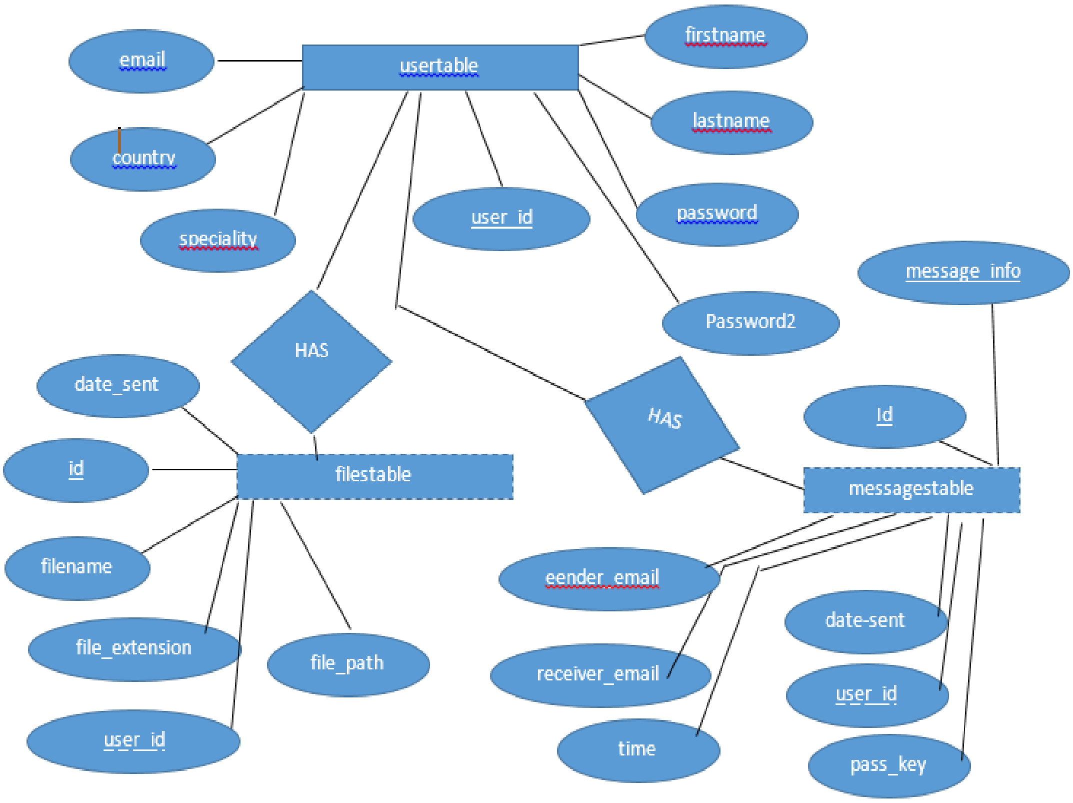
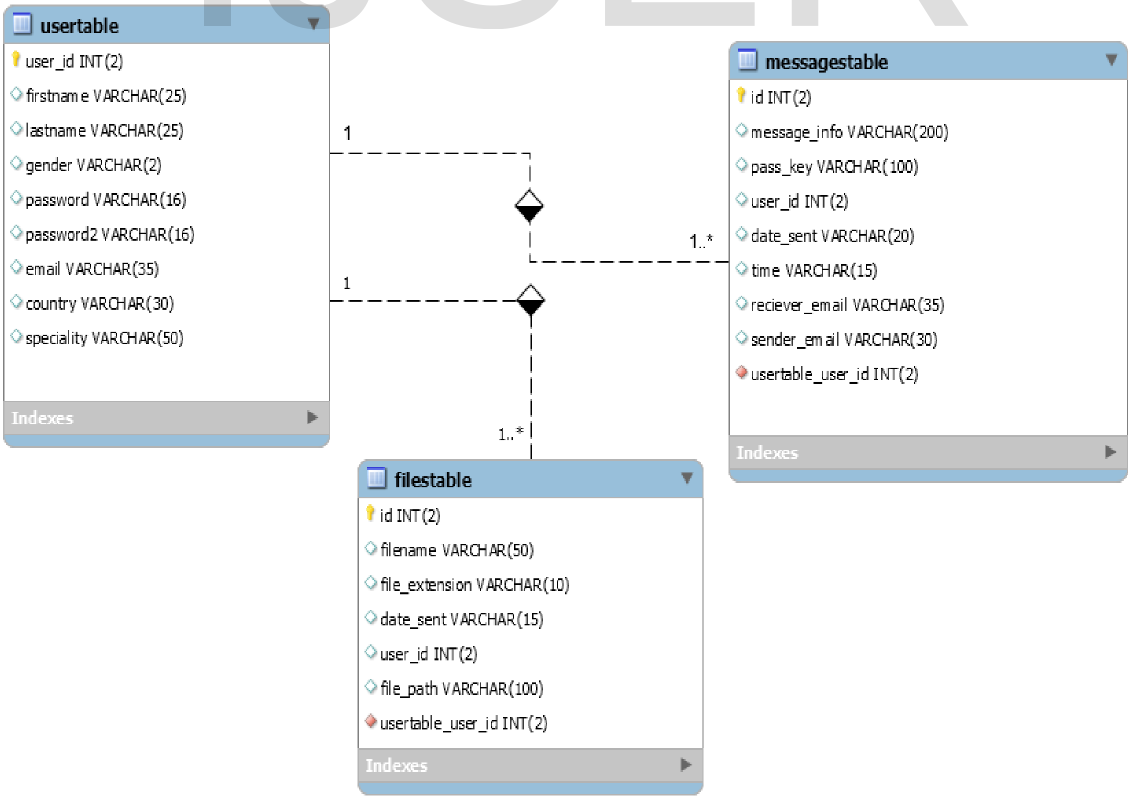


Figure 4 – Entity Relationship Diagram

After a comprehensive analysis of the system, the Files (filestable), Message (messagestable), and User (usertable) tablesare needed. Figure 5 shows the tables and their relationships.



usertable
user_id INT(2)
firstname VARCHAR(25)
lastname VARCHAR(25)
gender VARCHAR(2)
password VARCHAR(16)
password2 VARCHAR(16)
email VARCHAR(35)
country VARCHAR(30)
speciality VARCHAR(50)
Indexes

messagestable
id INT(2)
message_info VARCHAR(200)
pass_key VARCHAR(100)
user_id INT(2)
date_sent VARCHAR(20)
time VARCHAR(15)
reciever_email VARCHAR(35)
sender_email VARCHAR(30)
usertable_user_id INT(2)
Indexes

filestable
id INT(2)
filename VARCHAR(50)
file_extension VARCHAR(10)
date_sent VARCHAR(15)
user_id INT(2)
file_path VARCHAR(100)
usertable_user_id INT(2)
Indexes

Figure 5 - Database Tables and Relationships

2.2 The Application

The components of the application include User Interfaces, Plaintext, Encryption Algorithm, Cipher Text, Decryption Algorithm, and Encryption/Decryption Key. User Interfaces are views containing text boxes and buttons providing links or direct access to functions that meet the application functional requirements. Plaintext is the confidential data or information input to the encryption algorithm to generate a cipher text. In this case the user types and sends a message to a recipient.Encryption Algorithmis a mathematical process that produces a cipher text for any given plaintext and encryption key (Tutorialspoint, 2017). It is a cryptographic algorithm that takes plaintext and an encryption key as input and produces a cipher text.Cipher Text is the encrypted version of the plaintext produced by the encryption algorithm using a specific encryption key (in this case a generated key).Decryption Algorithmis a mathematical process, that produces a unique plaintext for any given ciphertext and decryption key (Tutorialspoint, 2017). It is a cryptographic algorithm that takes a ciphertext and a decryption key as input, and outputs a plaintext. In this case, the decryption key and the encryption key is essentially the same because this is a symmetric key algorithm. The decryption algorithm basically reverses the encryption algorithm and is thus closely related to it. Encryption/Decryption Key is a random sequence of strings used to encrypt and decrypt text respectively. It is generated randomly when an instance of the encryption system is run. In this case the AES algorithm uses a key size of 128 bits.

2.2.1 Interfaces

An implementation of a prototype of the developed model has a number of interfaces including Splash Page, Login Page, Register Page, Home Page, Direct Message Page, View Message Page, First Validation Page, and Second Validation Page, among others. Some of these are subsequently presented.Figure 6 depicts the Splash page. It is a welcome page into the application and stays on screen for a maximum of 2000 milliseconds before it disappears and is replaced by the Login page.

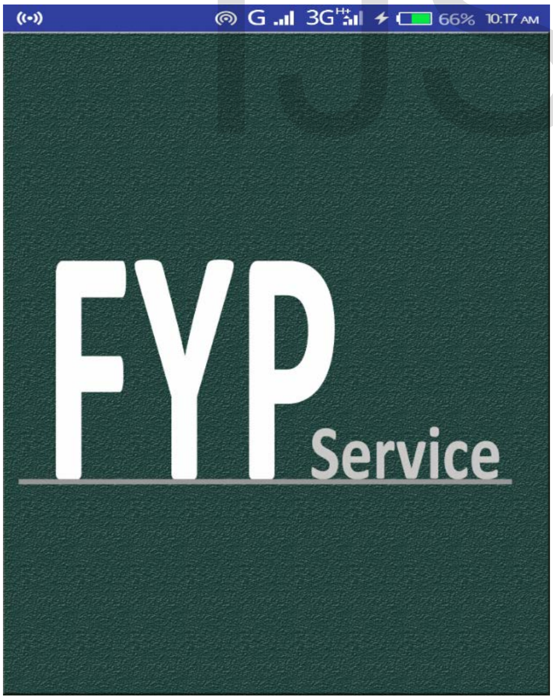


Figure 6 – Splash Page.

Figure 7 depicts the Login page, where the user’s email address and password required for authentication purposes.A button on this page also allows registrationof newusers.

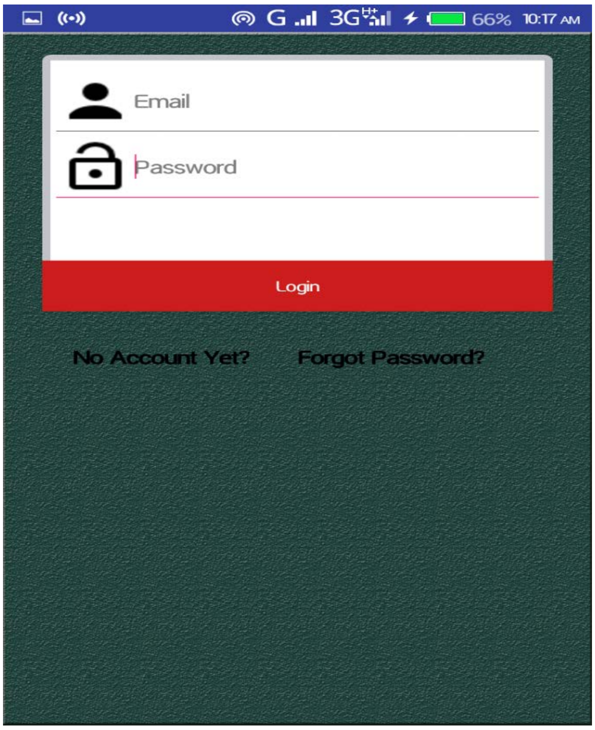


Figure 7 – Login Page.

Figure 8 presents the Register page. A new user provides details, which include first name, last name, country, gender, password, email address, and a check box for validation. The email address is a primary key, and the application ensures no two users share one. The user must also accept the terms and conditions of using the application.

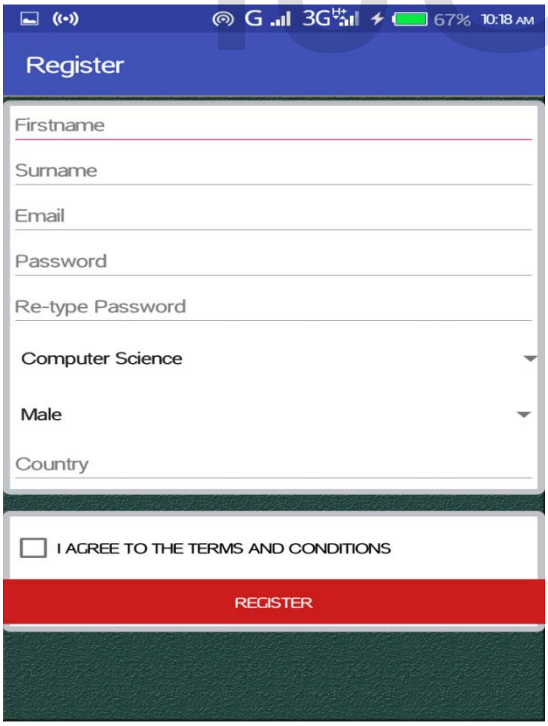


Figure 8 – Register Page

On successful login, the Home page (Figure 9) is displayed. Access to the main functionalities of the application is provided, including logout.

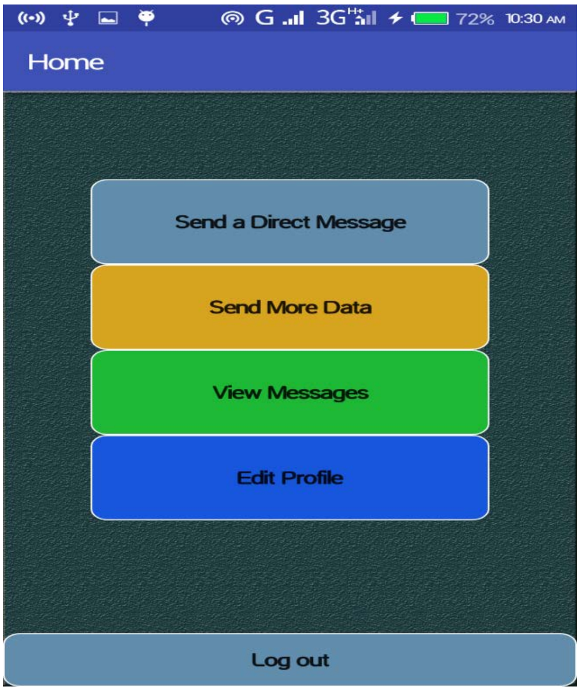


Figure 9 – Home Page

Figure 10 shows the Direct Message page through which confidential messages are passed. The recipient's registered name and the message to be sent are required. The system generates a key, attaches it to the message and recipient, and subsequently sends it through the Internet.

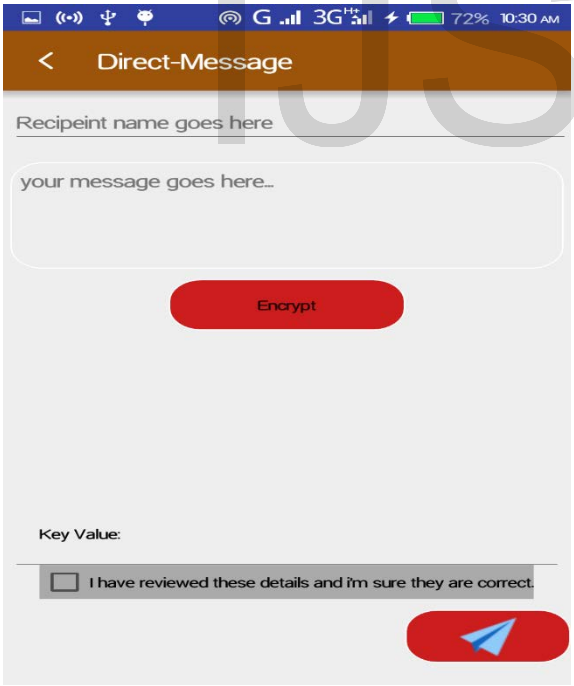
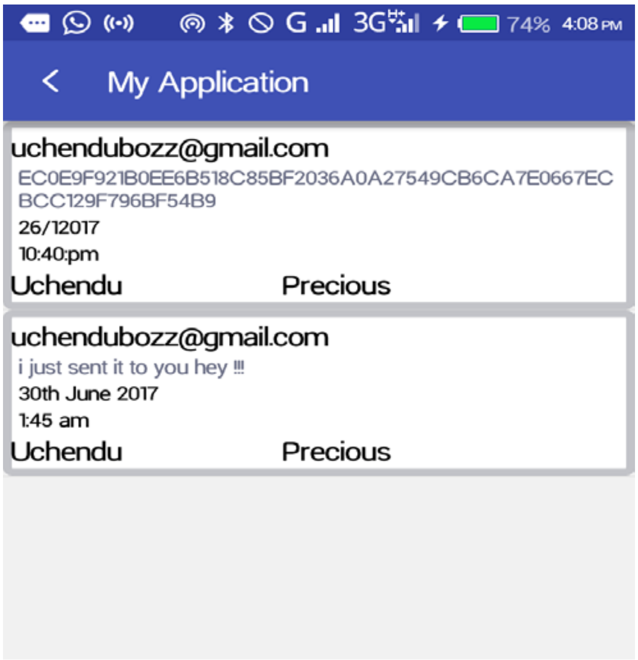


Figure 10 – Direct Message Page

A user with the email address uchendubozz@gmail.com sends a direct message to ola@gmail.com. The View Message interface (see Figure 11) shows that the user ola@gmail.com received two messages from uchendubozz@gmail.com.

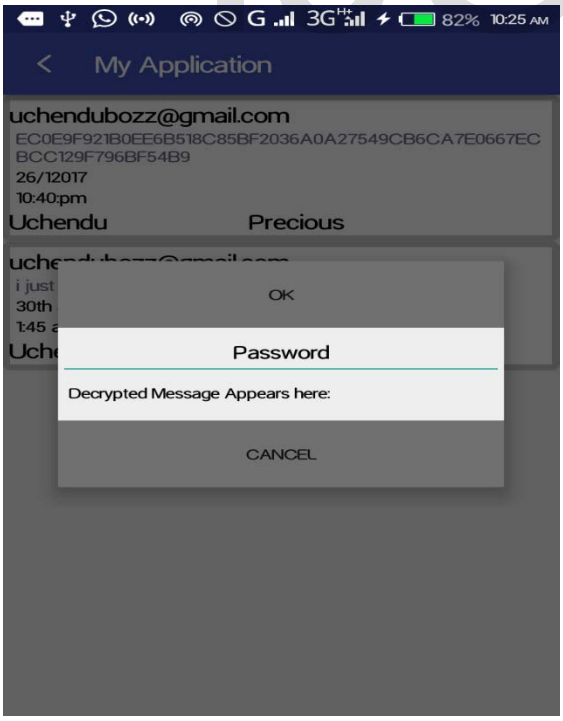


uchendubozz@gmail.com
EC0E9F921B0EE6B518C85BF2036A0A27549CB6CA7E0667EC
BCC129F796BF54B9
26/12017
10:40:pm
Uchendu Precious

uchendubozz@gmail.com
i just sent it to you hey !!!
30th June 2017
1:45 am
Uchendu Precious

Figure 11 – View Message Page

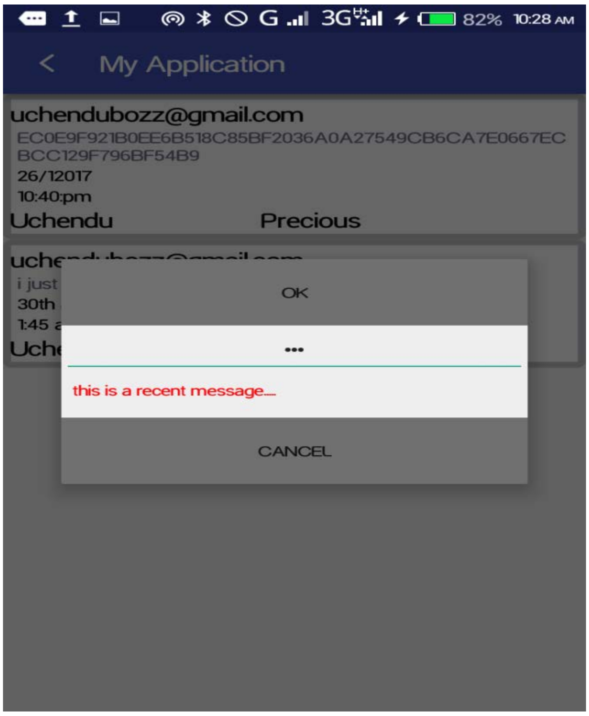
A little square like window comes up when the user clicks on a particular message on their list of messages (see Figure 12). The user's password is required in order to view the sent message in decrypted form. The system gets the password, checks that it matches the user's current password, queries the database and fetches the password based on the password and the message that was clicked. The server then distributes the key and the application gets it as a Post parameter and the message is decrypted into its plain text (see Figure 13).



uchendubozz@gmail.com
EC0E9F921B0EE6B518C85BF2036A0A27549CB6CA7E0667EC
BCC129F796BF54B9
26/12017
10:40:pm
Uchendu Precious

Password
Decrypted Message Appears here:

Figure 12 – First Validation Page.



uchendubozz@gmail.com
EC0E9F921B0EE6B518C85BF2036A0A27549CB6CA7E0667EC
BCC129F796BF54B9
26/12017
10:40:pm
Uchendu Precious

uche
i just
30th
1:45 a
Uche

this is a recent message....

Figure 13 – Second Validation Page.

3.0 LITERATURE REVIEW

Organisations are open systems that affect and are affected by their environment (Griffin, 2017). Some essential characteristics of an organization include task, technology, people and management. Information system is the software and hardware systems that support data-intensive applications (Neuman, Shasha and Vossen, 2016). Data is a raw fact or an unprocessed information, and can take the form of a number or statement such as a date, time or measurement. Information is generally known as processed data that is meaningful (Stairs and Reynold, 2014). In order for information to be produced, several processes, such as collection of data,data editing, data input, data storage, and data transformation, have to take place (Hardcastle, 2011).

There is the need to secure data or information transfer among individuals. The need for security is high as documents are transferred between individuals and from one place to another. Without security mechanisms in place, data breaches becomes more rampant.Information security necessitates protecting both the system hardware and the data that the computer hardware holds from unauthorized users, access, theft or damage.

Entities should build information security measures into procedures, systems, products and ingenuities at the design stage (Bassey, 2010).How entities handle individual’s information is controlled by the Privacy Act, and it entails taking practical steps in protecting personal information from mismanagement and loss (Australian Government , 2013). It is usually not distinctive when the data being sent is personal or business confidential. Adequate protection should be present.Data handling practices considers how information is been collected, handled and finally stored.

Education is moving from a knowledge-transfer model to a joint, active, self-directed and engaging model that helps learners increase their knowledge and improve the skills needed to excel in the “Learning Society” (Michelle , Ana and Jim, 2013).Education is the process of facilitating learning, or the acquisition of values, skills, views, and behaviours. Education has various methods like: training, teaching, conversations, and storytelling, among others. In the process of knowledge acquisition, various seminars, workshops are being held, devices and various gadgets are being utilized, data is being transferred in some way either between institutions, members of staff, learners others, and so on. There is need for confidential data protection (encryption). A typical laptop for a coach, teacher,other member of staff, and learners other is likely to have piles of sensitive data on it (Fleming, 2011). Encryption in a learning society is essential.

3.1 Security

What is secure is safe from harm and theft. Information security vulnerability is described as any weakness that can be exploited to violate a system. Risk is a measure of the cost of a vulnerability. It is a measure of the cost of a weakness. Risk management is the total process of identifying, measuring, controlling and minimizing the likelihood of an attack.Security is elimination or adequate reduction of vulnerabilities of assets and resources. There are several categories of safeguards. These include Communication security safeguards, Computer security safeguards, Physical security, and Media security, among others (Kim and Solomon, 2017). Categories of security service include Authentication, Access control, Data confidentiality, Data integrity, and Non-repudiation.

Security mechanisms are majorly divided into two, namely, human based and technology based. Some Human based mechanisms or techniques include managing technology life cycle andbeing very aware of e-mail attachments(right-click downloaded files and choose the option to scan the file manually with whatever security program available) (O'Reilly, 2011).

Primary security issues are confidentiality, integrity and availability. They are basic security issues, which technology must guarantee. Confidentiality is synonymous to privacy. Confidentiality has several aspects such as Privacy of Communications, Secure Storage of Sensitive Data, Authenticated Users, and Granular Access Control (Oracle Corporation, 2002). Integrity simply has to do with the data validity; data is protected from deletion and corruption in storage, in processing or in transit; while it resides within the database, it is being processedor while it is being conveyed over the network. Confidentiality and integrity must be met for data to be properly secure. They are inseparable.

3.3 Encryption

Encryption has been proven to be one of the most effective data protection controls available today (Cloud Security Aliance, 2012). The purpose of encryption is to ensure that only somebody who is authorized to access data will be able to read it plainly, using the decryption key. There are three main types of encryption. These are symmetric, asymmetric and hashing.

Symmetric encryption simply means taking a plain text and scrambling it to protect it from unauthorised reading and then unscrambling it again when it is needed, using the same key. Examples are Triple Data Encryption Standard (3DES), Advanced Encryption Standard (AES), Blowfish, International Data Encryption Algorithm (IDEA) and Rivest Cipher 4 (RC4).The key has to be secure even while it's being mutual among parties that rightfully needs it (Behrens, 2014).

Asymmetric technique takes understandable data, encrypts it, and decrypts it again at the other end, using different keys at both ends. Encrypters use a public key to scramble the data, and decrypters use the matching private (secret) key on the other hand to unscramble it again. Some asymmetric encryption mechanisms have the ability to cryptographically sign data, where the private key is used to create the signature, and the public key is used to verify it.Examples are Diffie-Hellman Key exchange, Rivest-Shamir-Adleman (RSA), and Digital Signature Standard (DSS).

Hashing is the transformation of a sequence of characters into a shorter fixed-length value or key that represents the original string. That value is referred to as a hash, which is impossible to reverse back to the original data, same data will always produce the same hash and given knowledge of only the hash, it is infeasible to create another string of data that will create the same hash (collision) (Behrens, 2014). Hashing is actually not a form of encryption, though it uses cryptography. It is possible with access to different hashes and lots of resources to find data that was hashed, if unsalted, which could be a password. It is, therefore, important to make use of strong hashing algorithms like "bcrypt" and "scrypt". It is important to remember that any system is only as secure as the weakest link in the chain.

3.3.1 Evaluating the AES Algorithm with DES

Data Encryption Standard (DES) was the first encryption standard to be recommended by NIST. DES is a 64 bit algorithm (with 64 bits block size). The weakness of DES in key size has been exploited as a compromise, which has necessitated the development of algorithms that do not have this weakness (Stallings, 2005).

AES is a blockcipher that has a variable key length of 128, 192, or 256 bits (the default). Its encryption is done on data blocks of 128 bits, in 10, 12 or 14 rounds, depending on the key size. AES encryption is fast and flexible (Stallings, 2005).AES was adopted as the official encryption method by the NIST of the US Government, and has been acknowledged globally (Townsend Security, 2017). Many suppliers of encryption software and hardware have integrated AES encryption into their services.The AES algorithm is neither a computer software nor a source code, but it is an analytical depiction of procedures concealing data.

3.3.2AES Modes of Operation

Several methods of using keys with the AES encryption method exist. These methods are known as “modes of operation”. NIST outlines a number of modes of operation for AES which include Output feedback (OFB), Electronic code book (ECB), Cipher block chaining (CBC), Counter (CTR), Cipher feedback (CFB), and Galois Counter Mode (GCM) (National Institute of Standards and Technology, 2001). The strength of AES is generally acknowledged, evidenced by its usage in various aspects of the global economy, including educational system.

3.3.3Key Distribution Centre

Assuming there exists a large number n of mobile people that intend on communicating with each other confidentially. A shared secret for each pair implies n(n-1)/2 distinct keys in the system (Joshi, 2008). Managing such a large number of keys becomes tiresome. A new individual joining the group must contact every other member to establish shared secrets with them.Instead of having a shared key for each pair of entities, what is prescribed is to have a centralized Key Distribution Centre (KDC), whichmanages and distributes keys to different entities when required. When two different entities desire communication with each other, they request the KDC to generate a shared key for them. When an online KDC is implemented, there would be only n keys, instead of n(n-1)/2 keys in the system. It should be noted, though, that the KDC server becomes a single-point-of-failure of the entire system and a performance bottleneck. Possible methods of key distribution are Physical distribution, Distribution using symmetric protocols (Kerberos - KDC), and Distribution using public protocols (Stallings, 2005).Advantages of implementing KDC includeCentralized key distribution, Ability to implement session and static keys, Suitability for large networks, Automatic key distribution, Fast key distribution, Ensuring backup and recovery of keys, and Control of key usages among entities.

Key management is the set of techniques and procedures backing up the establishment and maintenance of keying relationship between authorized bodies(Slideplayer, 2017)**.** Key management encompasses techniques and procedures supporting Initialization of system users within a field, Generation, dissemination, and installation of keying material, Update, cancellation, and destruction of keying material, and Storage, backup/recovery, and archival of keying material.There are two main types of key used in cryptography: static and session keys. Static keys (long-tern keys) are to be in use for a long term (time) period. When static keys are compromised, there are major complications that take place. Session keys (short-term keys) have a short life-time, and are usually used to provide privacy for the given time period. The compromise of a session key should only result in the compromise of that session’s secrecy and it should not affect the long-term security of the system (Hamilton, 2016)

Figure 14 illustrates Kerberos protocol of KDC. Alice sends a message to the KDC requesting for a session key to communicate with Bob. The message has a termination time t_{exp} and a nonce N. A nonce is a random number (Kak, 2016). The KDC responds with a ticket which comprises of a session key k_{AB}, a timestamp t_s the Internet Protocol (IP) address of Alice, the expiration time texp, and the nonce N. The message is encrypted with the shared key between Alice and KDC, $K_{A,KDC}$. The KDC also encrypts the ticket with the key that Bob shares with it ($K_{B,KDC}$), and sends it to Alice. Alice decrypts the message that was encrypted with $K_{A, KDC}$, and extracts the session key k_{AB} out of it. She then forwards a message to Bob that has her identity, Bob’s identity, and timestamp ts, and is encrypted with k_{AB}. She also sends the ticket that she received from the KDC, which was encrypted with $K_{B,KDC}$. Bob decrypts the ticket, and the session key k_{AB} is extracted out of it. It then sends a message back to Alice that has his and Alice’s identities, and the timestamp ts with 1 added to it. The message is encrypted with k_{AB}.

Kerberos protocol drives a KDC.

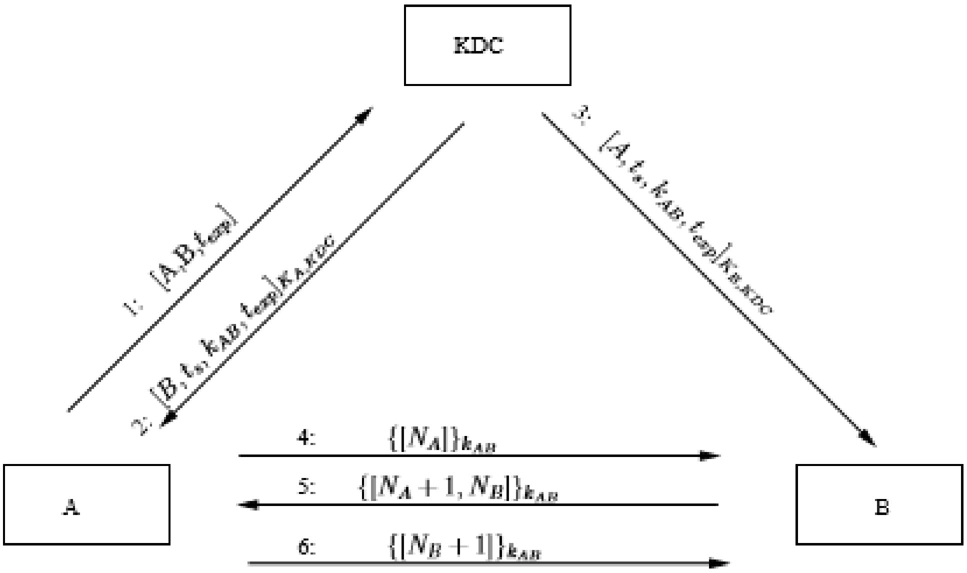

KDC
1: $[A, B, t_{exp}]$
2: $[B, t_s, k_{AB}, t_{exp}]_{K_{A,KDC}}$
3: $[A, t_s, k_{AB}, t_{exp}]_{K_{B,KDC}}$
4: $\{[N_A]\}_{k_{AB}}$
5: $\{[N_A + 1, N_B]\}_{k_{AB}}$
6: $\{[N_B + 1]\}_{k_{AB}}$
A
B

Figure 14 – Kerberos Protocol (Joshi, 2008) {**A** means Alice and **B** means Bob}

It should be noted that some attacks are possible. If we leave out Bob's identity in the messages from Alice, then a man-in-the middle attack isabout to. The man-in-the-middle intercepts the first message from Alice, and replaces Bob withBob'. The KDC replies back with a ticket that is encrypted with the shared key between itself and Bob'. The man-in-the middle then intercepts the message from Alice to Bob, and forwards it to Bob', and forwards the response from Bob' to Alice.

Design issues and flaws with Kerberos include the KDC uses passwords to authenticate users, which is not good. In addition, revocation of a key is easy. It requires just the removalof information of a user's key from the KDC to remove the user. Moreover, when the security of the KDC is compromised, then the whole system is compromised (Joshi, 2008). There are other protocols,such as Needham-Schroeder Secret-Key Protocol, Wide-Mouth Frog Protocol, and Otway-Rees Protocol, which help in key distribution (Hamilton, 2016). They also have their various faults. Kerberos protocol is the most suitable one to be used, despite the fact that it also has its own flaws. Addition measures are desirable to ensure high security and reliability.

A clear difference between the Needham-Schroeder protocol and the Kerberos protocol is that the latter makes a distinction between the clients, on one hand and the service providers on the other. But the Needham-Schroeder protocol does not (Kak, 2017). In the Kerberos protocol, the Key Distribution Centre (KDC) is divided into two parts, one devoted to client authentication, and the other in charge of providing security to the service providers. The first part is also regarded as Authentication Server (AS) and the other part Granting Server (TGS). Some things that the implementation of the KDC should address KDC and user authenticity and session key lifetime dependability. Figure 3 depicts the relationship and flow between two mobile devices and the KDC server, which this study implemented.

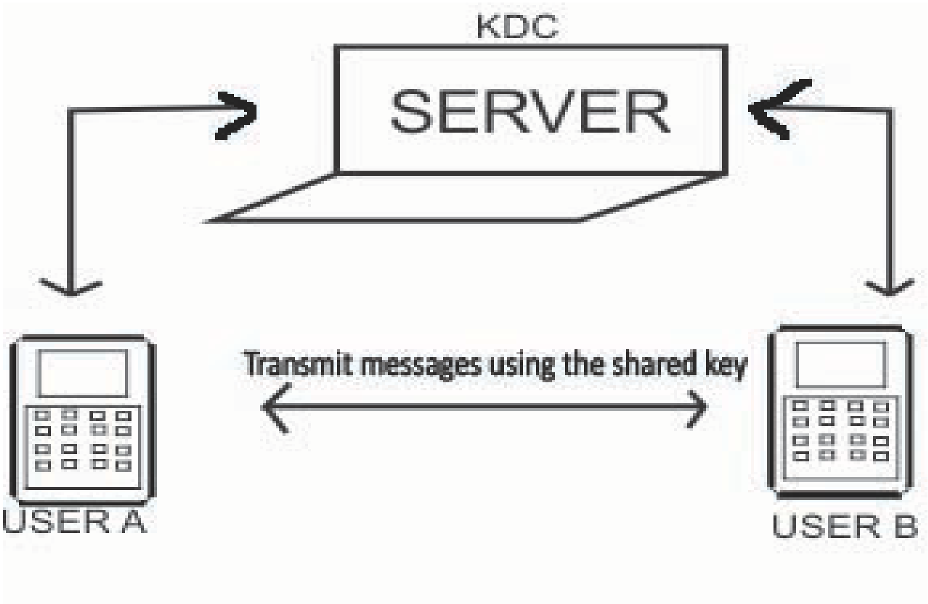


Figure 3 – Communication Path way between the KDC and Mobile Devices.

4.0 CONCLUSION

Different security measures have been implemented over time that have helped protect data confidentiality.However, security is a facet of computing that has to be improved continually. As efforts are been continually made to improve security, the notion of a perfectly secure system will always be an illusion as attempts to compromise systems never cease.

A model for secure data transfer on mobile device was developed.An implementation of the AES algorithm for encryption anda KDC, which adopted Kerberos protocol for key management and distribution, for Android platform, was done.

Future focus could be on implementing the application on other smart device Operating System platforms, with emphasison the system feasibility.

REFERENCES

Australian Government . April(2013). Guide to information security. *Creative Commons*. Retrieved From: https://www.oaic.gov.au/images/documents/privacy/privacy-guides/information security-guide-2013_WEB.pdf

Behrens, M. (2014, November 20). *Atomic Object*. Retrieved from: https://spin.atomicobject.com/2014/11/20/encryption-symmetric-asymmetric-hashing/

Cloud Security Aliance. (2012). Encryption. 10. Retrieved from:

https://downloads.cloudsecurityalliance.org/initiatives/secaas/SecaaS_Cat_10_Network_Security_Implementation_Guidance.pdf

Fleming, R. (2011). Encryption in education – If one of your staff laptops disappears – do you know the data is secure? Retrieved from: https://blogs.msdn.microsoft.com/education/2011/03/30/encryption-in-education-if-one-of-your-staff-laptops-disappears-do-you-know-the-data-is-secure/

Hamilton, G. (2016). Symmetric Key Distribution. Retrieved from

http://www.computing.dcu.ie/~hamilton/teaching/CA642/notes/KeyDistribution.pdf

Hardcastle, E. (2011). Business Information Systems. Retrieved From:

http://www.sciepub.com/reference/68121

Joshi, P. (2008). Key Distribution. Retrievd From:

https://people.eecs.berkeley.edu/~daw/teaching/cs261-f08/scribenotes/1108-joshi.pdf

Kak, A. (2017). Key Distribution for Symmetric Key Cryptography and Generating Random Numbers.Retrieved from:

https://engineering.purdue.edu/kak/compsec/NewLectures/Lecture10.pdf

Kim, D., and Solomon, M. G. (2017). *Fundamental Information Systems Security* (3rd Ed.). Burlington, MA: Jones & Bartlett Learning

Michelle , S., Ana, S., & Jim, B. (2013). How Ubiquitous Connectedness Can Help Transform

Pedagogy. Retrieved From:

http://www.cisco.com/c/dam/en_us/solutions/industries/docs/education/education_internet.pdf

National Institute of Standards and Technology. (2001). Advanced encryption standard (AES) development effort. Retrieved from: http://csrc.nist.gov/archive/aes/index2.html

Neumann, F., Shasha, D., and Vossen, G. (2016). Databases: Their Creation, Management and Utilization. Retrieved June 1, 2016, from:

https://www.journals.elsevier.com/information-systems/editorial-board

Oracle Corporation. (2002). Security Review. Retrieved From:

http://dl.acm.org/citation.cfm?doid=1008731.1008734

O'Reilly, D. (2011). How to secure your PC in 10 easy steps. Retrieved from: http://www.cnet.com/how-to/how-to-secure-your-pc-in-10-easy-steps/

Privacy Technical Assistance Center. (2011). Data Security: Top Threats to Data Protection. Retrieved from: http://ptac.ed.gov/sites/default/files/issue-brief-threats-to-your-data.pdf

Slideplayer (2017). Key Management in Cryptography. Retrieved from http://slideplayer.com/slide/5886840/

Stair, R. M. & Reynolds, G. W. (2014). *Fundamentals of Information Systems*. Boston, MA: Course Technology, Cengage Learning

Stallings, W. (2005). *Cryptography and Network SecurityPrinciples and Practices.* Retrieved From: http://www.inf.ufsc.br/~bosco.sobral/ensino/ine5680/material-cripto-seg/2014-1/Stallings/Stallings_Cryptography_and_Network_Security.pdf

TechTarget. (2014). Advanced Encryption Standard. Retrieved from: http://searchsecurity.techtarget.com/definition/Advanced-Encryption-Standard

Townsend Security. (2017). PCI DSS.Retrieved from:https://www.townsendsecurity.com/compliance/PCI

Tutorialspoint. (2017). Cryptosystems. Retrieved from: https://www.tutorialspoint.com/cryptography/cryptosystems.htm

United States National Institute of Standards and Technology. (2001). Announcing theAdvanced Encryption Standard (AES). Retrieved From: http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf

Griffin, D. (2017). Open System Organisational Structure. Retrieved from: http://smallbusiness.chron.com/open-system-organizational-structure-432.html

Zukime, M., Mat, J., Abdullah, O., Mohd, A. S., & Mohd, S. A. (2014). Data Security: Issuesand Challenges for Disaster. *International Journal Of Scientific & Technology Research*, Volume 3, Issue 8, 152-153.