ZAMBIA INFORMATION COMMUNICATION TECHNOLOGY (ICT) JOURNAL

Volume 3 (Issue 2) (2019) Pages 31-43

A Security Framework for Mobile Application Systems: Case of Android Applications

Michael Bwalya[1] and Christopher Chembe[2]
Mulungushi University, Department of Computer Science and Information Technology,
Box 80415, Kabwe, Zambia.
1. mikob87@gmail.com, 2. cchembe@mu.edu.zm

Abstract

Currently, mobile applications are playing a major role in many areas such as banking, social networking, financial apps, entertainment and many more. The increase in number of applications succumbs to several security vulnerabilities and thus focus should be given to security. As the number of vulnerabilities and, hence, of attacks increase, mobile applications need to be assessed and ensure that secure coding practices have been followed during development. Mobile application security breach can lead to fraudulent transactions through mobile applications, confidentiality and revenue loss through communications services misuse. Data that is shared on an unsecured channel is vulnerable to attacks and to stop unauthorized access to this data, there is need to encrypt the data before it is sent to the server. In this research work, different cryptographic algorithms for encrypting data and secure data sharing in mobile applications across communications channels were examined. Simulation methodology was used to investigate a suitable cryptographic algorithm and to design a security framework for mobile applications to solve mobile application security problems. The proposed framework employs the use of Advanced Encryption Standard (AES) algorithm for encrypting meter readings data being exchanged between a smart phone and a server. The meter reading datasets used in this research were obtained from the Water Utility Mobile Application for Meter Reading. The results obtained from the simulation of the security framework, showed that four fields namely: Account number, image path, meter number and phone number on which AES encryption was applied were in an unreadable format (ciphertext), implying that the fields have been successfully encrypted. This solution allows application users (meter readers) to transfer (upload readings) data between a smart phone and database server in a secure manner without facing the problem of data attack. Data being uploaded to the server is encrypted before it is transferred and decrypted once it reaches the server side. This solution addresses android application security in the application and network communications layers and data transmission. The research paper ensures information security is guaranteed between an organisation and its customers.

Keywords: Encryption Algorithm; Cryptography; Information security; Mobile application; Attacks; Advanced Encryption Standard.

I. Introduction

Mobile devices are quickly becoming the platform of choice for organizations to conduct business more effectively. There is a wide range of functionalities provided to the users by the mobile devices such as fast connection to social platforms, personal data storing, financial processes, web browsing and tons of services.

Android based devices have attracted massive market share due to its open architecture and the popularity of its application programming interface (APIs) in the developer community. The expanded popularity of the Android devices and associated monetary benefits has made it an ideal target for malware developers, resulting in big rise of the Android based security issues [1]. According to [2], the directness of these environments will lead to new applications and markets and will enable greater interfacing with existing online services. However, as the importance of the data and services of smartphones increases, so too do the opportunities for vulnerability. It is therefore important that this next generation of platforms provide a comprehensive and usable security infrastructure

In view of the above, this research involves developing a security framework that employs the use of cryptography in a mobile application system. Cryptography is the technique and science of keeping messages secure [3]. Cryptography is an integral part of modern world information security making the virtual world a safer place [4] and it is the best way for encryption [5]. Cryptography converts the original data into ciphertext which is an unreadable form (Encryption) and again converts the ciphertext into original form (Decryption) [6]. The two widely accepted and used cryptographic methods are 1) Symmetric-key algorithms 2) Asymmetric-key algorithms. Symmetric algorithms utilize the same key for encryption and decryption. This is termed as secret key. By using the same key, messages are encrypted by the sender and decrypted by the receiver. It contains algorithms like Data Encryption Standard (DES), Advanced Encryption Standard (AES), Triple DES,

Blowfish etc. Asymmetric algorithms use different keys. Public key is used for encryption and other private key is used for decryption. This is known as public key. The public key is known to the public and the private key is known to the user. It comprises various algorithms like Rivest, Shamir, & Adleman (RSA), Digital Signature Algorithm (DSA), Elliptic Curve(EC), Diffi-Hillman(DH) [7] [6].

The proposed solution uses symmetric algorithm as it has the speed and computational efficiency to handle encryption of large volumes of data. The strength of the encryption in symmetric cryptosystems goes with longer the key length. AES is the commonly used encryption technique nowadays, this algorithm is based on many substitutions, permutations and linear transformations, each executed on data blocks of 16 byte. As of today, there are no practicable attacks that exist against AES. Therefore, AES remains the preferred encryption standard for governments, banks and high security systems around the world [6], [8], [4].

This solution allows data to be encrypted before it is sent and decrypts the data once it reaches the server. In this regard, the solution addresses the concerns in android application security in the application and network communications layers and data transmission thereby achieving security goals of data namely: Confidentiality, Integrity and Availability (CIA).

This study will potentially identify critical success factors for Companies planning to start using mobile technologies to protect the integrity, confidentiality and availability of information in today's highly networked systems environment. This paper is valuable in that, Companies will have remediation measures and controls needed to mitigate identified vulnerabilities and implement secure interfaces. Apart from that, Mapping vulnerabilities to flaws at the architecture and design level helps prepare a comprehensive remediation plan.

II. Threats and Attacks in Mobile Applications

Type of attacks in network security

There are several type of attacks possible in a network that can be divided two categories [9], [10]:

I. **Passive attacks:** In these attacks, an attacker intercepts the data on transit with the intention of reading and analyzing the information not for modifying it. These are attacks in which attacker play no active part and there are less chances of an attacker's identity getting revealed. Wiretapping, sniffing and eavesdropping fall under this group.

II. **Active attacks:** In these attacks, an attacker intercepts the connection and alters the data. This can be done by sending virus, Trojan or any malicious packet and the chances of attacker getting traced back are there. Denial of Service ,Domain Name System (DNS) spoofing, Man in the middle attack, Address Resolution Protocol(ARP) poisoning, Buffer overflow, Heap overflow and Structured query Language (SQL) Injection are common active type attacks

Types of attacks in mobiles

The increase in mobile phone use has made it easy for attackers to attack as they have now a larger platform to exploit. There are a number of ways in which the type of attacks in mobiles can be segregated. Some of them are explained as follows:

Wi-Fi based attacks

An attacker can intercept a Wi-Fi communication by doing eavesdropping. The security in WLAN is more vulnerable. It is possible for an attacker to break the password easily get in the local network of the victim. In an event where an attacker prospers in breaking identification cipher, it becomes possible to attack both the phone and the entire network [11].

Web browser based attack

In web browser based attacks, an attacker uses leverages like stack based overflow and other vulnerabilities in libraries. This is possible in all kinds of operating system either Android or iOS. Smartphones are also vulnerable to phishing and other malicious web site based attacks and the biggest problem with smartphones is that they don't have strong antivirus protection yet [12].

Operating System based attacks

One may apply any number of secure mechanisms but if there is vulnerability in operating system, it might be going to affect one day surely. There are several loopholes in operating systems of smartphones as these are in earlier stages and developers are not much aware about the kind of attacks possible. It was likely to dodge the security of operating system and circumvent the bytecode verifier and gain access of core operating system. Similarly in windows mobile OS, one can easily edit the general configuration file to a modifiable file. It is also possible for a malicious attacker to do modifications in the directory whenever an application is installed as at that time it has root privileges [12].

Types of possible Threats:

In a study by [13], it has been indicated that there are several threats that are possible in applications. In another study [14] stated that input validation is the most dangerous and general type of attack. The author noted that developers tend to forget to put validation on what is fed to users. Because of this, malicious user provides unauthorized input that leads to crash or infect the application. Attacks that fall in this category are Buffer overflow, Cross-site scripting and SQL injection. Furthermore, it was indicated that authentication is one of the posed threats, in which user credentials are provided to prove the legitimacy to use application. This mechanism should be applied to some sensitive application so that illegitimate person cannot do interference. Attacks that are common in this category are: Brute force attack, Cookie reply, Dictionary attack and Credential theft.

Mobile Security

Mobile security can also be referred to as digital security, this is because digital security falls under the area of safeguarding the data that is on phones, computers or internet [15]. A study

by [15] further indicated that digital security includes safeguarding of digital characters. It encompasses taking all needed precautions to ensure that identities, resources and technology in networked and mobile world are secure. Digital products that are networked can be hacked or stolen. In simple terms, digital Security is securing networked systems. As for [14], it was stated that when it comes to digital security concerning smartphones, the platforms used are not greatly protected and very susceptible to attack. Smartphone operators are unaware about the security issues of their phone. The main operating system commonly used in smartphones are android, iOS, Windows, blackberry, Symbian, Bada.

Challenges of Mobile security

A study by [13] stated that smartphone users are exposed to different threats. These threats may disturb operation and transfer user data from smartphones. The main threat targets are:

i. Data: This is the main target of any attacker. Sensitive information like passwords or Debit/Credit card number may get stolen.

ii. Identity: Smartphones have a different identity like IMEI, IMSI or UDID. Apps may transmit all these information to steal the identity of owner.

iii. Availability: one can deprive the services or limit the access by attacking a smartphone.

Application Security

Application security is an arm of security that focuses mainly on the security of application built for various platforms like mobile application, web application and system application. This ensures that there is no weakness in design, development, deployment and maintenance of application. It also checks the complete code's life cycle of an application to avoid the security gaps in policy[16], [17].

III. Understanding Cryptography

A technique used to make data incomprehensible to an unauthorized person is called Cryptography. By doing so, confidentiality is guaranteed to genuine users [4]. On the other hand, The author in [6] stated that key area of concern in the acceptance of cloud is the security of the data in the cloud database server. There is need for a great degree of privacy and authentication. Cryptography is one of the essential techniques that can guarantee protection of data in a cloud database server. Cryptography offers various symmetric and asymmetric algorithms to ensure data security. According to [18], it was stated that encryption is the method of transforming normal text to unreadable format. Decryption is the method of transforming encrypted text to normal text in the readable format.

Classification of Cryptography

There are a number of algorithms used to encrypt text into cipher text, but these algorithms are not adequate because encryption is a very common practice for upholding information security. The growth of encryption is moving toward a future of unending prospects. Daily new encryption techniques are discovered [19].

The classification of well-known cryptographic techniques is shown in fig.1. below [20].

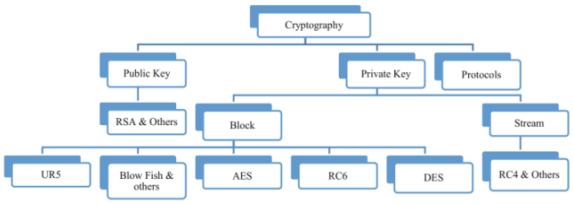

Figure 1: Classification of Cryptographic Algorithms [19]

This paper [20] stated that encryption algorithms can be categorized into two; Symmetric and Asymmetric key encryption. These algorithms are as shown in figure 2 and 3 respectively.

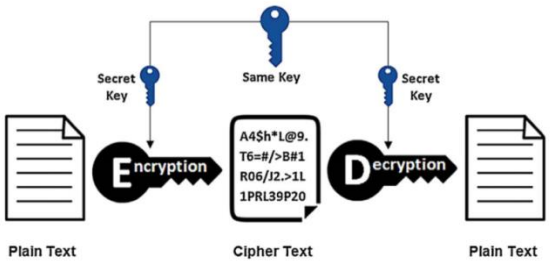

Figure 2: Symmetric Encryption [21],

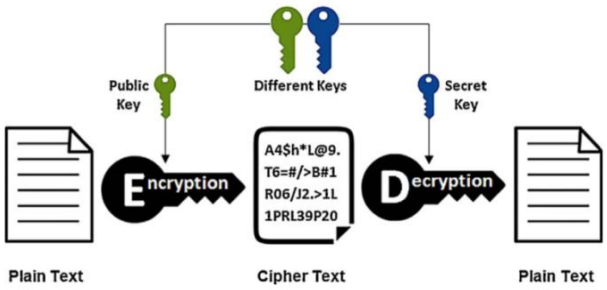

Figure 3: Asymmetric Encryption [21]

Purpose of Cryptography

According to [20], There a number of security goals that is provided cryptography to ensure the privacy of data, non-alteration of data and so on. Cryptography is widely used today because of its great security advantages. Following are the various goals of cryptography [18], [22].

i. Confidentiality: Data in computer is transmitted and only authorized party can access it.

ii. Authentication: The data received by any system has to check the identity of where it is coming from whether the data is received from an authorized person or a false identity.

iii. Integrity: Only the authorized party is permitted to alter the transmitted data.
iv. Non Repudiation: Guarantees that neither the sender, nor the receiver of message should be able to reject the communication.
v. Access Control: Only the authorized parties are able to access the given information.
vi. Service Reliability and Availability: Unsecure systems usually get attacked by intruders, which may affect their availability and type of service to their users. Therefore a system should be secure and provide a way to grant their users the quality of service they expect.

Comparisons of different Cryptographic Algorithms

[5] provides a comparative examination of encryption algorithm based on 14 factors. The Encryption techniques that were examined are AES, DES, 3DES, RSA and results are presented in Table 1.

Table 1 Comparison of encryption algorithms [5]

s/n	FACTOR	AES	DES	3DES	RSA
1	Algorithm type	Symmetric	Symmetric	Symmetric	Asymmetric
2	Encryption	Fast	Moderate	Slower	Slower
3	Decryption	Fast	Moderate	Slower	Slower
4	Key length in bits	128,192 & 256	56	56,112 or 168	1024 or greater
5	Block size in bits	128	64	64	512 or more
6	No. of rounds	10,12 & 14	16	16	1
7	Key used	Same for both encode and decode data	Same for both encrypt and decrypt data	Three different keys to encrypt, decrypt and again encrypt	Different keys to encrypt and decrypt data
8	Key for Ciphering and deciphering	Uses Same key	Uses Same key	3 different keys	Different
9	Algorithm for Ciphering and deciphering	Uses Different Algorithm	Uses Different Algorithm	Uses Different algorithm	Uses Same algorithm
10	Algorithm scalability	Not scalable	Scalable	Scalable	Not scalable
11	Security	Higher security	Not secure	Effective Security	Less security
12	Vulnerability	BFA (Brute Forced Attack)	BFA, Linear & differential cryptanalysis attack	BFA, sweet32 attack	BFA and Oracle attack
13	Speed of simulation	Faster	Faster	Faster	Faster
14	H/w and S/w Implementation	Fast implementation	As compared to software better in hardware implementation	Efficient in hardware but not in software	Not efficient

IV. Related Works

In a study on security in mobile cloud applications this paper [23] stated that the services provider proposed answers for matters in the Cloud. These security complications regarding data transmission are answered by service providers by means of security protocols such as SSL/HTTPS. However, this kind of protocols are high energy consuming on one hand and offer security properties on a second hand as a block without taking into consideration the type of data transmitted or the user anticipations. The framework that was proposed by the researcher was able to secure the data transferred between the elements of the same mobile cloud application; and to guarantee the integrity of the applications at the time of installation on the device and when being updated. According to [24], the author presented Secure Application INTteraction (SAINT), this is an improved structure that manages install-time approval tasks. Additionally, [25] proposed a security model for location-based services(LBS) using outsourced database(ODB) and reveal how to use distributed storage and international mobile subscriber identity (IMSI) as user identification to ensure location of data is secured. Apart from that, it strengthened privacy and authentication.

In another study by [26], a distributed security infrastructure for mobile agents were described. The first feature of the infrastructure is believable; this means that mechanisms are provided for authenticating information furnished by an agent. A second security property is survivable. What this means is that a mobile agent can be programmed to withstand different attacks by malicious hosts on each individual agents; this is achieved through encryption as well as agent replication and voting. The major feature of the infrastructure is that mobile agents are themselves used to enforce the security properties. Furthermore, The author in [27] proposed a security framework for mobile agent systems. This work was initiated by a strict conceptual forming of mobile agent systems, which shows the most important ideas for mobile agent system and thus unifies their image and defines the associations concerning them.

A study by [28] evaluated the mobile operating systems of two giant technology providers Apple and Google and concluded that they are almost similar in terms of technology. But, android has a few hitches, which are signing process, permission system problem in case of social engineering and fast vetting process. For IOS, these worries are handled very well. Specially that App store is the only place where to download app. This paper [29] detailed a study of android users in trying to shed light on how users see the risks linked with app permissions and in-built adware. There were several questions given in a web study, with results representing exciting differences between males and females in installation conduct and approaches to security.

According to [30], security weaknesses of the Android system poses risk to safe mobile use of users. In an event of serious flaws, there may even be property harms. A study by [31] suggested that though it is very problematic to offer comprehensive security in android devices, there are safe and secured way to use smart devices positively to circumvent misuse by hackers. The researcher further explained that these days private and delicate data is kept on smart devices for quick access. There is more need to take mobile security extra seriously as there is growing usage of internet and mobile devices. Therefore, everyone's priority should be to understand security and protection of data. In a study by [1], the insights in android security enforcement tools, threats to the prevailing security enforcement and associated matters, malware development timeline between 2010-2014, craftiness

mechanisms used by the malware authors were indicated. An insight into the strengths and shortcomings of the known research methodologies was also given.

In the study related to android, the author in [32] stated that whereas the Android message passing system upholds the making of rich, interactive applications, it also brings about the likelihood for attack especially if developers do not take safety measures. Android Inter-application communication were examined and presented several classes of possible attacks on applications. Exiting transmission could put a mobile application at risk of transmission theft. On the other hand, incoming communication can put an application at risk of malicious doings and Transmission injection. A tool called comdroid can be used by most developers to analyze their own applications before they are released, by application reviewers to analyze applications in the Android Market, and by end users [33]. This author analyzed 100 applications and proved the results by hand with 20 of those applications. Of the 20 applications, 12 applications were recognized with one susceptibility each. This shows that applications can be susceptible to attack and that developers should take extra precautions. Some vulnerabilities are due to user unfamiliarity of diverse settings that are present in android devices [31] [34].

In a study on comparative investigation of several encryption algorithms for data transmission, the author in [35], analyzed the performance metrics of encryption algorithm bearing in mind the following factors like time to compute, memory utilized and number of Bytes output. The results from the simulation showed the comparison of three encryption techniques which are AES, DES and RSA with same text file for five experiments, number of Bytes output for AES and DES is identical for different text file sizes. It was noticed that the RSA has a very smaller number of Bytes output compared to AES and DES algorithm. The time taken by RSA is greater compared to the time taken by AES and DES. Based on the used text files and the simulation results obtained, it was settled that DES algorithm takes least encryption time and AES algorithm has least memory utilization while encryption time is very small in case of AES and DES algorithm. RSA takes the greatest encryption time and memory utilization is also very high but number of Bytes output is least when it comes to RSA algorithm. Additionally, the author in [36] gives a detailed study on symmetric key encryption such as DES, 3DES, AES, and Blowfish. It was resolved that private key encryption run faster than public key encryption techniques such as RSA etc. and the memory necessity of private key encryption is lesser than public key encryption algorithms. Furthermore, it was indicated that the security side of private key encryption is greater than public key encryption. Similarly, in [37] focused on two frequently used private key encryption such as Blowfish and AES. These methods were compared and their performance was assessed. The results from the investigations were given to establish the performance of these methods. In addition to that, this paper [38] provided a comprehensive performance comparison between four mostly used encryption techniques: DES, 3DES, AES, and Blowfish. The contrasts were carried out by running several different settings to process different sizes of information blocks in order to assess the algorithm's encryption and decryption speed. The simulation setup was in C# programming language. The outcomes from this paper showed that blowfish is better in terms of performance when compared to the rest of encryption methods.

A study by [39] concluded that most symmetric algorithms have high encryption ration. Using A5 variations is better when developing Stream Cipher. In Asymmetric algorithm, RSA appears to be better whereas in symmetric algorithms AES appears to be better. The researcher further noted that Blowfish and RC variations were found to be susceptible in comparison to others, while Twofish and Threefish were found less secure in contrast to AES.

In another study by [40], two most extensively used symmetric encryption techniques were compared i.e. data encryption standard (DES) and advanced encryption standard (AES). The factors that were looked at were avalanche effect due to one bit variation in plaintext keeping the key unchanged, memory needed when implementing and simulation time necessary for encryption. The property of any encryption algorithm where a minimal change in either the key or the plaintext should give a noteworthy change in the cipher text is known as avalanche effect.

AES has high avalanche effect compared to DES, whereas memory needed and simulation time for DES is greater than that of AES, which clearly represents that AES is better than DES. The ideal encryption technique for messages exchanged between objects through chat-channels, and is beneficial for objects that encompass monetary transactions is AES.

It was stated by [18] that AES encryption is flexible and scalable and it is the fastest encryption method. AES is also easier implement. It was further explained by [6], that the needed memory for AES algorithm is less compared to other symmetric algorithms like DES, 3DES and blowfish. According to [41], The level of security in AES is very high because it uses 128, 192 or 256-bit key in the algorithm. The author in [5] indicated that AES displays resistance against a variety of attacks. Because of this, AES is a considered a highly protected encryption method. Apart from that, this paper [42] stated that AES has been designed to work swiftly and competently in both software and hardware and also cater for small devices such as smart phones. AES will offer extra security in the long run because of a large block size and a longer key that it uses. It was further stated by [6] that unlike other symmetric encryption methods, AES encryption algorithm has no weaknesses and limitations despite having a minimal storage space and high performance.

On the other hand, this paper [41] presented the insights on Data Encryption Standard (DES), as one of the extensively recognized, openly available methods. According to [43] 3DES was developed to address the identified faults in DES without forming the entire new cryptosystem. DES uses a 56-bit key which is not sufficient to encrypt sensitive information of users

or organizations. A study by [5] stated that 3DES makes use of a 3 key set in EDE (Encrypt-Decrypt-Encrypt) mode. In 3DES, the key length is extended by using the algorithm 3 times resulting in a key size of 168 bit long, which is 3 times of 56. A three 64 bit keys is used which are as follows K1, K2, K3. The K1 key is used for encrypting the data, K2 key is utilized to decrypt the data and the K3 key is used for again encrypt the data.

In a study by [44], it was settled that AES is faster and more proficient compared to other encryption methods. There is a minor difference in performance of several symmetric key methods when considering the transmission of data. Even in circumstances involving data transmission, AES would be appropriate especially in cases where the encrypted data is kept at the other end and decrypted several times. Another study by [45] discussed the key advantages of AES with respect to DES. It was indicated that AES can be easily implemented in high level or low level languages.

According to [46], it was stated that both Symmetric and Asymmetric Key algorithms are very much efficient in securing the transmitted information over any communication channels. The author highlighted the simple and proposed algorithms related to these cryptographic techniques. In Symmetric Key Cryptography, a single key is used for both encryption and decryption purposes. On the other hand, Asymmetric Key Cryptography uses two separate keys to prevent any unethical access to the data. The public key remains public and the private key is not shared. There is better security in this technique than the former. Moreover, Asymmetric Key Cryptography offers high information confidentiality and non-repudiation because of the use of Digital Signatures. However, Symmetric Key Cryptography is broadly used because of its straightforwardness.

V. Research Methodology

This chapter is devoted to a discussion of methodological aspects including simulation approaches that were adopted and implemented in the study.

Computer simulation involves running the executable simulation model and carrying out several experiments by changing the parameters. The resultant data can then be likened with both theoretical and empirical investigations. This is the primary phase in creating new study understandings that will help advance current concepts and finally create fresh ones [47]. According to [48], the drive of simulation is to well comprehend an exciting occurrence, such as the technology dispersion process, in order to foresee variables of interest. In the same vein, [49] indicated that simulation permits modelers and owners of problems to gain better insights of difficult systems as it allows them to evaluate the problems from different scopes.

Additionally, the author in [50] stated that simulation aids to attain a comprehensive picture of the actual problem and there is more precision in the problem representation and result.

A study by [51] emphasizes the value of simulation for learning not only by using the model, but also by creating a model. How the creation process supports an understanding of models being representations of systems was also stressed.

Research Design

When developing a model, there is need to meet a particular use and be as simple as possible. A simulation model is a structural model, what this means is that a model has logical and causal associations that happen in the systems. Simulation model development is an iterative procedure where a number of forms of a model are developed prior to attaining a usable model [52]. Figure 4 below shows several steps involved in simulation method.

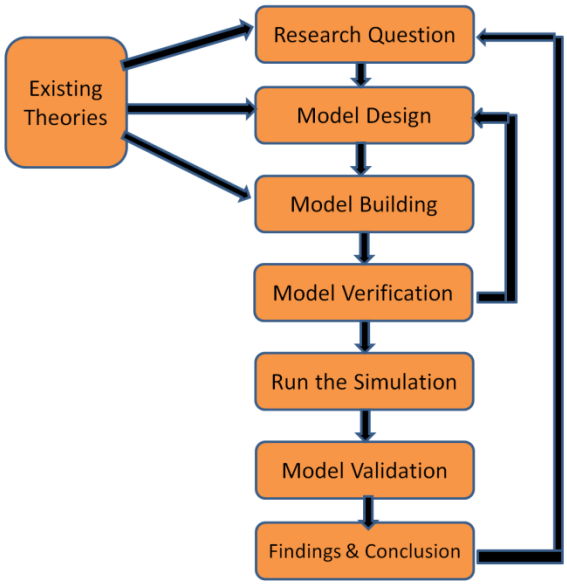

Figure 4: Simulation Steps

Research Questions

This research identified specific research questions that were appropriate for study by simulation. A Literature review was carried out in order to identify the gaps and help come up with questions for the research. The identified research questions were as follows.

i. To what extents are mobile application systems exposed to security threats and attacks?
ii. How can security in mobile application systems be addressed?
iii. How can we assess and evaluate the security framework for mobile applications?

Model Design

The requirement of a suitable objective to be made in the simulation and the choice of a suitable simulation approach is referred to as model design. There are several different simulation techniques that can be used; all these can be determined by the issue being probed. Model design will comprise of some literature survey to help in coming up with

the factors for the model and the original settings for the simulation.

Model Building

This involves constructing the simulation model. There are several existing software programs that can be used to support exact simulation approaches. This research used Progress telerik fiddler tool for running the simulations.

Model Verification

Verification is basically the debugging of the system to ensure that the model being built is working correctly. This is achieved by performing the simulation and testing whether model is working correctly. Any errors encountered during the simulation should be corrected.

Developing a usable simulation model is an iterative process which involves a number of versions of a model to be developed prior to attaining a complete model.

In efforts trying to verify the model, several different tests were carried out both on the program to be used on android side (java code) and the one to be used on the server side (C# code). The same meter number was used and encrypted in both programs which gave the same ciphertext and plaintext, indicating that the both programs were suitable for the simulation. This is highlighted in figure 5 and 6 below.

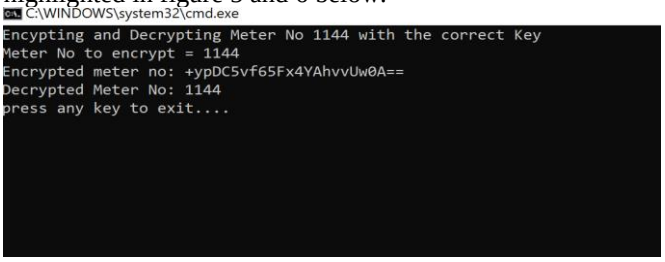

Figure 5: Encrypting and Decrypting of Meter No. 1144 in C#

```
run:
Encrypting and Decrypting Meter No
Meter No to Encrypt::    1144
Encrypted Meter No::     +ypDC5vf65Fx4YAhvvUw0A==
Decrypted Meter No::     1144
BUILD SUCCESSFUL (total time: 0 seconds)
```

Figure 6: Encrypting and Decrypting of Meter No. 1144 in java

Run the Simulation

According to [53], Simulations can be contemplated as a virtual experiment in which a sequence of experiments can be ran under diverse settings that can be varied as required. In addition to that, [54] identified five elements to these kind of experiments: the initial conditions being, the structure of time, outcome size, the total iterations made and any disparity in model parameters. Variation permits different norms to be tested in order to provide answers to the research questions and also to test the models sensitivity to alterations in parameters. The Screen shot below show the results obtained from Progress Telerik fiddler after running the unencrypted and encrypted algorithms in the mobile application.

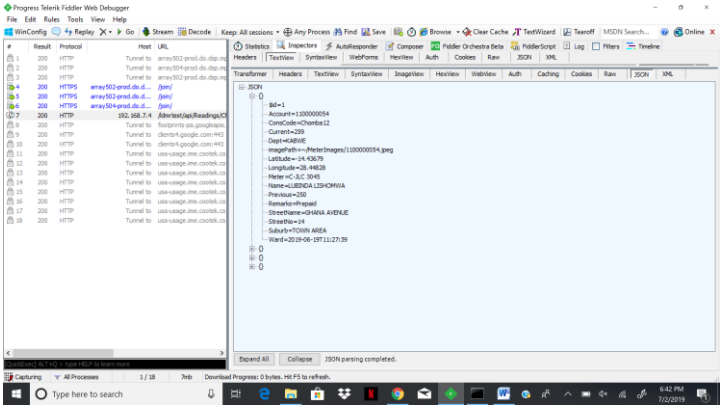

Figure 7: Sample generated unencrypted meter readings.

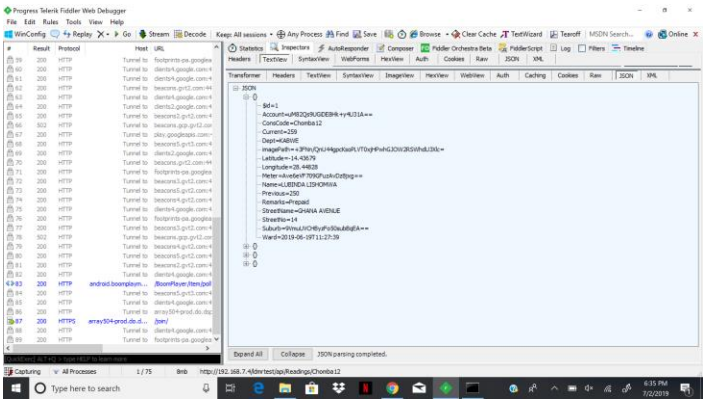

Figure 8: Sample generated encrypted meter readings.

The results shown in figure 7 and 8 above represents a sample of information obtained after running the simulation on an unencrypted and encrypted mobile application.

Model Validation

Validation of any simulation model is a crucial task. Model validation is defined as the confirmation that a computerized model within its domain meets a satisfactory range of accuracy consistent with the planned use of the model. The process of instituting whether the simulation model's output has met the required model's intended cause over the domain of the model's planned applicability is called validation. Validation testing and evaluation process are carried out here. Since simulation is utilized in model validation, any lacks found may be due to what was developed in any of the stages that involved when developing the simulation model including developing the system's theories [52].

In order to validate our model, the following setup was built in which fiddler was installed on a windows machine to act as

Man-in-the Middle to capture traffic and intercept data being transferred from mobile application. The mobile app was installed on an Android phone.

Step by step procedure is given below:

i. Install fiddler on the windows machine and connect that machine to DSL modem.
ii. Connect the Android phone with an installed application to the same DSL modem.
iii. Configure the proxy settings on the Android Phone with network settings on the windows machine.
iv. Start fiddler on windows machine. Now all traffic of the android phone is routed through windows machine.
v. Launch the mobile application from the android phone to upload meter readings and communicate with the server. The application included both the encrypted and decrypted version.
vi. Traffic was captured on windows machine and analyzed.

These steps were carried out with the setup shown in figure 9 below:

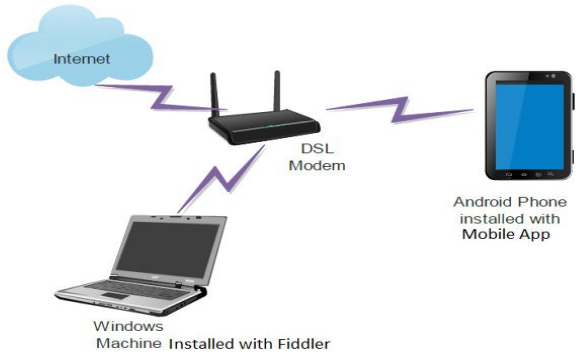

Figure 9: Network setup using fiddler as a proxy on windows machine

The following observations were made from the captured traffic.

i. All the meter reading details were showing when the unencrypted mobile application was installed on the application and used to upload readings.
ii. All the data in the fields (account number, image path, meter number and phone number) that have been encrypted using AES were in an unreadable format (ciphertext).

Validation Test

According to [55], validation itself is viewed as a process and an evidence for "building the right model". As for [56], validation is explained as a confirmation of conclusions drawn from simulations by independent observations. This is based on the use of empirical facts and logic. Additionally, [57] stated that how much to test or when to stop testing depends on how much confidence is needed with respect to the project objectives and requirements. The testing should continue until there is enough confidence in credibility and acceptability results. The sufficiency of the confidence is imposed by the intended uses. When developing of a simulation model it is always important to carry out validation tests [58] .

VI. Results

This Section presents the results that were generated from the simulation. Figure 10 shows the results obtained from fiddler after capturing and uploading readings using the unencrypted mobile application. It can be seen that all the data in the fields is in plain text and readable.

On the other hand, Figure 11 clearly shows the results obtained when the readings are captured and uploaded using the encrypted mobile application. AES encryption has been applied on four fields namely: Account number, image path, meter number and phone number. It can be seen that data in these fields is in an unreadable format (ciphertext). Figure 12 shows the result of AES encryption when applied on user passwords in SQL database.

Figure 13 shows unencrypted meter reading data generated from a web API, this data consist of four different customer details. Figure 14 shows the same data as in figure 13, but this time the meter reading data (account number, image path, meter number and phone number) that is generated from a web API is encrypted. This was successfully achieved after using an encrypted mobile application system.

It is always very vital to have insights regarding performance, strength and weakness of the algorithms in order to apply an appropriate cryptography algorithm to an application. In trying to choose an appropriate cryptographic algorithm, a number of different tests were carried out using a C# program to compare 3DES and AES in terms of encryption time and decryption time. The two algorithms were applied in C# using Visual Studio IDE. The text files used as input were of sizes 50kb, 1mb, 5mb and 10mb. Same input files were used throughout the experiment for all algorithms in order to properly compare. Same mode which is ECB was used for all algorithms. The results obtained from the experiment are shown in table 2 and 3 below, additionally; these results have been represented using a line chart and a bar chart to clearly show that AES takes less encryption and decryption time.

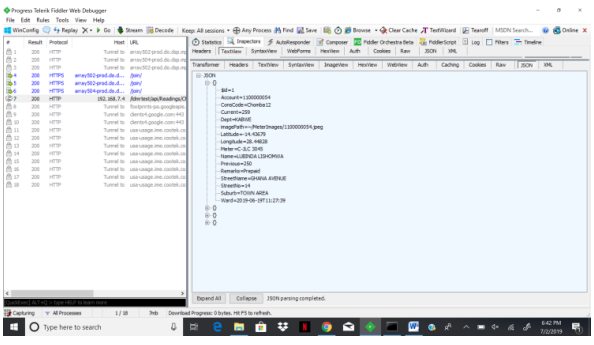

Figure 10: Result generated unencrypted meter readings.

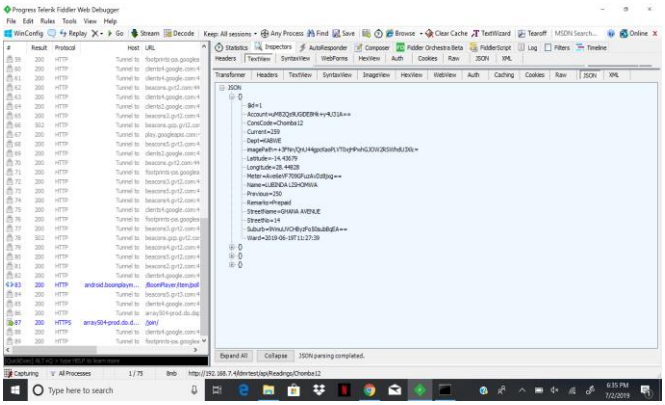

Figure 11: Result generated encrypted meter readings.

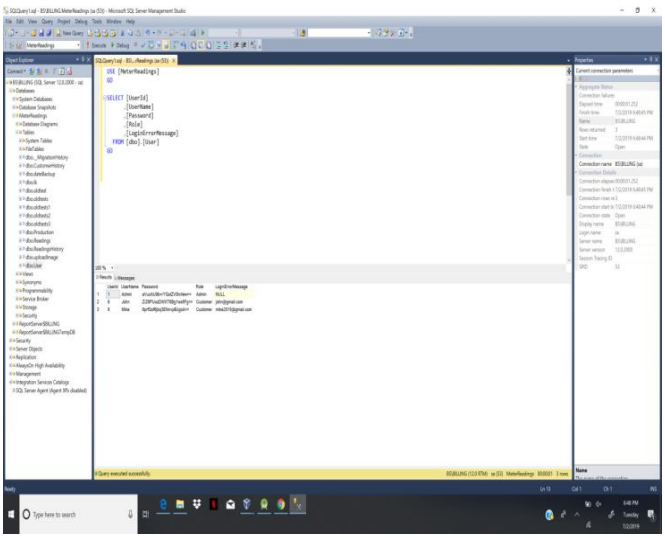

Figure 12 user passwords encrypted in the database.

[{"Sid":"1","Account":"1100000054","Current":259.0,"Previous":250.0,"Remarks":"Prepaid","Meter":"C-JLC 3045","StreetName":"GHANA AVENUE","StreetNo":"14","Dept":"KABWE","ConsCode":"Chomba12","Ward":"2019-06-19T11:27:39","Suburb":"TOWN AREA","Name":"LUBINDA LISHOMWA","Latitude":-14.43679,"Longitude":28.44828,"imagePath":"~/MeterImages/1100000054.jpeg"},

{"Sid":"2","Account":"1100000055","Current":918.0,"Previous":918.0,"Remarks":"Borehole","Meter":"07-011714","StreetName":"JAMESON AVENUE","StreetNo":"64","Dept":"KABWE","ConsCode":"Chomba12","Ward":"2019-06-20T09:32:36","Suburb":"TOWN AREA","Name":"JEFF RUTH","Latitude":-14.43894,"Longitude":28.453165,"imagePath":"~/MeterImages/1100000055.jpeg"},

{"Sid":"3","Account":"1100000787","Current":7783.0,"Previous":7652.0,"Remarks":"Active","Meter":"3687","StreetName":"MULUNGUSHI ROAD","StreetNo":"2","Dept":"KABWE","ConsCode":"Chomba12","Ward":"2019-06-21T12:41:34","Suburb":"TOWN AREA","Name":"LIFE TRUST","Latitude":-14.438035,"Longitude":28.451785,"imagePath":"~/MeterImages/1100000787.jpeg"},

{"Sid":"4","Account":"1100000788","Current":5250.0,"Previous":5230.0,"Remarks":"Active","Meter":"07-012587","StreetName":"PICKARD CRESCENT","StreetNo":"1","Dept":"KABWE","ConsCode":"Chomba12","Ward":"2019-06-23T09:47:15","Suburb":"TOWN AREA","Name":"DESAI M M","Latitude":-14.4405683,"Longitude":28.4594502,"imagePath":"~/MeterImages/1100000788.jpeg"}]

Figure 13: Unencrypted Meter readings generated from web API data

[{"Sid":"1","Account":"uM82Qs9UGiDE8Hk+y4U31A==","Current":259.0,"Previous":250.0,"Remarks":"Prepaid","Meter":"Avc6eVF709GFuzAvDz8jxg==","StreetName":"GHANA AVENUE","StreetNo":"14","Dept":"KABWE","ConsCode":"Chomba12","Ward":"2019-06-19T11:27:39","Suburb":"9VmuUVCHByzFo50subBqEA==","Name":"LUBINDA LISHOMWA","Latitude":-14.43679,"Longitude":28.44828,"imagePath":"+3FNn/QnU44gpcKsoPLVT0xjHPwhGJOW2RSWhdU3Xlc="},

{"Sid":"2","Account":"AbJ3bM2NrOcC21Mxz46w8w==","Current":918.0,"Previous":918.0,"Remarks":"Borehole","Meter":"yYjxjJkjnLbgYFVtQ9ofA==","StreetName":"JAMESON AVENUE","StreetNo":"64","Dept":"KABWE","ConsCode":"Chomba12","Ward":"2019-06-20T09:32:36","Suburb":"9VmuUVCHByzFo50subBqEA==","Name":"JEFF RUTH","Latitude":-14.43894,"Longitude":28.453165,"imagePath":"+3FNn/QnU44gpcKsoPLVT9JmE7PSZGAuvAh6U2VVh+k="},

{"Sid":"3","Account":"QEsJnOnhO++S9HQPLIKV/A==","Current":7783.0,"Previous":7652.0,"Remarks":"Active","Meter":"mJSF6ZM1+3410vuO8ADCQQ==","StreetName":"MULUNGUSHI ROAD","StreetNo":"2","Dept":"KABWE","ConsCode":"Chomba12","Ward":"2019-06-21T12:41:34","Suburb":"9VmuUVCHByzFo50subBqEA==","Name":"LIFE TRUST","Latitude":-14.438035,"Longitude":28.451785,"imagePath":"+3FNn/QnU44gpcKsoPLVT2yvF/bymwJPUCbBL8GRzWY="},

{"Sid":"4","Account":"YzhelprXnysylEFVISUSmg==","Current":5250.0,"Previous":5230.0,"Remarks":"Active","Meter":"m+cgaAci7vLzti3e+hQlng==","StreetName":"PICKARD CRESCENT","StreetNo":"1","Dept":"KABWE","ConsCode":"Chomba12","Ward":"2019-06-23T09:47:15","Suburb":"9VmuUVCHByzFo50subBqEA==","Name":"DESAI M M","Latitude":-14.4405683,"Longitude":28.4594502,"imagePath":"+3FNn/QnU44gpcKsoPLVTxwIC/+665vBF2GwFfp1uXo="}]

Figure 14: Encrypted Meter readings generated from web API data

Table 2 below shows text files of different sizes and their encryption and decryption time taken by 3DES algorithm in milliseconds.

Table 2: 3DES Encryption and Decryption time

Triple Data Encryption Standard (3DES)			
FILE SIZE	**Start Time (ms)**	**End Time (ms)**	**Difference (ms)**
10mb	345	800	455
5mb	562	789	227
1mb	463	615	152
50kb	123	235	112

Table 3 below shows text files of different sizes and their encryption and decryption time taken by AES algorithm in milliseconds.

Table 3: AES Encryption and Decryption time

Advanced Encryption Standard (AES)			
FILE SIZE	**Start Time (ms)**	**End Time (ms)**	**Difference (ms)**
10mb	364	512	148
5mb	423	588	165
1mb	392	575	183
50kb	268	468	200

Figure 15 and figure 16 have been shown using line chart and bar chart respectively, these shows the time taken by AES and 3DES to encrypt and decrypt different text file sizes. The results obtained clearly shows that AES takes less encryption and decryption time on larger file sizes when compared to 3DES.

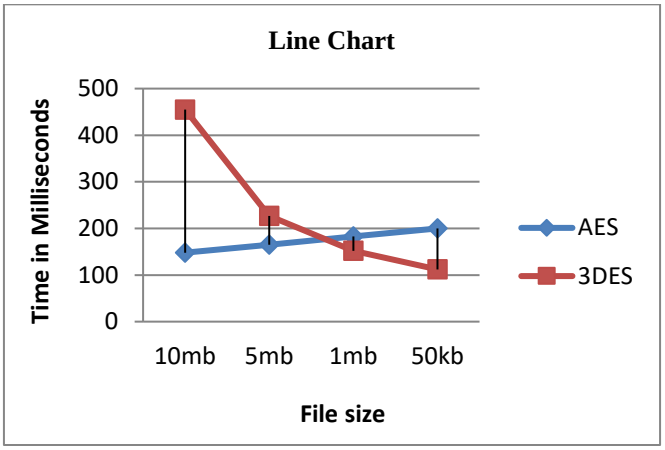

Figure 15: Line chart representing Encryption and Decryption time for files of different sizes

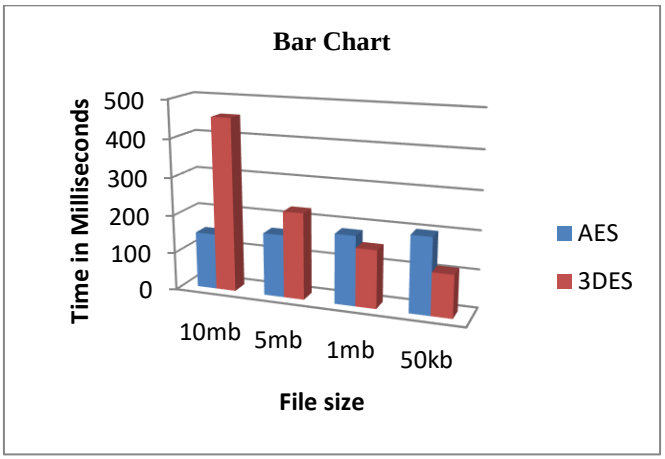

Figure 16: Bar chart representing Encryption and Decryption time for files of different sizes.

VII. Discussion

The main focus of this study was to develop a security framework for mobile application systems that is able to encrypt data transferred from the mobile phone to a server using AES encryption method. Several solutions that have been developed were presented, in trying to find solutions to the most important challenges of security and privacy of data being exchanged between mobile applications and servers. In view of this, a summary of our findings were presented from the carried out literature review, this further powered the relevance of this research into finding a solution that could work in most mobile application systems where there is data exchange between mobile apps and servers across communication channels.

This research employed the use of an established cryptographic algorithm in the development of a security framework for mobile application systems to protect data being transmitted, as this would improve a high degree of privacy and security of data. Advanced Encryption Standard (AES) was used. According to [59], this technique uses a number of replacements, ordering and transformation. Because of the strength that it has, AES was favored. Unlike 3DES and RSA, AES is firmly resistant to a lot of attacks. Based on the experimental result generated, it was concluded that AES algorithm takes less encryption and decryption time than 3DES. In 3DES the encryption process is prolonged than in AES, because same encryption process is repeated three times in 3DES [59]. A target file size of about 5 mb was being uploaded, hence the choice for using AES which is faster than 3DES on larger files. With RSA the encryption and decryption time is very high. Since RSA is an asymmetric key algorithm, it uses one way function which is not easy to invert using prime numbers. The use of modular exponentiation and other computations makes RSA slow compared to symmetric key algorithms. It is in this regard that AES was preferred.

This study designed a system that allows the users who are meter readers to transfer (upload readings) data between a smart phone and server database in a secure manner without facing the problem of data attack. Data being uploaded to the server is encrypted before it is transferred and decrypted once it reaches the server side; the whole idea behind this is to secure the data while being transmitted across networks, therefore, any access to the data that is unsanctioned will be rendered useless since every bit of information being transmitted is scrambled. As indicated by [60], the best technique for safeguarding the data that is being transferred is to apply encryption on data before the transmission and uploading process to ensure that the data remains protected against any authorized access at all times. This study further demonstrates that the usage of cryptographic techniques increases the security levels of encrypted mobile information.

This research would have been even more enlightening if the validation included even other mobile platforms like iOS, Windows, Symbian etc. However, with the results obtained from this research study, it is strongly felt that the developed framework can be used to protect and secure data in different mobile applications.

VIII. Conclusion

This research presented the challenges of security and privacy of data being exchanged between mobile applications and servers. Security of data is very important for applications where sensitive data is going through communication channels. Security of data is one key area in accepting mobile application systems. The designed security framework for mobile application addresses several challenges posed on meter readings data such as unauthorized access to data, data manipulation and data leakages. These security flaws do not only affect the business and reputation of the company using a mobile application but it can also lead to loss of data, for example vulnerabilities in an app can allow an attacker to intercept data being transferred and if data is not encrypted manipulations can easily be made on the data. This study made use of meter readings data, from the captured meter readings that were uploaded using the encrypted mobile application, AES encryption was applied on four fields namely: Account number, image path, meter number and phone number. It was

seen from the experimental results that data in these fields was in an unreadable format (ciphertext) indicating a successful encryption. The framework employed the use of AES cryptography which has a complex encryption process and has proven to be the best encryption method. The simulation results between 3DES and AES concluded that in terms of completing time, AES is faster. By applying this encryption technique, this study made sure that the security goals of data Confidentiality, Integrity and Availability (CIA) were met.

Future Work

As a future work, the security framework will further be tested on different mobile platforms. Hybrid cryptographic algorithms will be utilized to efficiently secure the data and information which is transmitted through systems. Several simulations will be carried out to assess and mitigate the vulnerabilities that are exploited by attackers on different mobile platforms such as stealing users' confidential information without their consent.

References

[1] P. Faruki *et al.*, "Android security: a survey of issues, malware penetration, and defenses," *IEEE Commun. Surv. Tutor.*, vol. 17, no. 2, pp. 998–1022, 2015.

[2] W. Enck, M. Ongtang, and P. McDaniel, "Understanding android security," *IEEE Secur. Priv.*, no. 1, pp. 50–57, 2009.

[3] N. D. Jorstad and T. S. Landgrave, "Cryptographic algorithm metrics," in *20th National Information Systems Security Conference*, 1997, pp. 1–38.

[4] P. Patil, P. Narayankar, D. G. Narayan, and S. M. Meena, "A comprehensive evaluation of cryptographic algorithms: DES, 3DES, AES, RSA and Blowfish," *Procedia Comput. Sci.*, vol. 78, pp. 617–624, 2016.

[5] J. Kaur, S. Sharma, and M. Tech, "Secure image sharing on cloud using cryptographic algorithms: survey," *Int J Future Revolut Comput Sci Commun Eng*, vol. 4, no. 2, pp. 319–325, 2018.

[6] V. R. Pancholi and B. P. Patel, "Enhancement of cloud computing security with secure data storage using AES," *Int. J. Innov. Res. Sci. Technol.*, vol. 2, no. 9, pp. 18–21, 2016.

[7] Y. Kumar, R. Munjal, and H. Sharma, "Comparison of symmetric and asymmetric cryptography with existing vulnerabilities and countermeasures," *Int. J. Comput. Sci. Manag. Stud.*, vol. 11, no. 03, 2011.

[8] M. N. A. Wahid, A. Ali, B. Esparham, and M. Marwan, "A Comparison of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish for Guessing Attacks Prevention," 2018.

[9] J. Ning, J. Xu, K. Liang, F. Zhang, and E.-C. Chang, "Passive attacks against searchable encryption," *IEEE Trans. Inf. Forensics Secur.*, vol. 14, no. 3, pp. 789–802, 2018.

[10] D. Kapetanovic, G. Zheng, and F. Rusek, "Physical layer security for massive MIMO: An overview on passive eavesdropping and active attacks," *ArXiv Prepr. ArXiv150407154*, 2015.

[11] Neal Leavitt, "Mobile Security: Finally a Serious Problem?," *IEEE Computer society*, 2011.

[12] P. Kumar, M. G. Singh, and V. P. Singh, "Analyzing Data Leakage Using Third Party Connections in Mobile Applications," PhD Thesis, 2015.

[13] R. Roman, J. Lopez, and M. Mambo, "Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges," *Future Gener. Comput. Syst.*, vol. 78, pp. 680–698, 2018.

[14] P. Kumar, M. G. Singh, and V. P. Singh, "Analyzing Data Leakage Using Third Party Connections in Mobile Applications," PhD Thesis, 2015.

[15] B. Schneier, *Secrets and lies: digital security in a networked world*. John Wiley & Sons, 2011.

[16] W. Enck, D. Octeau, P. D. McDaniel, and S. Chaudhuri, "A study of android application security.," in *USENIX security symposium*, 2011, vol. 2, p. 2.

[17] G. McGraw, "Software security," *IEEE Secur. Priv.*, vol. 2, no. 2, pp. 80–83, 2004.

[18] J. Thakur and N. Kumar, "DES, AES and Blowfish: Symmetric key cryptography algorithms simulation based performance analysis," *Int. J. Emerg. Technol. Adv. Eng.*, vol. 1, no. 2, pp. 6–12, 2011.

[19] P. Dixit, A. K. Gupta, M. C. Trivedi, and V. K. Yadav, "Traditional and Hybrid Encryption Techniques: A Survey," in *Networking Communication and Data Knowledge Engineering*, Springer, 2018, pp. 239–248.

[20] E. Thambiraja, G. Ramesh, and D. R. Umarani, "A survey on various most common encryption techniques," *Int. J. Adv. Res. Comput. Sci. Softw. Eng.*, vol. 2, no. 7, 2012.

[21] V. Lozupone, "Analyze encryption and public key infrastructure (PKI)," *Int. J. Inf. Manag.*, vol. 38, no. 1, pp. 42–44, 2018.

[22] Adedeji Kazeem B. & Ponnle Akinlolu.A, "A New Hybrid Data Encryption and Decryption Technique to Enhance Data Security in Communication Networks: Algorithm Development.," *Int. J. Sci. Eng. Res.*, vol. 5, 2014.

[23] D. Popa, M. Cremene, M. Borda, and K. Boudaoud, "A security framework for mobile cloud applications," in *Roedunet International Conference (RoEduNet), 2013 11th*, 2013, pp. 1–4.

[24] M. Ongtang, S. McLaughlin, W. Enck, and P. McDaniel, "Semantically rich application-centric security in Android," *Secur. Commun. Netw.*, vol. 5, no. 6, pp. 658–673, 2012.

[25] P.-Y. Chen, S.-M. Cheng, and K.-C. Chen, "Smart attacks in smart grid communication networks," *IEEE Commun. Mag.*, vol. 50, no. 8, 2012.

[26] C. Bryce, "A security framework for a mobile agent system," in *European Symposium on Research in Computer Security*, 2000, pp. 273–290.

[27] M. Loulou, M. Jmaiel, and M. Mosbah, "Dynamic security framework for mobile agent systems:

specification, verification and enforcement," *Int. J. Inf. Comput. Secur.*, vol. 3, no. 3/4, pp. 321–336, 2009.

[28] A. Hayran, M. İğdeli, A. YILMAZ, and C. Gemci, "Security Evaluation of IOS and Android," *Int. J. Appl. Math. Electron. Comput.*, vol. 4, no. Special Issue-1, pp. 258–261, 2016.

[29] G. Robinson and G. R. Weir, "Understanding android security," in *International Conference on Global Security, Safety, and Sustainability*, 2015, pp. 189–199.

[30] J.-K. Park and S.-Y. Choi, "Studying security weaknesses of android system," *Int. J. Secur. Its Appl.*, vol. 9, no. 3, pp. 7–12, 2015.

[31] P. P. Ghogare and M. P. Patil, "A Study of Security Awareness Among Android Users," *Int. J. Comput. Sci. Eng. Technol. IJCSET*, 2017.

[32] A. P. Felt, M. Finifter, E. Chin, S. Hanna, and D. Wagner, "A survey of mobile malware in the wild," in *Proceedings of the 1st ACM workshop on Security and privacy in smartphones and mobile devices*, 2011, pp. 3–14.

[33] E. Chin, A. P. Felt, K. Greenwood, and D. Wagner, "Analyzing inter-application communication in Android," in *Proceedings of the 9th international conference on Mobile systems, applications, and services*, 2011, pp. 239–252.

[34] T. I. Mamun and L. Alam, "Android Security Vulnerabilities Due to User Unawareness and Frameworks for Overcoming Those Vulnerabilities," *Int. J. Comput. Appl.*, vol. 137, no. 1, pp. 14–21, 2016.

[35] S. M. Seth and R. Mishra, "Comparative analysis of encryption algorithms for data communication 1," 2011.

[36] M. Agrawal and P. Mishra, "A comparative survey on symmetric key encryption techniques," *Int. J. Comput. Sci. Eng.*, vol. 4, no. 5, p. 877, 2012.

[37] M. A. Kumar and S. Karthikeyan, "Investigating the efficiency of Blowfish and Rejindael (AES) algorithms," *Int. J. Comput. Netw. Inf. Secur.*, vol. 4, no. 2, p. 22, 2012.

[38] A. A. Tamimi, *Performance Analysis of Data Encryption Algorithms. Retrieved October 1, 2008 Fromhttp*. 2008.

[39] N. Advani, C. Rathod, and A. M. Gonsai, "Comparative Study of Various Cryptographic Algorithms Used for Text, Image, and Video," in *Emerging Trends in Expert Applications and Security*, Springer, 2019, pp. 393–399.

[40] G. Singh, "A study of encryption algorithms (RSA, DES, 3DES and AES) for information security," *Int. J. Comput. Appl.*, vol. 67, no. 19, 2013.

[41] M. N. A. Wahid, A. Ali, B. Esparham, and M. Marwan, "A Comparison of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish for Guessing Attacks Prevention," *J. Comput. Sci. Appl. Inf. Technol.*, vol. 3, pp. 1–7, 2018.

[42] N. Aleisa, "A Comparison of the 3DES and AES Encryption Standards," *Int. J. Secur. Its Appl.*, vol. 9, no. 7, pp. 241–246, 2015.

[43] V. Subhashini and N. Geethanjali, "A New and Novel Study of Comparison on Cryptographic Algorithms using AES, DES and RSA for Network Security," *Int. J. Res.*, vol. 5, no. 21, pp. 634–644, 2018.

[44] S. A. Hirani, "Energy consumption of encryption schemes in wireless devices," PhD Thesis, University of Pittsburgh, 2003.

[45] N. Penchalaiah and R. Seshadri, "Effective Comparison and evaluation of DES and Rijndael Algorithm (AES)," *Int. J. Comput. Sci. Eng.*, vol. 2, no. 05, pp. 1641–1645, 2010.

[46] S. Chandra, S. Paira, S. S. Alam, and G. Sanyal, "A comparative survey of symmetric and asymmetric key cryptography," in *2014 International Conference on Electronics, Communication and Computational Engineering (ICECCE)*, 2014, pp. 83–93.

[47] M. Ihrig and K. G. Troitzsch, "An extended research framework for the simulation era," in *Proceedings of the Emerging M&S Applications in Industry & Academia/Modeling and Humanities Symposium*, 2013, p. 12.

[48] N. Gilbert and K. Troitzsch, *Simulation for the social scientist*. McGraw-Hill Education (UK), 2005.

[49] J. Zulkepli and T. Eldabi, "Towards a framework for conceptual model hybridization in healthcare," in *2015 Winter Simulation Conference (WSC)*, 2015, pp. 1597–1608.

[50] N. Mustafee, S. Brailsford, A. Djanatliev, T. Eldabi, M. Kunc, and A. Tolk, "Purpose and benefits of hybrid simulation: contributing to the convergence of its definition," in *2017 Winter Simulation Conference (WSC)*, 2017, pp. 1631–1645.

[51] I. Lorscheid, "Review of Simulation and Learning," 2016.

[52] R.G. Sargent, "AN INTRODUCTORY TUTORIAL ON VERIFICATION AND VALIDATION OF SIMULATION MODELS," *Proc. 2015 Winter Simul. Conf.*, 2015.

[53] J. P. Davis, K. M. Eisenhardt, and C. B. Bingham, "Developing theory through simulation methods," *Acad. Manage. Rev.*, vol. 32, no. 2, pp. 480–499, 2007.

[54] J. R. Harrison, Z. Lin, G. R. Carroll, and K. M. Carley, "Simulation modeling in organizational and management research," *Acad. Manage. Rev.*, vol. 32, no. 4, pp. 1229–1245, 2007.

[55] N. Tsioptsias, A. A. Tako, and S. Robinson, "Model validation and testing in simulation: a literature review," 2016.

[56] W. F. van Gunsteren *et al.*, "Validation of molecular simulation: an overview of issues," *Angew. Chem. Int. Ed.*, vol. 57, no. 4, pp. 884–902, 2018.

[57] O. Balci, "Golden rules of verification, validation, testing, and certification of modeling and simulation applications," *SCS MS Mag.*, vol. 4, no. 4, pp. 1–7, 2010.

[58] R. G. Sargent, "Verification and validation of simulation models," in *Proceedings of the 2010 Winter Simulation Conference*, 2010, pp. 166–183.

[59] N. Aleisa, "A Comparison of the 3DES and AES Encryption Standards," *Int. J. Secur. Its Appl.*, vol. 9, no. 7, pp. 241–246, 2015.

[60] Sakinah Ali, Sa Wail Abdo Ali Alhiage, and Farida Ridzuan, "Mobile Application Design for Protecting the Data in Cloud Using Enhanced Technique of Encryption," *Int. J. Eng. Technol.*, 2018.