# CHAPTER ONE

## **1.1 INTRODUCTION**

Currently, encryption is one of the most popular and effective data security methods used by organizations. The purpose of data encryption is to protect digital data confidentiality as it is stored on computer systems and transmitted using the internet or other computer networks. The project “Data Encryption for secure storage and transfer” uses Advanced Encryption Standards due to its strong encryption algorithm.

These algorithms provide confidentiality and drive key security initiatives including authentication, integrity, and non-repudiation. Authentication allows for the verification of a message’s origin, and integrity provides proof that a message’s contents have not changed since it was sent. Additionally, non-repudiation ensures that a message sender cannot deny sending the message.

This application will be able to allow people to share important documents among themselves without having to fear about security of the files due to the strong encryption algorithm used and sharing of the key only among themselves thus avoiding any form of attack.

## **1.2 PROBLEM DEFINITION**

The most basic method of attack on encryption today is brute force, or trying random keys until the right one is found. Of course, the length of the key determines the possible number of keys and affects the plausibility of this type of attack. It is important to keep in mind that encryption strength is directly proportional to key size, but as the key size increases so do the number of resources required to perform the computation.

AES uses key size of 128 bits thus making it hard for anyone without the key to decrypt the data. This will prevent any form of attack from brute force, side-channel attacks to cryptanalysis. The main priority of Data Encryption for Secure Storage and Transfer is to ensure that no data file can be decrypted in any way unless it is by the receiver and ensure that the transfer and storage of the data is secured.

## **1.3 OBJECTIVES**

## **GENERAL OBJECTIVE**

To create an offline Encryption application using AES algorithm which will be able to encrypt sensitive, important files, videos or images such as research, evidence etc. for secure storage in computers or hard disks and transfer across the internet.

## **SPECIFIC OBJECTIVES**

The system has a number of objectives as listed below;

1. To protect the confidentiality of digital data stored on computer systems or transmitted via the internet or other computer networks.
2. To analyze the existing encryption algorithm and applications.
3. To create an encryption algorithm that is easy to use but strong and efficient to both users’ hardware and software.
4. To develop an application that will make people encrypt their data before storing or sharing them.
5. To ensure that the application is accessible to anyone who wishes to secure their data.

## **1.4 SCOPE OF THE PROJECT**

The system can be used by anyone since it is an offline application regardless of where the person might be as long as they have the key. The data encryption application can be used to encrypt any size of data whether large or small since it does not have size limitations. During encryption the user will be required to choose the data file to encrypt and enter the encryption key. This system is platform independent hence runs on both Linux and Windows platforms.

## **1.5 LIMITATIONS OF THE PROJECT**

1. There is no guarantee that the methods of attack on the encrypted data such as brute force will not succeed.
2. In case the encrypted data is damaged or tampered with, there is no assurance that it will be decrypted successfully.
3. The application can only be run on a computer or laptop which are compatible with the application.
4. The system has limited accessibility as screen readers can have difficulties using it.

## **1.6 BENEFITS OF THE PROJECT**

1. This system will provide all security check ups which can be performed during encryption and decryption of documents.
2. Its strong bit encryption algorithm will make sure that others will not be able to hack or change the file/data attributes.
3. It ensures guaranteed access to encrypted data by authorized users by automating storage back-up for critical master encryption keys.
4. Data encryption guarantees data integrity.
5. It helps the encrypted data to be transmitted securely
6. Data encryption provides confidence that your encrypted data backups are safe.

**2.0 CHAPTER TWO**

**2.1 Literature Review**

Data Encryption provides the ability to encrypt data both for transmission over non-secure networks and for storage on media. The flexibility of key management schemes makes data encryption useful in a wide variety of configurations. Covered data must be encrypted when transmitted across networks to protect against eavesdropping of network traffic by unauthorized users. In cases where source and target endpoint devices are within the same protected subnet, covered data transmission must still be encrypted as recommended below due to the potential for high negative impact of a covered data breach.  The types of transmission may include client-to-server, server-to-server communication, as well as any data transfer between core systems and third party systems.

Without data encryption all digital data, including Blue Ray, can be retrieved no matter the format. Tapes offer no encryption.

While Mac and Windows are offering software utilities by default to encrypt entire hard disks and drives (File Vault and Bitlocker, respectively), there have been known vulnerabilities in both. Generally, many security experts have found that these default hard disk encryption tools are not fool proof, and can be cracked.

AES was published as FIPS PUB 197 [NIST (2001)], intended to replace the DES for commercial applications. AES was selected by a public competition. Though all of the six finalists were judged to be sufficiently secure for AES, the final choice for AES was Rijndael based on the three selection criteria: security, cost, and algorithm characteristics. Rijndael [Daemen (2002)] uses a 128-bit block size and supports 128, 192, and 256 bit keys. It is not based on feistel cipher structure like DES, Blowfish and other symmetric block ciphers, rather based on the Square cipher that uses S-boxes (substitution), shifting, and XOR operations.

AES has been adopted by the U.S. government and is now used worldwide. It supersedes the Data Encryption Standard (DES), which was published in 1977. The algorithm described by AES is a symmetric-key algorithm, meaning the same key is used for both encrypting and decrypting the data;

In the United States, AES was announced by the NIST as U.S. FIPS PUB 197 (FIPS 197) on November 26, 2001. This announcement followed a five-year standardization process in which fifteen competing designs were presented and evaluated, before the Rijndael cipher was selected as the most suitable;

AES became effective as a federal government standard on May 26, 2002 after approval by the Secretary of Commerce. AES is included in the ISO/IEC 18033-3 standard. AES is available in many different encryption packages, and is the first (and only) publicly accessible cipher approved by the National Security Agency (NSA) for top secret information when used in an NSA approved cryptographic module.

# 3.0 CHAPTER THREE

# 3.1 PROJECT PLANNING AND METHODOLOGY

## **Introduction**

Software development and designing undergoes a cycle that is well defined in the Software Engineering Industry. This life cycle is referred to as SDLC (Software Development Life Cycle).

This cycle constitutes a series of processes which are steps to be followed during development of any software. This steps are key – best software engineering practices which help a developer output an elegant system which achieves the objectives stated since it shortens that curve.

SDL has a number of methodologies that will be a choice of the developer based on how robust the software in question is. These include Incremental model, Spiral model, Prototyping and others like Waterfall model. In the problem analysis phase, the existing system will be studied by collecting factual information from the system users concerning the business and the perceived problems, causes and effects. From all this information, better understanding of the existing system's problems will be gained.

In the development of the Data Encryption for Secure Storage and Transfer I choose to use Incremental model.

.

## **3.2 METHODOLOGY**

Incremental model has been used as the methodology. The incremental model combines elements of the linear sequential model (applied repetitively) with the iterative philosophy of prototyping. The incremental model applies linear sequences in a staggered fashion as calendar time progresses. Each linear sequence produces a deliverable “increment” of the software. The system was broken down into modules. During the initial module development, an initial version of the system was developed. Each module passed through the requirements, design, implementation and testing phases. A working version of software was produced during the first module, so you have working software early on during the software life cycle. Each subsequent release of the module adds function to the previous release. The process continues till the complete system is achieved.



Figure 1.0: Incremental model design.

**Advantages of Incremental Model:**

1. Generates working software quickly and early during the software life cycle.
2. This model is more flexible – less costly to change scope and requirements.
3. It is easier to test and debug during a smaller iteration.
4. In this model customer can respond to each built.
5. Lowers initial delivery cost.
6. Easier to manage risk because risky pieces are identified and handled during it’d iteration.

**Disadvantages of Incremental Model**:

1. Needs good planning and design.
2. Needs a clear and complete definition of the whole system before it can be broken down and built incrementally.

## **3.3 FEASIBILITY STUDY**

Feasibility was conducted to identify the best encryption application that can encrypt both files, videos and images thus making it efficient to its users. This included an identification description, an evaluation of the proposed application and selection of the best encryption algorithm that can be used to encrypt all the data files.

The requirements of the applications were specified with a set of constraints such as the objectives of the application and the description of the outputs. The data collection was done using Interviews and Questionnaires.

## **3.4 SYSTEM REQUIREMENTS**

The study of specification of the requirements is very essential since it’s the primary goal of the system analyst to improve the efficiency of the existing system for the development of the new system, a preliminary survey of the existing applications was conducted. Investigation done whether the upgrading of the system into an application program could solve the problems and eradicate the inefficiency of the existing system.

## **Project Facilities Requirement**

## **3.4.1 Software Requirement**

The software requirement for developing the system consists of development platform, development tools, database management system and others software.

**Development Platform**

For my application I choose Windows 8.1, NetBeans 8.0.2 IDE, as my development environment because collectively they offered many features and advantages such as reliability, easy to use, and high performance that suite the needs of the project.

**Development Language**

For the client side, I used Java as my development language because it is secure hence hard to be compromised. I also used several Java libraries e.g. mysql-connector-java-5.1.23.

**Database Management System**

On the server side which is the database, I used MySQL (XAMPP) as the database system because it is a multi- user, multithreaded server that uses SQL to interact with and manipulate data. It is the most popular open source SQL database.

## 

## **3.4.2 Hardware Requirement**

The minimum hardware requirements for my system include;

Intel core i3 or higher processor

M2GB and above RAM

2.3GHz processor

250GB and above hard disk.

# CHAPTER FOUR

* 1. **SOFTWARE DESIGN**

## **4.2 DATABASE DESIGN**

Database is an integrated collection of data. These database files are the key source of information into the system. The main objective of database systems is to store information of users who can login into the application. The overall objective in the development of database is for the authentication of the application users before they can login. Database Management Systems (DBMS) allow data to be protected and organized separately from other resources. Below is the tables I used in my project. I used one table to store users’ information which is connected to the application using the java connector.

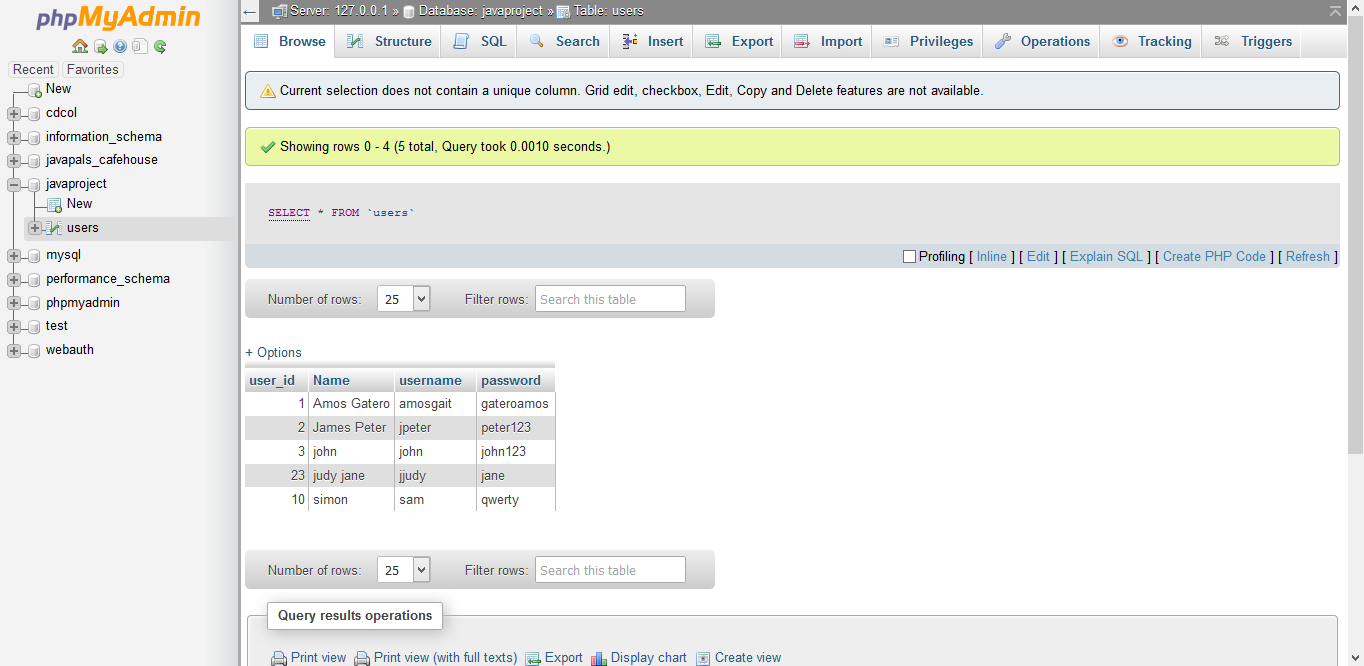
****

Figure 3.0: javaprojects’ database tables.

## **4.3 INTERFACE DESIGN**

It involves documenting the current user interface and the various elements needed to fulfill the user requirements. The images of the user interface pages are included to demonstrate the application’s look and feel.

Description of complete user interface specification:

Java Connector

After running the application, it must establish a connection first with the database before proceeding.

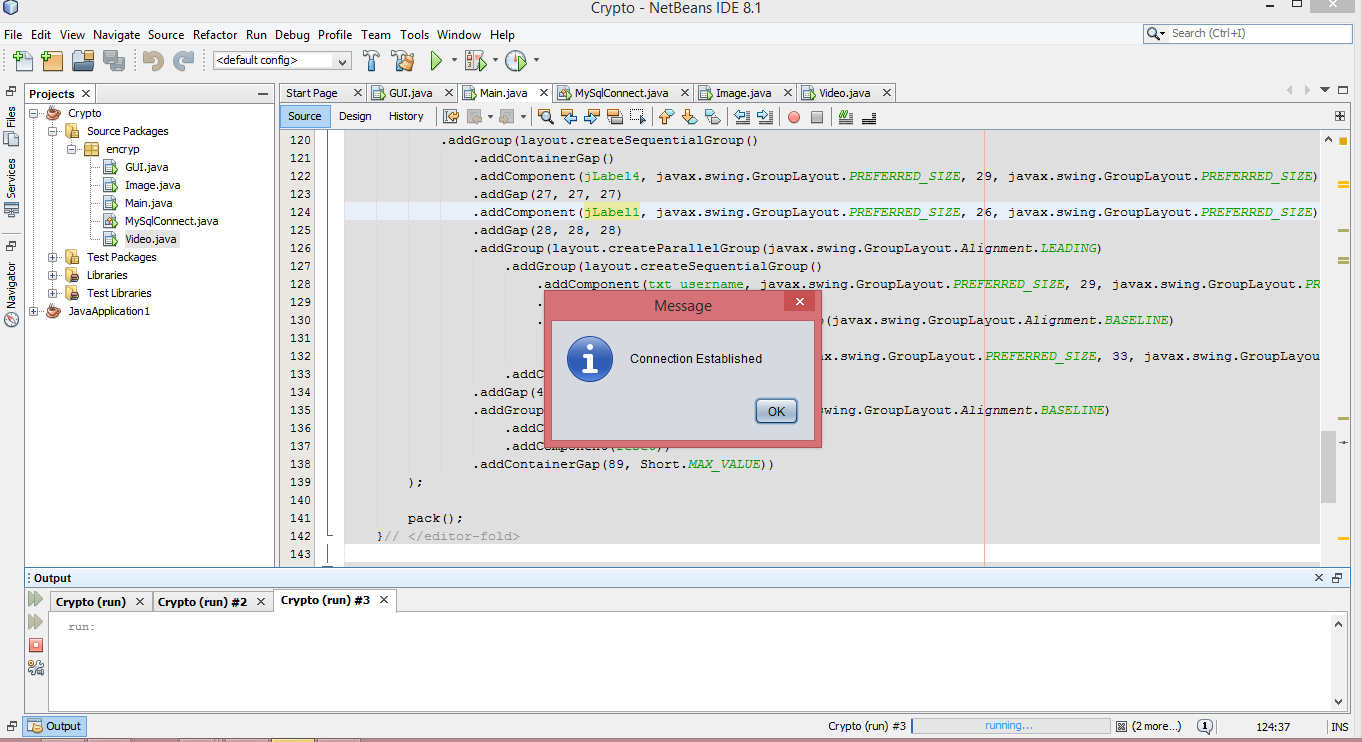


Figure 4.0: Connection Established with the Database.

The Login JFrame:

The main screen will contain the login page as shown in the figure below. The login JFrame consists of the User login section. They consist of two text boxes-username and password. The user cannot login unless the username and password matches the ones in the database table. The user login leads to the file encryption jframe.



Figure 5.0: Login JFrame

How the user interface behaves:

When a user input his/her username and password he/she must be authenticated before access is granted to the various sections. An error message is issued when the user enters the wrong username or password otherwise the user is allowed to gain access to the sections that they are privileged to use.

## **File Encryption and Decryption JFrame**

After Logging in the user is taken to the file encryption and decryption interface where the user can encrypt or decrypt different types of files which include word documents, PowerPoints and pdfs.

The interface has different parts which are:-

1. The browse button which is used to choose the file to be encrypted/decrypted.
2. The JText field for entering the encryption key.
3. The encryption and decryption buttons for the encryption and decryption of the plain text and cipher text respectively.

Below is a JFrame which shows the file encryption and decryption interface.



Figure 6.0: File encryption JFrame

Below is a JFrame which shows after the file has been chosen and encrypted.



Figure 7.0: JOptionPane showing data encrypted successfully

Below is a JFrame which shows image encryption and decryption

****

Figure 8.0: image encryption JFrame

Below is a JFrame which shows video encryption and decryption

****

Figure 8.0: video encryption JFrame

For each data encryption interface we have file, image and video encryption and decryption in which each interface performs its function separately.

After the data has been encrypted the name of the file encrypted changes. E.g.

1. For a video e.g. video.Mp4 it changes to encrypt.Mp4
2. If it is a document file i.e. Document.ppt/pdf it changes to encrypt .ppt/pdf.
3. For an image file i.e. image.jpg it changes to encrypt.jpg

When the files are decrypted they will change from encrypt to decrypted file which can be open and viewed just like the original ones.

**4.4 DATA STORAGE AND TRANSFER (Encrypted)**

After the data i.e. video, image or files have been successfully encrypted they can then be stored securely in the computers’ hard disk since they cannot be accessed by any unauthorized persons. This will help very much in in securing those sensitive and very important files that are not supposed to be accessed.

The encrypted files can also be stored into the clouds thus making it accessible at any time and place. Even though cloud have their own encryptions to protect the files being stored in the cloud it would be better if the individual storing the file encrypt it by himself first.

After encrypting the data, the encrypted data can also be shared to someone else either across the internet or using flash drives or external disk. The only thing the receiver will be required to have is the encryption key which s/he will use to decipher the encrypted data once received. The key should not be shared publicly to avoid any sought of attack.

## **4.5 SYSTEM IMPLEMENTATION**

Implementation involves converting a system specification into an executable system. It involves a consideration of strategies that are to be adopted by the user during system operation and the practical tasks.

**Operational and Testing Environments**

1. **Test environment**

I conducted my testing procedures by following the methodology that I uses-incremental model. Where I tested the functionality of each module after finishing to code it so as to add to the previous module sequentially until the whole application was tested. This is in order to avoid recurring errors all through the system. Actually I did do much debugging at the end as I had done most of it during my initial testing phases.

1. **Operational environment**

The system will run on desktops and will require internet connection for the purpose of sharing the encrypted files with others across the internet. All the users will access the system using a graphical user interface (GUI).

# 5.0 CHAPTER FIVE

### **5.1 CHALLENGES, RECOMMENDATIONS AND CONCLUSION**

## **5.2 CHALLENGES**

There were a lot of challenges during the project activity. Below are a few of them;

**Resources constraint**

The nature of the project dictated a lot with respect to its monetary demands. A lot of resources were required e.g. buying internet bundles, doing some research across the internet among other needs that could go beyond the financial stature of a student thus posing a major challenge.

**Time constraint**

The research involved a lot of undertakings such as reading, internet activities, analyzing data, system designing, coding, testing and documentation. With a lot of pressure from the assessing board the time allocated for the project completion was not enough.

**Difficulty in Choosing the Correct Encryption Algorithm**

There are many encryption algorithms which are used e.g. DES, Triple DES, AES among others. It was difficult to choose the right algorithm since all of them are widely used but I settled with AES since it is efficient to both hardware and software, it has a strong bit encryption algorithm and it uses 128 bit per block key.

## 

## **5.3 CONCLUSION**

Designing and developing this project provided me with a real platform to translate the theoretical class work in to practical work. Combining class work i.e. programming skills, software engineering among other knowledge and skills is a tortuous road especially for novice students. And it’s because of that reason I would like to thank my friends, lecturers and family for being with me all the way. Along the road I came head to head with many hindrances but they strengthened me more and through perseverance and application of modelling techniques I was able to triumph at the end finally. The knowledge I gained from this experience will plough the road for me to be that software developer I have always dreamt to be. Therefore, I will be able to solve complex challenges in future and make a living out of it.

## 

## **5.4 RECOMMENDATIONS**

**To Students**

1. They should be creative enough to come up with unique projects which they can even make a living out off.
2. They should learn programming skills early enough so as to avoid inconveniences during the project period.
3. They should highly attend events and meet-up e.g. boot camp to keep themselves up-to-date with skills and also shorten their learning curve by knowing what to learn and where to get the necessary resources.

**To The Department of Computer Science**

1. The department should allow students to use programming language (s) of their choice so as to promote creativity.
2. The Lecturers should be more practical oriented and up-to-date with technology.
3. The Lecturers should be encouraging so as to get the best out of students.
4. The departments should organize tech events and meet-ups.

## **5.4 REFERENCES**

1. Liang, Y.D. (2011).*An Introduction to Java Programming*. 8thed. New York: Prentice Hall.
2. Kendall, P.A. (1996).*Introduction to System Analysis and Design: A Structured Approach*. New York: McGraw Hill.
3. Ramakrishman R. and Gehrke J. (2003) *Database Management Systems*. 3rded. New York: McGraw Hill.
4. Robert Richardson, 2008 CSI Computer Crime and Security Survey at 19.[i.cmpnet.com](http://i.cmpnet.com/v2.gocsi.com/pdf/CSIsurvey2008.pdf)
5. Bellare, Mihir. "Public-Key Encryption in a Multi-user Setting: Security Proofs and Improvements." Springer Berlin Heidelberg, 2000. Page 1.