Quest Journals
Journal of Electronics and Communication Engineering Research
Volume 3 ~ Issue 4 (2016) pp: 01-05
ISSN(Online) : 2321-5941
www.questjournals.org

Research Paper

Appendix B: Development of Cryptosystem for Jewellery Business

Dr. Minal Moharir[1], Jayashree Patil[2]
[1]Associate Professor Department Of R. V College of Engineering
[2]PG Student Department of CSE R.V College of Engineering
Bengaluru, Karnataka, India

Received 09 August, 2016; Accepted 30 August, 2016 © The author(s) 2016. Published with open access at **www.questjournals.org**

***ABSTRACT**: In today's technical environment, organizations are becoming more dependent on their information systems. It is vital to be worried about information security, because much of the value of an organization lies in the value of its information. In any business all these information will be keep flowing between different types of medium. So if correct security is not provided, then there may be a chances of loss of an important data. Objective of this article is to secure text files and xml files. Three cryptographic algorithms are used to build this cryptosystem to secure these files and those are DES, AES and Triple DES. DES is used to secure text files with less than one MB in size, AES is used to secure text files with more than one MB in size and triple DES is used to secure xml files. This cryptosystem guarantees full security compared to previously followed manual method, in that method no algorithms were used as part of a cryptosystem so full security was not there. The results have guaranteed that cryptosystem overcomes the previous problems.*

***Keywords:** DES, AES, Triple DES*

I. INTRODUCTION

In every business or organization, information systems plays very important role. The success or profit of any business depends on its information systems. So it is very important in every business to provide proper security to whole information systems. Along with information security, computer security and ethics is also very important. This awareness can be given by giving computer security and ethics education. Every organization should maintain computerized solution to maintain their all-important documents, files and so on.

In any business, information like employee's details, customer details, financial details, design plans, source code details, implementation details, testing details, profit and loss details including confidential information that needs to be hold on behalf of customers or clients are all very important and needs to be secured. So it is very important and necessary to train an employees regarding information security awareness.

All these information will be keep flowing between different types of medium. So if correct security is not provided, then there may be chances of loss of an important data. Providing security to information has so many advantages like it ensures information security from a wide variety of viruses, guarantees project continuation, minimizes different kind of losses and increases business profit. Protection of confidential data has become one of the main necessity of an organization and also it has become an ethical and legal requirement in many cases. So optimal information security investment has become the key concern for organizations. As the number of companies are increasing, the competition has also increased. So security risk management has become very important in companies and organizations. Every organization should maintain information security management system by adopting suitable practices as defined by International Standard Organization (ISO).

II. SYSTEM ARCHITECTURE

Bigger structures are always partitioned into tinier sub-systems those give some corresponded set of services. The diagram strategy of seeing these sub-systems and working up a structure for sub-system control and correspondence is called Architecture arrangement and the yield of this setup methodology is an clarification of the item plan.

The below figure 1 shows the system architecture of development of cryptosystem. This cryptosystem has actually developed between two main softwares, Enterprise Point of Sales System (EPOSS) and Enterprise Resource Planning (ERP). Enterprise Point of Sales System (EPOSS) generates files for encryption and after encryption those files use to store in a separate folder before performing decryption. During decryption, those files will be extracted from that folder one by one and decryption will be performed. Finally decrypted files will be saved in Enterprise Resource Planning Oracle (ERP Oracle).

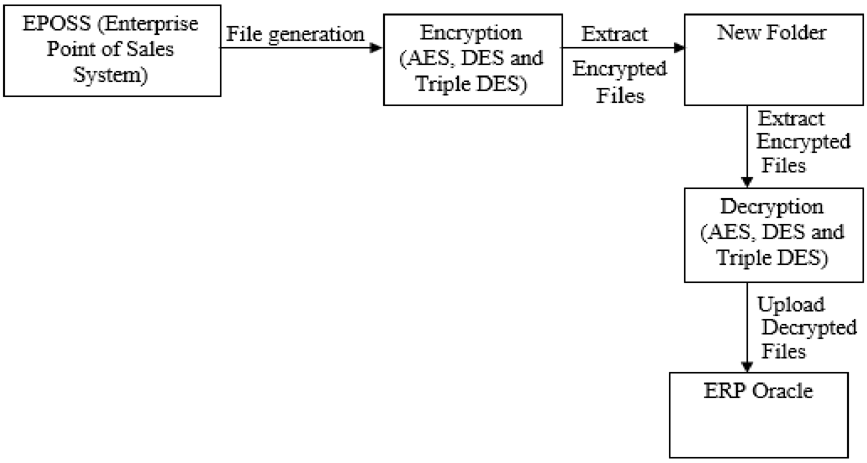
EPOSS (Enterprise Point of Sales System)
File generation
Encryption (AES, DES and Triple DES)
Extract
Encrypted Files
New Folder
Extract Encrypted Files
Decryption (AES, DES and Triple DES)
Upload Decrypted Files
ERP Oracle

Figure 1: System Architecture of Development of Cryptosystem

III. DATA FLOW DIAGRAMS

UML is a multilevel best in class plan dialect contains number of outline charts to speak to various perspectives of the System. Data flow diagram is a type of UML diagram which is widespread model for multimedia applications and signal processing. DFDs are diagrammatic representation of the flow within the system. Data flow diagrams helps in better perception of essentials and setup.Data flow diagrams are utilized to show how information is overseen in a framework. For a detailed analysis they are used to model the data processing aspect of the system. It characterizes data flow between different modules of the system. The information is adjusted at every stage moving to the following stage. A Data stream outline (DFD) is a graphical representation of the development of information through a data framework. DFD chart is made out of 4 essentials those are procedure, information stream, outer substance and information store.

A. Data Flow Diagram – Level 0

Level 0 data flow diagram is also called as **context level** data flow diagram. It represents the whole system as a single process or represents the entire working of a system in a single process. This context level DFD is then expanded in further levels.

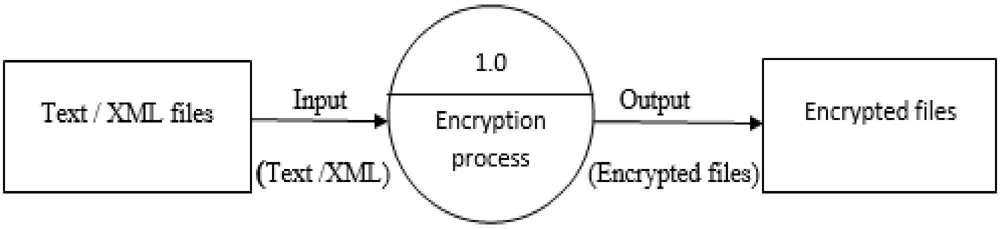

Figure 2: Data Flow Diagram Level 0

The above figure 2 shows the context level (Level 0) Data Flow Diagram of Cryptosystem. The input to the process is either text file or XML file, process performed is encryption and output provided by encryption process is encrypted text or xml files.

B. Data Flow Diagram – Level 1

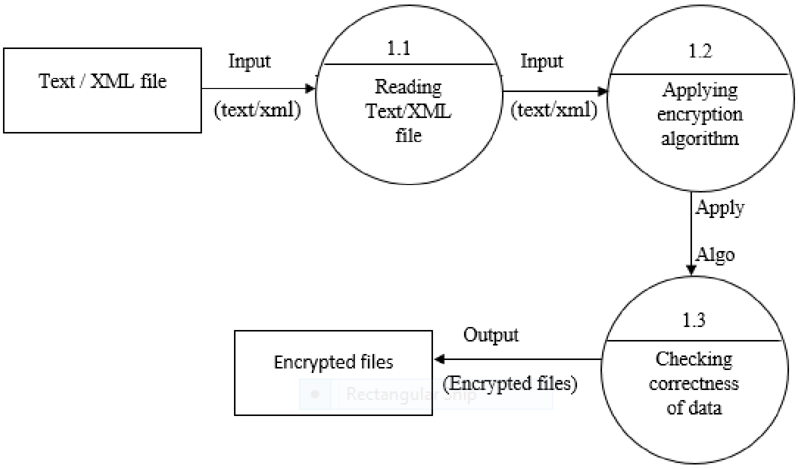

Figure 3: Data Flow Diagram Level 1

This is just an extended version of level 0 DFD. Here the applied process will be expanded and explained in detail with more steps. Level 1 provides more accurate information than Level 0.The above figure 3shows level 1 Data Flow Diagram. Here the input to the process is text or XML file and output is encrypted file. Here the encryption process is divided in to further steps before giving an encrypted data.

3. Data Flow Diagram – Level 2

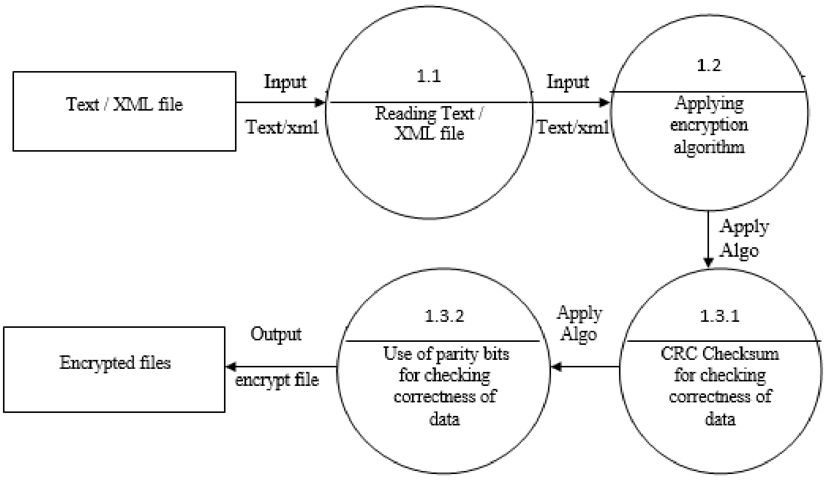

Figure 4: Data Flow Diagram Level 2

The above figure 4 shows level 2 data flow diagram. Input given is either text file or XML file and output provided is encrypted file. The encryption process is divided in to further steps. Cyclic Redundancy Code (CRC) checksum has used here to check the correctness of data. It provides more detailed information than level 1 and it shows complete flow of the project. Level2 data flow diagram is more detailed view than level 0 and level 1.

IV. EXPERIMENT ANALYSIS AND RESULTS

This project has developed to secure text files and xml files while flowing between the different systems. So with this project, information that flows between different systems has secured and thereby security has been provided to the entire system. As indicated by overview general spending on information security has come to $71.1 billion in 2014. This spending has growed a further 8.2 percent in 2015 to reach $76.9 billion. In 2016 it has come to $80 billion.

Before using this software, the traditional or manual method was followed to provide security, but manual method can't guarantee full security. In this case, there may be a chances of loss of data and also it can't secure large files at a time. In manual method, files can be modified by the person who have that authorization and end-users can't get the required file. This project is 10 times better than manual method as it was developed by using 3 cryptographic algorithms and those are DES, AES and Triple DES and this project is able to secure different types of files in very less time.

Table 1: Text Files Statistics

File size	Time to encrypt 1 file in seconds	Time to encrypt 7 files in seconds	Time to decrypt 1 file in seconds	Time to decrypt 7 files in seconds
1MB	5	35	5	35
2MB	10	70	10	70
3MB	15	105	15	105
5MB	25	175	25	175

The above table 1 shows Text file statistics. The project takes same time to encrypt and decrypt a file of the same size.

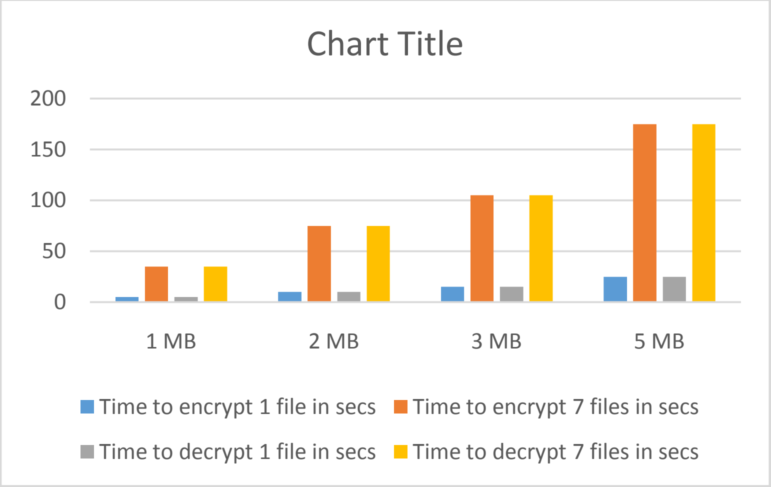

Figure 5 – Text file statistics

The above figure 5 shows text file statistics in graphical form. The X – axis shows files with 1MB, 2MB, 3MB, 5MB and Y –axis shows time taken to encrypt and decrypt those files in seconds. The graph shows that it takes same time to encrypt and decrypt a file with same size.

Table 2: XML file Statistics

File size	Time to encrypt 1 file in seconds	Time to encrypt 7 files in seconds	Time to decrypt 1 file in seconds	Time to decrypt 7 files in seconds
1MB	6	42	6	42
2MB	12	84	12	84
3MB	18	126	18	126
5MB	30	210	30	210

The above table 2 shows XML file statistics. Here also the software takes same time to encrypt and decrypt the file with same size but it takes more time to encrypt XML files compared to text files, because the format of XML file is bit complicated compared to text files.

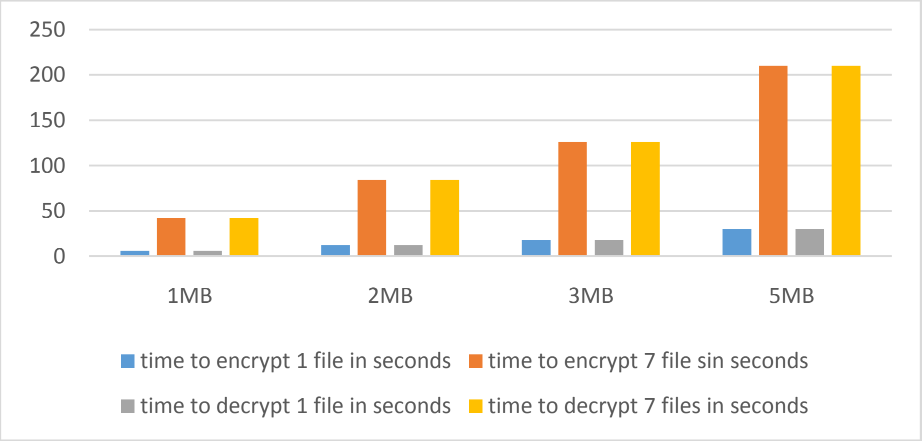

Figure 6 – XML file statistics

The above figure 6 shows graphical representation of XML file statistics. As given in above table 2 the graph shows that it takes same time to encrypt and decrypt the file with same size. As a result of experiment analysis this project is 10 times better than manual method as it was developed by using 3 cryptographic algorithms and those are DES, AES and Triple DES and this project is able to secure different types of files in very less time.

V. CONCLUSION

This project provides basic information of cryptosystem that is developed by using 3 cryptographic algorithms, those are Data Encryption Standard (DES), Advanced Encryption Standard (AES) and Triple DES. It also explains system architecture and data flow diagram. As a result of experiment analysis this project is 10 times better than manual method as it was developed by using 3 cryptographic algorithms and those are DES, AES and Triple DES and this project is able to secure different types of files in very less time.

REFERRENCES

[1]. M.M Alshomrani, Mehtab Mehdim, "The importance and dilemmas of security education in information system", National Workshop on Information Assurance Research, vol 32, 2012, pp. 1 – 5.

[2]. Eric Amankwa, Marianne Loock, Elmarie Kritzinger, " A conceptual analysis of information security education, information security training and information security awareness definitions", 9th International conference for Internet technology and secured transactions (ICITST), vol 14, 2014, pp. 248 – 252.

[3]. Ali Farooq, Syed Rameez, Ullah Kakakhel, "Information security awareness: Comparing perceptions and training preferences", 2nd National Conference on Information Assurance (NCIA), Vol 24, 2013, pp. 53 – 57.

[4]. R. Lublinerman and S. Tripakis, "Translating data flow to synchronous blockdiagrams",IEEE/ACM/IFIP Workshop on Embedded Systems for Real-Time Multimedia, Vol 12, 2010, pp. 101-106.

[5]. S. Handigund, S. Sajjanar and Arunakumari B. N., "Resuscitation of syllogism within unified modeling language levels through the renovation of object diagram", International Conference on Advances in Computing, Communications and Informatics (ICACCI), Vol 10, 2015, pp. 2397-2401.

[6]. International Conference on Advances in Computing, Communication and Informatics (ICACCI), Vol 10, 2015,pp. 2397-2401.