A Web Based Document Encryption Application Software for Information Security in Tertiary Institutions

Ibeneme-Sabinus Ifeoma Livina.[1*], Amadi Emmanuel Chukwuemeka[2], Ekedebe Nnanna[3], Nwokonkwo Obi[4], Ibeneme Sabinus Ikechukwu[5] and Ajah Benjamin Ogonnaya[6]

[1]Graduate Assistant, Department of Cybersecurity, School of Information and Communication Technology (SICT), Federal University of Technology, Owerri, E-mail: **peseesabim@gmail.com and ifeoma.ibeneme-sabinus@futo.edu.ng**

[2]Lecturer I, Department of Information Technology, School of Information and Communication Technology (SICT), Federal University of Technology Owerri, E-mail: emma.amadi@futo.edu.ng

[3] Lecturer II, Department of Information Technology, School of Information and Communication Technology (SICT), Federal University of Technology Owerri, E-mail: ekedebe.nnanna@futo.edu.ng

[4] Senior Lecturer, Department of Information Technology, School of Information and Communication Technology (SICT), Federal University of Technology Owerri, E-mail: obiokonwo@futo.edu.ng

[5] Senior Lecturer, Department of Geology, School of Physical Sciences (SOPS), Federal University of Technology Owerri, E-mail: sabinusibeneme@futo.edu.ng

[6]Technologist, Department of Computer Science, Faculty of Natural and Applied Sciences (FNAS), Federal Polytechnic Nekede Owerri, E-mail: ogonnaya.ajah@fedponek.edu.ng

[*]Corresponding Author: Ibeneme-Sabinus, Ifeoma Livina peseesabim@gmail.com and ifeoma.ibeneme-sabinus@futo.edu.ng

Abstract: A web based user friendly document encryption application software was developed as a better cryptographic online system used in securing important tertiary institutions' documents such as students' Official Grade Report (OGR) sheets, computed and approved results, transcripts, examination and test question papers, Senate/Council documents and any other sensitive or important document needed to be secured from unauthorized users. It is a known fact that problems like unsecured information, information misuse, tampering of sensitive documents by unauthorized persons, stress of hiding sensitive documents from unauthorized persons and locating hidden sensitive documents exist in any system/unit where proper data security mechanism is not in place. In this research work, an online cryptographic system was designed, using Advanced Encryption Standard (AES) algorithm, to secure important documents. The Analysis and Design of this system followed the Structured System Analysis and Design Methodology (SSADM) using web tools. The output of the software shows that the application can encrypt files and save in the database and can only be decrypted using a cipher key automatically generated by the system. With this software, sensitive information can be easily accessed without stress or fear and it has created a more reliable and safer platform to secure such sensitive documents other than the primitive method of using username and password.

Keywords: *Cipher key, Cryptography, Data, Encryption, Information, Tertiary Institution.*

Received: Feb 27, 2020 Revised: May 21, 2020 Accepted: April 24, 2020

DOI: 10.5281/zenodo.3909971

1. Introduction

Cryptography, or cryptology was coined from Ancient Greek word κρυπτός, Romanized as *kryptós* meaning "hidden/secret"; and γράφειν *graphein* meaning "to write", or *-λογία -logia* which implies "study", respectively [1]. In cryptography, encryption is the process of encoding information. It is the method by which plaintext or any other type of data is converted from a readable form to an encoded version that can only be decoded by another entity if they have access to a decryption key [2]. The importance of information security in these modern days cannot be overemphasized. With the rapid evolution of data exchange in network environments, information security has been the most important process for data storage and communication [3]. The rapid growth of digital data transmission has significantly increased the importance of information security in our modern digital life [4]. In data communication the development of new transmission technologies have ascended the need for specific strategy for security mechanisms [5]. Cryptography and different encryption techniques provide security and protection to the data transmitted over non secure networks used for digital transmission of data, hence the scrambling of plaintext delivers a safe and nice significance for secured data and communication [6]. Many researchers have worked on the use of different encryption techniques in data security. Some of such interesting researches are briefly reviewed herein. [7] saw cryptography as the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication and data origin authentication. [8] proposed an encryption system, with its security occurring in networking, storage and other applications and noted that rapid increase in processed data calls for very high-performance implementations of the algorithms utilized. [5] used different parameters to compare modified AES encryption technique with conventional AES and observed that performance of the modified AES algorithms varies on different parameters. [9] compared the results of synthesized and simulated algorithm using Xilinx ISE and Model Sim software with previous work and adduced that higher security is achieved when AES algorithm is implemented on hardware as well as software. [6] recognized that the AES rule is capable of using cryptographic keys of 128, 192, and 256 bits with implementation of AES block cipher of 256-bits and 256-bit key size. [10] encapsulated that the Xilinx HLS tool enabled quick realization of the AES encryption processes design and make optimizations which greatly increased throughout the AES algorithm. [11] carried out investigations on cyber-attacks in android by adopting various malware classification and detection techniques and observed that the ANFIS method detects malware application with high accuracy, with a very high detection rate when compared with other techniques. Due to present need, it is expedient to have fast algorithm which performs the crypto process in time efficient and secure manner, and as such, the best method is performing the crypto operation in parallel using available hardware technology [12]. [13] proposed the use of Visual Key Cryptography in bringing more strength for authentication and access control to provide adequate information security as the task of preserving authentication on the basis of simple alphanumeric passwords is quite challenging. This research work strives to incorporate encryption techniques to sensitive tertiary institutions' information such that only authorized user(s) can gain access to the information. There have been reported cases of leakage and misuse of information in some establishments and institutions. When such sensitive information gets into the wrong hands, the future of such institution is in great jeopardy as such information can be tampered with, erased, erroneously interpreted and may be deposited in public domain. Hence this research designed a secured processing system using the Open Secure Socket Layer (OPENSSL) data encryption technique to protect sensitive documents in tertiary institutions. Figure 1 shows a schematic diagram of an encryption process.

Received: Feb 27, 2020 Revised: May 21, 2020 Accepted: April 24, 2020

DOI: 10.5281/zenodo.3909971

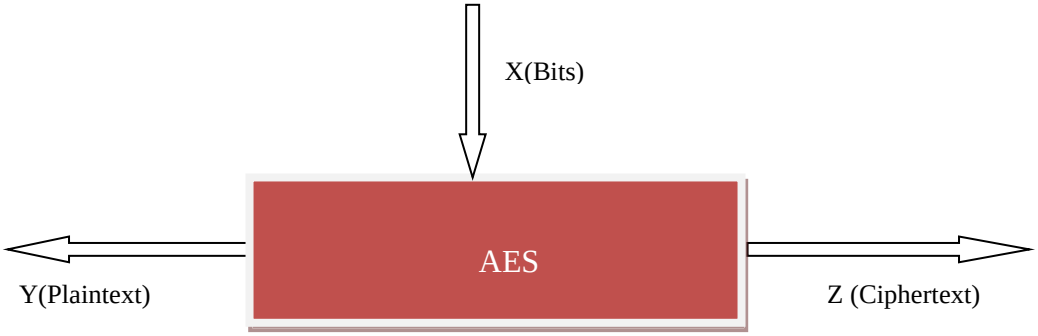

Fig 1: Schematic Diagram of an Encryption Process

2. Objectives of the Research

The new system will achieve the following objectives:

1. Encrypt Tertiary institutions' documents thereby eliminating the problem of an unauthorized user tracing the document and guessing the logging details since the system will be the one to generate the cipher key.
2. Move the encrypted document from the user PC to the new system database thus saving the authorized user the stress of carrying his/her PC from one place to another and can even access his/her encrypted documents anywhere since the new system will be hosted online.

3. Methodology

The methodology used in this research is the Structured System Analysis and Design Method (SSADM). It is an approach that involves a step-to-step process for building a software system. This is widely used in computer application development method.

Some of the methods often used during system development process are listed below:

1. Structured System Analysis and Design Method (SSADM)
2. Spiral Method
3. Object-oriented method
4. Agile
5. Prototyping
6. Unified Modeling Language (UML)

The reasons for choosing SSADM in this research are:

1. It provides easy training
2. Provides easy understanding of the system
3. Provides tools and techniques required by the system
4. With this methodology, there is a reduced risk of failure
5. It is detailed
6. It separates data from procedures
7. Each phase of the project is built by the previous phase
8. SSADM is process oriented (It models actions that capture and manipulate data throughout the system).

3.1 Data Collection

During the data gathering stage at various Schools (Faculties) in the Federal University of Technology Owerri, the researchers interviewed some academic and non-academic staff of different Departments, Units, Centers, Directorates and Institutes on how their sensitive data or information are being secured. Their

Received: Feb 27, 2020 Revised: May 21, 2020 Accepted: April 24, 2020

DOI: 10.5281/zenodo.3909971

responses to the questions were integrated into a working piece that propelled this research. During the interview conducted, the researcher discovered that:
1. Most staff use password to lock their Personal Computer in other to secure their sensitive information which a hacker or unauthorized user can guess and break into the system.
2. Some also hide their sensitive documents inside a preferred folder in their Personal Computer which can be traced and compromised.
3. Others face the stress of carrying their systems from one place to another to ensure that the information contained therein are not tampered with.

From the above reports with the attendant stress in securing information, there is a need to improve the system by designing a software that will secure this information with ease.
Thus, the under listed questions were borne out of the zeal to simplify the application of the intended software viz:

1. Can the new system (developed software) be user friendly, easier and more reliable in securing sensitive documents?
2. Will the new system effectively secure and safeguard sensitive documents from unauthorized users?
3. Can the new system eliminate the former method of using only Username and Password in securing sensitive documents?
4. Can the new system reduce the stress of hiding sensitive information from unauthorized persons?
5. Can the new system reduce the problem of locating sensitive documents in Personal computers?

With the burning desire to ensure that the answers to all the questions above were in the affirmative, the researchers developed the program for the software which tackled these problems headlong.

3.2 *System Analysis Procedure*

The program design structure used in developing this system is called structured programming.
The new system provides interface to support human interaction and enable user to encrypt and decrypt sensitive documents stored in his/her personal computer. The data flow diagram is shown in figure 2 while figure 3 shows the program flow chart.

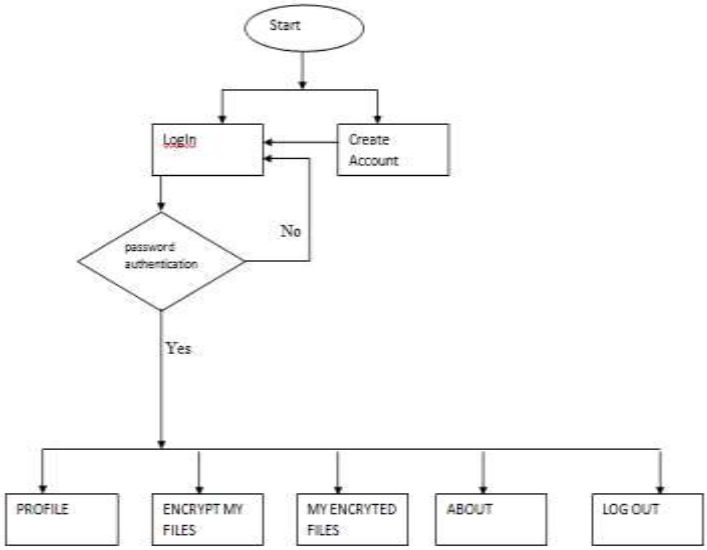

Fig 2: Data flow diagram

Received: Feb 27, 2020 Revised: May 21, 2020 Accepted: April 24, 2020
DOI: 10.5281/zenodo.3909971

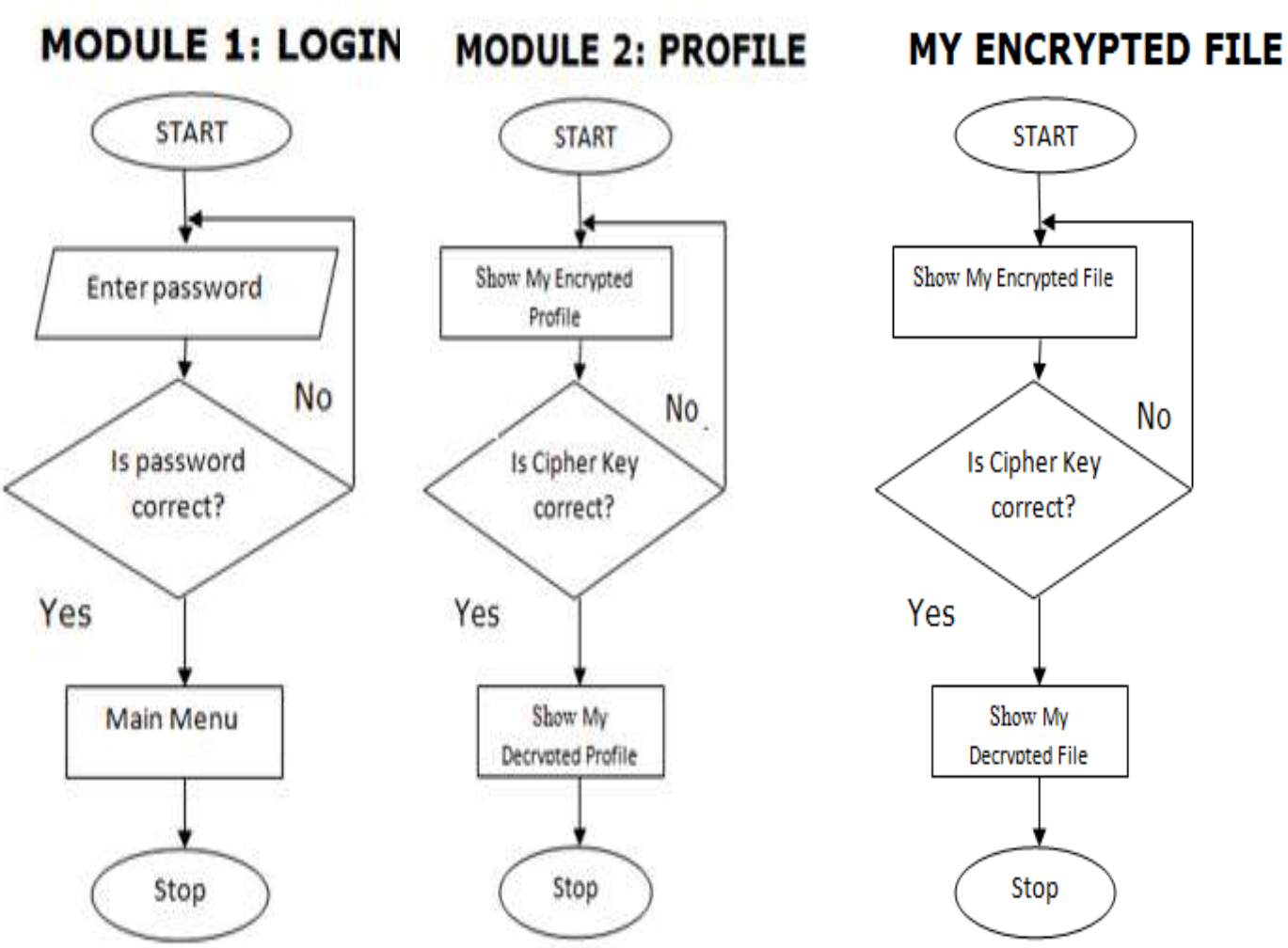

Fig 3: Program flowchart

3.3 Algorithm

Step1: set login to 1
if i !=1 goto 2
check if i >= n
if i >= n login user using php_session and goto 3;
if i !>= n show error message

Step 2: register
accepts fullname, email and password
encrypt fullname, email and password
check if check if i >= n
if check if i >= n return error message
if check if i !>= n store in database
generate a cipher key for data decryption
goto 1

Step3. show user profile encryted

Received: Feb 27, 2020 Revised: May 21, 2020 Accepted: April 24, 2020
DOI: 10.5281/zenodo.3909971

'decrypt my profile'
accept cipher key
if i >= n show error message and goto 2
if i !>= n show user profile
accepts i
if i =1 show error message and goto 2
if i =2 generate new cipher key

Note: encryption and Decryption of data is using a php Open SSL function

4. Modules and Interfaces

4.1 Modules

The system (developed software) consists of 7 modules. They are as follows:
MODULE 1: LOGIN
This module is for Logging by the User
MODULE 2: CREATE ACCOUNT
This module is for creating a new account for the User
MODULE 3: MY PROFILE
This module displays the User Information in encrypted format.
MODULE 4: ENCRYPT MY FILE
This module is used to encrypt the user sensitive documents.
MODULE 5: MY ENCRYPTED FILES
This module displays the User encrypted files.
MODULE 6: ABOUT
This module displays the information of the researchers.
MODULE 7: SIGN OUT.
This module takes the user out of the existing field and back to the login interface.

4.2 Interfaces

The front-end of the system is built using Materialize, CSS and HTML which use PHP to communicate to the Database. MySQL Server serves as the back-end engine providing the useful or needed information to be displayed on the front-end panel for the authorized user.

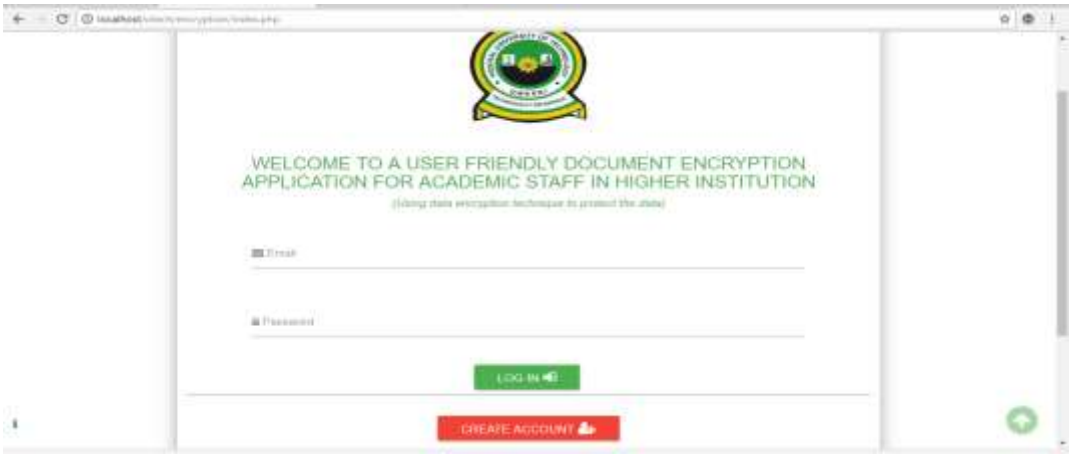

Fig 4: Login Interface

Received: Feb 27, 2020 Revised: May 21, 2020 Accepted: April 24, 2020
DOI: 10.5281/zenodo.3909971

Figure 4 displays the login interface. This is where the users will be able to gain access into the system by providing their Email and Password. If the Email and Password provided are not correct, the user will not be able to login.

When access is gained to the system, the profile screen is displayed showing the users profile details in encrypted format and from there the user can select from the available submenus. The profile menu for the software is displayed in figure 5 below.

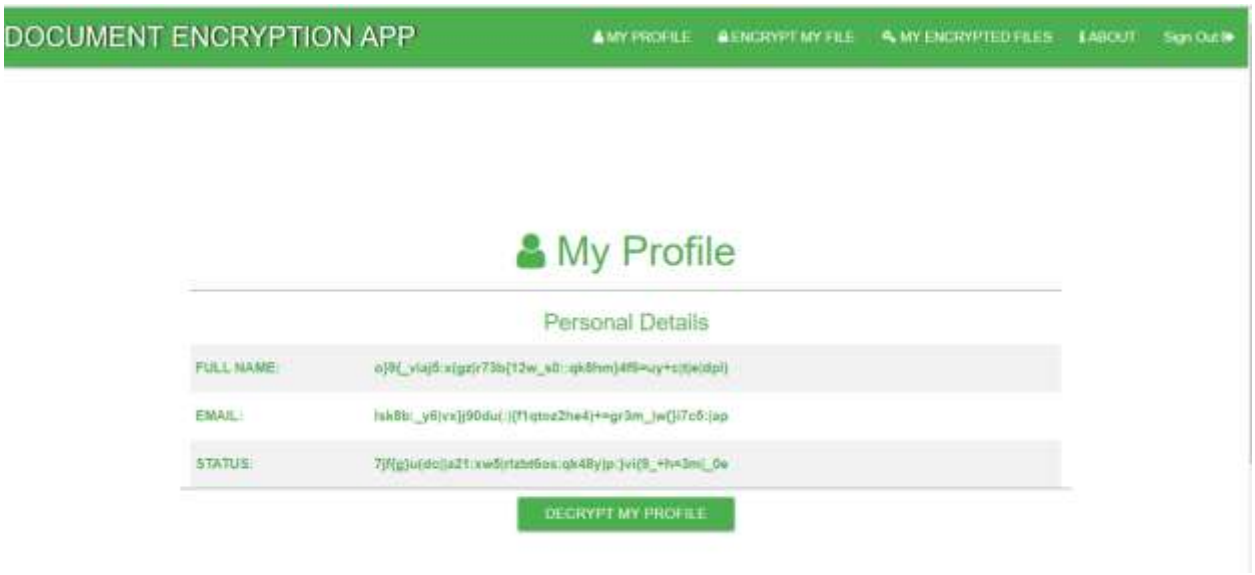

Fig 5: Profile Interface

Create Account page: These are the source documents being worked on. The main input documents in this project are the staff's sensitive documents. The keyboard will be used as the main input device. Figure 6 shows the Create Account interface.

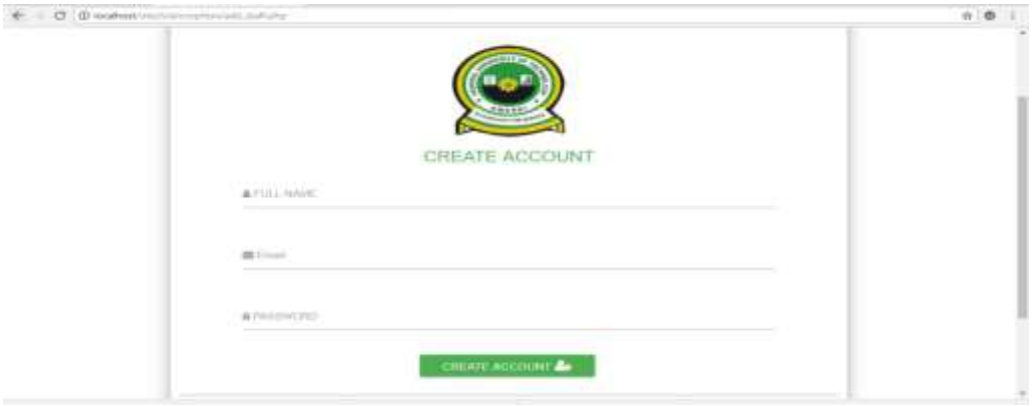

Fig 6: Create Account Interface

Received: Feb 27, 2020 Revised: May 21, 2020 Accepted: April 24, 2020

DOI: 10.5281/zenodo.3909971

Encrypt My File Interface: The interface demanding for the input file to be encrypted is displayed in figure 7 below.

Fig 7: Encrypt my file Interface

4.3 Output

This software was able to encrypt files and securely save them in the system database which can only be decrypted using a cipher key automatically generated by the system. The encrypted file interface is shown in figure 8.

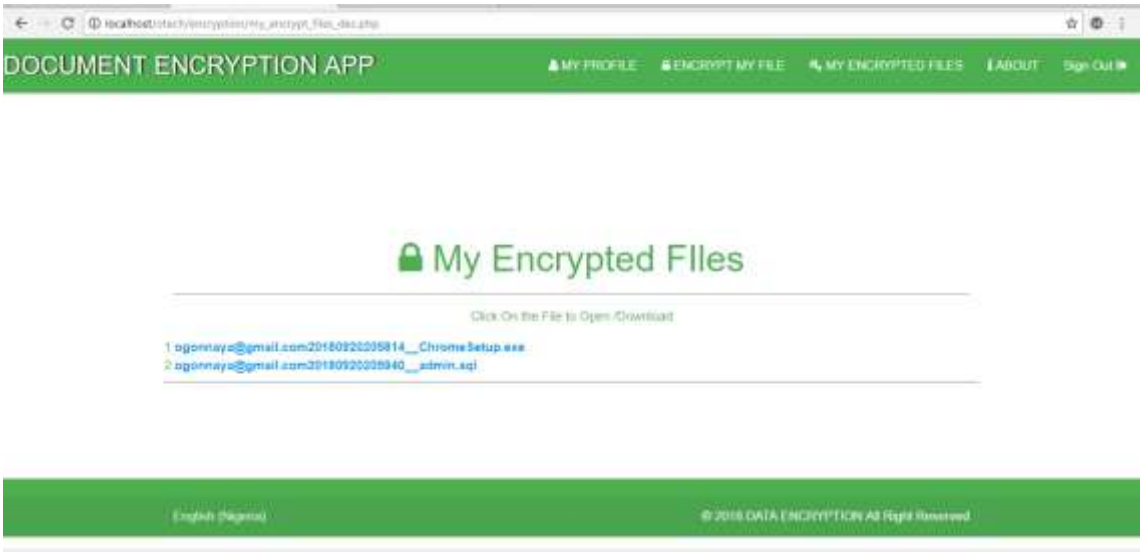

Fig 8: Encrypted file Interface

Received: Feb 27, 2020 Revised: May 21, 2020 Accepted: April 24, 2020

DOI: 10.5281/zenodo.3909971

4.4 Database Design specification

This holds the encrypted document. Table 1 shows the Entity Relation Diagram (ERD) used in the database.

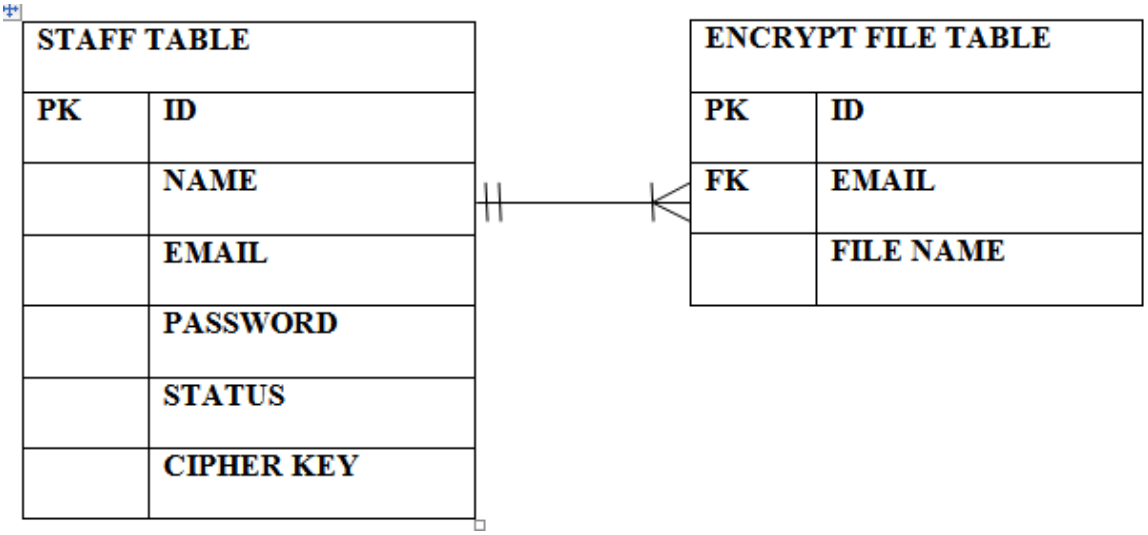

Table 1: Entity Relational Diagram (ERD)

5. Conclusion

Data encryption has played a vital role in different areas of life especially in securing sensitive documents from unauthorized users. Securing sensitive documents using data encryption technique has a wide range in which one cannot access the data unless the key to decrypt it was given to him/her. In addition, the adopted manual method by which the academic and nonacademic staff in higher institutions use in securing sensitive documents has a lot of loop holes and it is prone to manipulation by external person(s). This research developed a user-friendly application software to secure university documents like Official Grade Report (OGR) sheets, computed and approved results, transcripts, examination and test question papers, Senate/Council documents thereby guarding against tampering of such institution's sensitive information by unauthorized users.

References

[1] Liddell Henry George, Scott Robert, Jones Henry Stuart, McKenzie Roderick (1984). A Greek-English Lexicon. Oxford University Press. page 827.

[2] Agrawal, Monika (2012). A Comparative Survey on Symmetric Key Encryption Techniques. International Journal on Computer Science and Engineering. 4: pages 877–882. CiteSeerX 10.1.1.433.2037

[3] Jasim, O., Abbas, S., Horbaty, E. and Salem, A. (2015) Evolution of an Emerging Symmetric Quantum Cryptographic Algorithm. Journal of Information Security, 6: pages 82-91. doi: 10.4236/jis.2015.62009.

[4] Rohan Rayarikar, Sanket Upadhyay, Priyanka Pimpale, (2012). SMS Encryption using AES Algorithm on Android, IJCA, Volume 50- No.19, pages 12-17.

[5] Kirti Prakash Choudhury, Sangeeta Kakoty (2017). Comparative Analysis of Different Modified Advanced Encryption Standard Algorithms Over Conventional Advanced Encryption Standard Algorithm. International Journal of Current Research and Review vol. 9, issue 22: pages 31-34.

[6] Isaac Kofi Nti, Eric Gymfi and Owusu Nyarko (2017), Implementation of Advanced Encryption Standard Algorithm with Key Length of 256 Bits for Preventing Data Loss in an Organization, Department of Electrical/Electronic Engineering, Sunyani Technical University, Ghana. International Journal of Science and Engineering Application, vol. 6 issue 03: pages 87-101.

Received: Feb 27, 2020 Revised: May 21, 2020 Accepted: April 24, 2020

DOI: 10.5281/zenodo.3909971

[7] Kshyamasagar Mahanta, Hima Bindu Maringanti (2015). An Enhanced Advanced Encryption Standard Algorithm. International Journal of Advanced Trends in Computer Science and Engineering (IJATCSE), Vol. 4 , No.4: pages 28 - 33.

[8] Vinodh Gopal, Jim Guilford, and Wajdi Feghali (2015). Application of Classical Encryption Techniques for Securing Data-A Threaded Approach. International Journal on Cybernetics and Informatics. vol.4, No.2: pages 125-132.

[9] Umalaxmi Sawant, Kishor Wane (2016). Analysis of the Effective Advanced Encryption Standard Algorithm. International Journal of Advanced Research in Computer and Communication Engineering Vol. 5, Issue 3: pages 965-967.

[10] Luka Daoud, Fady Hussein, and Nader Rafla (2019). Optimization of Advanced Encryption Standard (AES) Using Vivado High Level Synthesis (HLS). EPiC Series in Computing Volume 58: pages 36-44

[11] Vignesh (2020). Incremental Research on Cyber Security Metrics in Android Applications by Implementing the ML Algorithms in Malware Classification and Detection. Journal of Cybersecurity and Information Management (JCIM) Vol. 3, No. 1, pages 14-20.

[12] Karthikeyan S, Sairamn, Manikandan G,and Sivaguru J. (2012). The Use of Parallel Processing Enhances the Speed of System when Compared to the Traditional Crypto Systems. International Journal on Cybernetics & Information (IJCI) Vol. 4, No. 2: page 127.

[13] Gadicha (2020). Implicit Authentication Approach by Generating Strong Password through Visual Key Cryptography Journal of Cybersecurity and Information Management (JCIM) Vol. 1, No. 1, pages. 5-16.

Received: Feb 27, 2020 Revised: May 21, 2020 Accepted: April 24, 2020

DOI: 10.5281/zenodo.3909971