International Journal of Cyber-Security and Digital Forensics (IJCSDF) 6(4): 162-178
The Society of Digital Information and Wireless Communications (SDIWC), 2017 ISSN: 2305-0012

Enhancing AES with Time-Bound and Feedback Artificial Agent Algorithms for Security and Tracking of Multimedia Data on Transition

[1]A.O. Isah, [2]J.K Alhassan, [3]S.S Olanrewaju, [4]Enesi Femi Aminu.

[1]Department of Cyber Security Science, Federal University of Technology, Minna, Nigeria

[2]Department of Cyber Security Science, Federal University of Technology, Minna, Nigeria

[3]Department of Cyber Security Science, Federal University of Technology, Minna, Nigeria

[4]Department of Computer Science, Federal University of Technology, Minna, Nigeria

[1]ao.isah@futminna.edu.ng, [2]jkalhassan@futminna.edu.ng, [3]lanrezubair@yahoo.com, [4]enesifa@futminna.edu.ng

ABSTRACT

Unsecured information travelling over the network from a source to an intended destination are very vulnerable to cyber attacks. Millions of information have been hijacked and stolen across the globe within the last few years, translating to several millions of Dollars in damages. This paper is on the improvement of the security of existing systems that are mainly encryption systems implementing algorithms such as the Advance Encryption Standard (AES), Rivest Shamir and Addleman (RSA) encryption algorithm, without an active alert system for users. This is by designing and implementing an enhanced Advanced Encryption Standard file encryption model to secure and track information on transition. The implementation was achieved by codifying a Timing Circuit Algorithm (TCA) and Feedback Artificial Agent (FAA) into an Advance Encryption Standard algorithm to control decryption and monitor data along the transition path. Information encrypted with this system cannot be decrypted until the due date and time specified, the monitoring agent also sends reports of decryption to administrator's e-mail address and phone number. The model was implemented with Java programming language; the system achieved the desired results when tested.

KEYWORDS

Encryption, Decryption, Multimedia Data, Transition, Tracking, Information Security.

1 INTRODUCTION

Dynamism in the world of Information Technology (IT) is very vital for exchange of knowledge since no individual or group can be an island within the vast oceans of information. However, transportation of sensitive information within an organisation or between organisations is mostly endangered while on transit with an ever increasing array of malicious hackers [1]. The information technology world is in an era of constant change as a result of business ideas turning up from information technology firms. These business ideas could be in the form of text, graphics, audio or videos. Apple is one of those companies that produce new devices on regularly basis to target new market areas [2]. In the launching of iPod, the then Chief Executive; Steve Jobs, presents it to an astonished audience by asking them the use of the tiny pocket in their jeans? He said it is meant for a tiny music player called iPod that can store more than one thousand songs using a small chip of high memory size. This revelation inspires a generous patronage from lots of buyers. This valuable business information could have been stolen by their competitors through data hijacking on transit from Apple's online communication network.

More so, the Chinese economy has been growing tremendously in recent years that it has attracted

United States (US) accusation of individuals in China of cyber attacks and industrial secret information hijack. The US emphasized further that some of the attacks traced down to China are not just about military espionage but are targeted to business information that gives Chinese business owners a competitive edge in the global market [3].

Similarly, State and National Examination bodies are grappling with information leakages in form of examination questions and sensitive materials. This has resulted in increased cases of examination malpractices. The vulnerability of examination questions and materials is inherent in the transition from the examination offices to the examination centres [4].

Last but not the least, is the popular cyber attack against Sony Pictures in the last months of 2014 [3]. The hacking group, Guardian of Peace, had earlier attack and leaked the email accounts of staffs of Sony Pictures, publishing the private emails of some top management personnel that have racial contents in order to instigate people against the leaders in Sony Pictures that contribute to its successes in the Hollywood industry. Thereafter the hackers threaten Sony Pictures not to release their new film titled "The Interview", a comedy film that mimics the assassination of North Korean leader Kim Jong-un, as well as publishing a lot of other upcoming films on online download sites. Sony Pictures lose millions of dollars as they had to heed the threat of hackers by cancelling the release of a film they spent much money advertising to the general public [6]. On the part of top government officials, it was an embarrassment in terms of national security. The US President, Barack Obama has to intervene and ordered the release of the film after many days has passed by and asserts that Sony Pictures made a mistake by heeding to the threats of hackers by not screening the film on the initial date scheduled for it [5].

Consequently, the security and tracking of information on transition is an uphill task for institutions of government and business organisations; hence this study proposes the use of an Enhanced Advanced Encryption Standard (AES) File Encryption System for the Security and tracking of information Transition by embedding Feedback Artificial Agent (FAA) and Time Circuit Algorithm (TCA).

1.1 Motivation

The Authors' motivation is inspired by the high prevalence of data or confidential records breached or stolen across the world. The Risk Base Security (RBS) report of February 2014 for Open Security Foundation revealed that several attacks were successfully carried out that resulted in exposing hundreds of millions of data and confidential information in most advanced countries as the statistics shows in Table 1

Table 1. Statistics of Data exposed and Stolen in 2014 (Risk Based Security report, 2014)

Exposed Records Ranking	Country	Total Exposed Records	Percentage of Exposed Records
1	United States	546,846,693	66.5%
2	South Korea	140,238,121	17.1%
3	Australia	42,672,848	5.2%
4	Sweden	29,000,002	3.5%
5	Japan	22,162,392	2.7%
6	China	12,012,056	1.5%
7	United Kingdom	11,669,949	1.4%
8	Taiwan	6,468,738	0.8%
9	Germany	2,101,718	0.3%
10	Canada	1,564,966	0.2%

1.2 Statement of Problem

Many authors such as [6, 7, 8], all tried to improve the security of data either on transition or at rest, with the use of cryptography and steganography. The problem the existing solutions could not solve is that, the authors were not able to develop a model for monitoring the data on transition or at rest. The concern of the authors of this paper is to add a mechanism for securing and tracking of an encrypted multimedia data of any high security and economic value on transition. The mechanism also alerts the sender via a registered mobile number and email address, of any attempt to either hack sent multimedia data or the successful decryption

of the multimedia data by the genuine consignee. The solution proffered by this study also works effectively on data at rest. However, the focus of the research is on multimedia data on transition as data becomes more vulnerable while on transition between two or more communicating nodes in the internet.

1.3 Aim and Objective

The aim of this study is to provide security and tracking for Information multimedia data on transition using enhanced AES file encryption system. This will be achieved by the following objectives;

i. To design a model for secured multimedia data on transition from a source to destination
ii. To implement enhanced Advanced Encryption Standard (AES) algorithm using java programming language, Feedback Artificial Agent (FAA) and Timing Circuit Algorithm (TCA) to monitor encrypted multimedia data on transition.

To test the performance of the designed model for secured multimedia data on transition.

1.4 Feedback Artificial Agent (FAA)

The Feedback Artificial Agent (FAA) can be defined as the mechanism embedded in the software implementation of this study to effect the sending of alert in the form of short text messages via a registered mobile phone number and email address.

1.5 Time Circuit Algorithm (TCA)

The Time Circuit Algorithm (TCA) can be defined as the mechanism for effecting predetermined time of decryption for any multimedia data encrypted and sent on transition.

2 REVIEW OF RELATED WORK

[6], presents that Steganography allows a user to securely hide messages in a cover media and to extract hidden message from the same media. Singh *et al* agrees that the varieties of steganography techniques; some of which are more complex than others, all have respective strong and weak points. The paper proposes the combined concept of Cryptography and steganography with the use of Elliptic Curve Cryptography (ECC). The main focus of the research is to encrypt the data with Asymmetric Cryptography and apply the steganography technique to hide encrypted data and thus make it a hybrid model. Existing hybrid approach which uses RSA with steganography is suffering from big performance hit. However, the limitation of the work lies in the fact that it lacks a feedback artificial agent that can monitor an encrypted multimedia data on transition.

[7], are concerned about a secured pathway for data transmission, explaining that multicast routing for wireless mesh networks has focused on metrics that estimate link quality to maximize throughput. Nodes must collaborate in order to compute the path metric and forward data. The assumption that all nodes are honest and behave correctly during metric computation, propagation, and aggregation, as well as during data forwarding, leads to unexpected consequences in adversarial networks where compromised nodes act maliciously. The authors identify novel attacks in wireless mesh networks. The attacks exploit the local estimation and global estimation of metric to allow attackers to attract a large amount of traffic. The authors demonstrate both the attacks and defense strategy using On-Demand Multicast Routing Protocol (ODMRP). The limitation of the work is that it is the network pathway of the data being transmitted that is secure, the data becomes vulnerable the moment it enters through a differently configured network and such, it is better to encrypt the data for a more reliably data security irrespective of the network.

[9], explained that security is required for the protection of delivery of multimedia data, thus this security is provided by the use of encryption. The authors used selective encryption for protecting multimedia data that takes less computational workload and provides five levels of security from level 0 to level 4. These five levels of security are; level 0 where there is no encryption, level 1 where the headers from the sequence layer down to the

slice layer is encrypted, the encryption of Intra-frame coded blocks (I-blocks) and the complete encryption of level 1 occurs in level 2, at level 3 the encryption of Intra Frames (I - Frames) and all the remnants of I-blocks and finally at level 4, the complete encryption of multimedia data (video). The study was not able to effects the timing of decryption for improved security assurance of the multimedia data.

[8] argue that Image covers the highest percentage of multimedia data and that its protection is very important. The authors submit that the use of cryptography is an effective tool for assuring the confidentiality of transmitting images over the internet.
The paper presents a review on image encryption techniques of both full encryption and partial encryption schemes in spatial, frequency and hybrid domains. However, the study focused on image only as a multimedia data and very silent on how other multimedia data type can be protected by encryption over the internet.

[10], highlights that Mobile Ad-Hoc Networks (MANETs) established efficiency in the deployment for number of fields, but highly vulnerable to security attacks, a situation that seems to be more challenging for wireless networks. The paper proposes Reliable Data Security Architecture (RDSA) for multi-path multimedia streaming over wireless network to improve multiple path routing efficiency in frequent communication failures due to channel interferences. The proposal framework provides better bandwidth allocation and reduces transmission delay. Simulations are carried out with Dynamic Source Routing (DSR) and Ad-hoc On-demand Distance Vector (AODV) protocols for efficient multi-path multimedia data transmission security scheme. Although, the authors improve the security of multimedia data using RDSA as a methodology, the research could not include a feedback artificial agent system to monitor attempts by hackers to compromise data over the wireless network.

In order to prevent offline and online attacks [11], the authors showed in their analysis of password managers, that the Mobile password manager is the most effective. The limitation of their work lies in the fact that although, passwords are important protective measures in information security but, they only serve as a first line of defense while encryption is last line of defense. This we have utilized with additional elements of defense proposed and implemented in our paper by tracking with time-bound algorithm otherwise herein called Timing Circuit Algorithm (TCA) and the Feedback Artificial Agent (FAA).

[12], studied how to Enhance Multimedia Security in Cloud Computing Environment Using Rivest Shamir Adleman (RSA) algorithm and Advanced Encryption Standard. The authors methodology is system model that merely listed the usually computation of Rivest Shamir and Adleman algorithm as well as the transformation rounds in Advance Encryption Standard. The authors were able to present a concise explanation of the two encryption techniques. The goal of the study was not achieved as the paper could not add to existing knowledge.

[13], tries to impact a change on the RSA algorithm against recent efforts by hackers which the authors called secure RSA for secure document transmission as there are numerous situations where there is the need to secure record transmission, for instance in banking, e-shopping, state security data sharing. The study concentrates on data transfer utilizing Secure RSA, which eliminates some vulnerability of RSA that may keep a hacker from stealing and abuse of information. The authors could not implement this frame work for multimedia data.

[14], noted that most communication channels are no longer one to one, as other devices in the network also receives data generated by a device in the same network through multicast transmission architecture. This is due to the fast improvement of information and network technologies. These multicast systems that enhance rapid delivery of messages in the network also open up loopholes to snooping attacks in the network. The study submits that one to one encryption is no longer effective for the security of data. So, the authors proposed a novel anonymous multi-receiver encryption, in

which receiver's decryption key is fixed. Furthermore, the model provided anonymity of receivers, performance analysis and comparisons with other schemes.

[15], although in their work, emphasizes the complexity and the uncertainty of information security, but they showed that the risk can be minimized by assessing the risk, and then applied Genetic Algorithm (GA) to reducing it by assigning variables to GA and run an iterative tests by the arranged elements. The results were finally compared with the admissible risk volume. However, the authors were able to use the GA to minimize the security risk in information which is one of the concerns of our paper, but securing encrypted information from unauthorized decryption and tracking by the administration could not be solved by the application of the GA proposed by this reviewed work.

2.1 Analysis of the Existing Systems

The need to analyze existing software systems was taken into recognition as it is the bases for justifying this thesis titled Security of Multimedia Data on Transition Using Enhanced AES File Encryption System. This was done by picking and explaining the features and uses of a number of encryption softwares, that are commonly used for online and offline communication security in paragraphs.

The merits of the software are that it has a simple graphical user interface, small memory size as an application and the ability to access text file directly from the computer system. However, the demerits of BCTextEncoder include being text only encrypting software and the need to carefully select the appropriate decryption password from the list of saved keys.

Secretpad in figure 1 is trusty encryption technique based text encryption software that has just three components. The components are the tool bar, where the file, edit, format, view and help features are located. It uses passwords to encrypts texts and only that same password can be use to decrypt it. It makes use of simplified graphical user interface like that of windows notepad. It is useful for the storage of passwords, secret correspondence and other confidential information. The software automatically closes the window in case of long inactivity. Installation is not required as users only need to down load and run it.

Source: listoffreeware.com, 2014

Figure 1. Secretpad Encryption Software.

The drawback inherent in the use of the software is that encryption and decryption icons cannot be easily located, it hidden under the file icon. Also, trusty encryption algorithm is highly vulnerable to hack attacks.

Arcanum Editor in figure 2 is robust encryption software for texts, using a combination of Advanced Encryption Standard (AES), Bytes, Base64, Rot 13 and 1337 Speak encryption techniques. Individual algorithms can be selected at will whenever there is the need to encrypt a classified text based information, as well as choosing a password when using the AES algorithm. The advantages of the encryption software include the present of the different encryption algorithms and a user friendly graphical user interface. The disadvantages include its being text only encryption software.

Source: listoffreeware.com, 2014

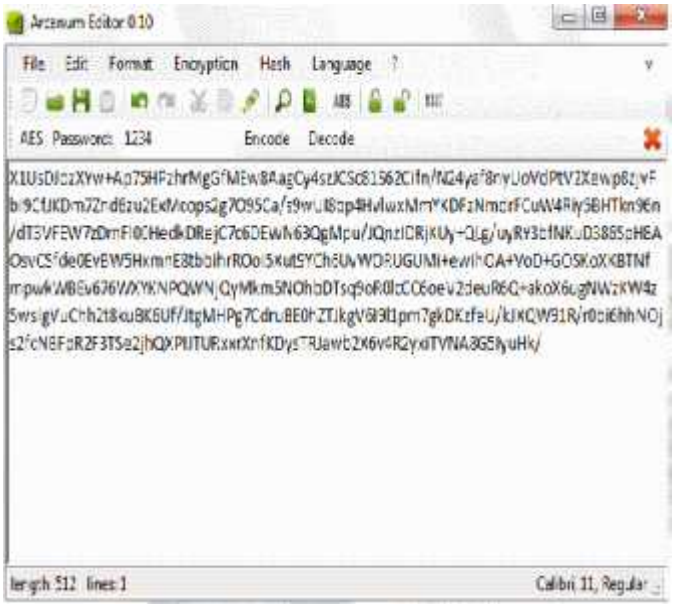

Figure 2. Arcanum Editor and Encryption Software

AES (256-bit) software in figure 3 is Advanced Encryption Standard algorithm technique based encryption software that uses a 256-bit key length password. It can be used to encrypt and decrypt a text while on a removable disk. Encrypted texts are decrypted by entering the same password, failure to do so will pop-up error message. There are other variations of Advanced Encryption Standard, that is, the 128-bits and 192-bit. However, this software uses the 256-bits length only. The merits of the software include a strong encryption and decryption key that is very difficult to crack by hackers and a simple layout of the user interface. The demerits are its inability to encrypt multimedia data and add other variations of AES.

Simple Text Encryptor in figure 4 is a free program, similar to AES encryption software but uses a small encryption key length of 128 bits. It has a simple graphical user interface and has two versions; the one that has to be installed and the other are zipped and stand alone. The zipped only need to be unzipped. Keys are generated randomly to encrypt a text and the same key is entered to decrypt.

Although this is a simply text editor, it has the ability to encrypt texts messages that are intended to be kept confidential. It occupies small memory space and could be installed; the user cannot decide the keys. During execution, the editor allows random generation of keys that can be used to encrypt texts that are saved in .txt file format only and multimedia file cannot be handled by it.

Source: listoffreeware.com, 2014

Figure 3. AES (256bit) Encryption Software.

Source: listoffreeware.com, 2014

Figure 4. Simple Text Encryptor Software

The analysis of existing encryption software in this study includes, Cryptditor shown in figure 5. It adopts Advanced Encryption Standard technique. The software can be used to encrypt any imported text data. Multiple files can be opened in its tabbed windows and encryption and decryption of texts are effected with a password. Cryptditor have basically two components, the tool bar and the text editor. The tool bar is the place holder of file, edit, tab, format and help. Text to be encrypted or decrypted can be typed on the text box or pasted on it. The user then click the file icon and pops out a box showing the Enter password and Repeat password text fields, Passphrase quality. On the box, the user clicks ok to encrypt, decrypt or cancel the process.

Source: listoffreeware.com, 2014

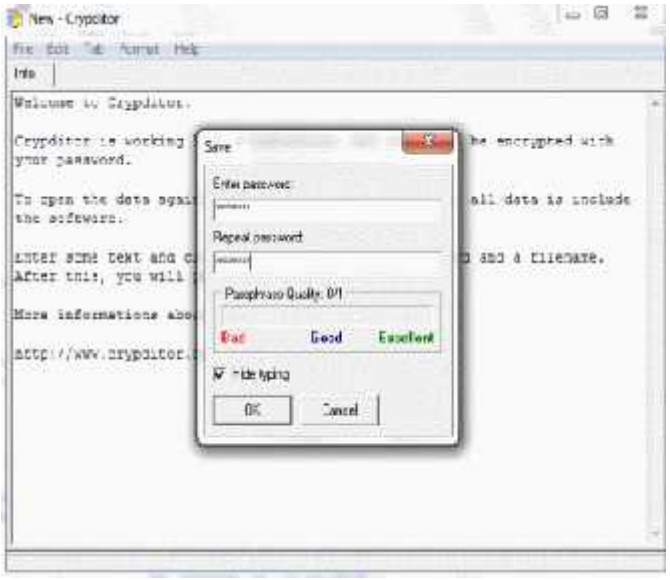

Figure 5. Cryptditor Encryption Software.

Encryption Tool in figure 6 encrypts files with a combination of MD5, SHA1, and the Advanced Encryption Standard. This makes it one of the very strong tools for encryption of confidential texts. It requires the uses of password to encrypt and decrypt files and a mechanism for checking the strength of a chosen password. The Encryption tool has two components, a tool bar and a text box for editing texts. There are file, edit, tools and about icons. The user has to click tools to select the encryption window to open. The encryption window has a Hash algorithm icon to select the desired encryption algorithm, PW iteration icon, and the key size icon.

Source: listoffreeware.com, 2014

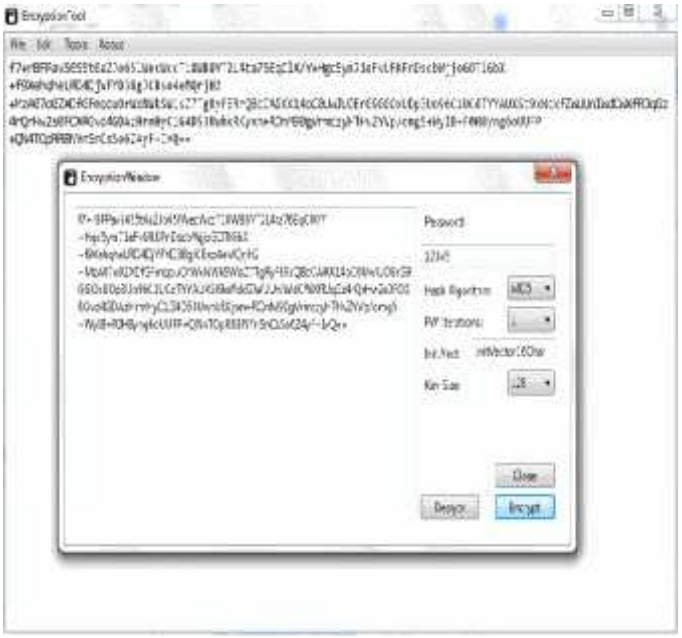

Figure 6. Encryption Tool Software

2.2 Summary

Finally, in this chapter, the authors were able to pin point the methodology used in the related work reviewed, highlight the strengths and weaknesses of the individual studies and then relate it to this study. Available software implementation of different encryption techniques were also analyzed with respect to how it works number of components, the encryption technique adopted, its strengths and weaknesses. All these put together provided a fundamental understanding of the challenges faced with data security on transition and then gives a clue to how it can be improved on in this work; the aim of which is the Security and tracking of Multimedia Data on Transition with an enhanced AES with a Time-Bound and Feedback Artificial Agent Algorithms. The enhancement is based on the addition of Feedback Artificial Agent (FAA) and Time Circuit Algorithm (TCA). In the analysis of existing systems, it can be deduced that most of the encryption softwares are mainly text encryption softwares that cannot encrypt video, graphics and audios. However, some of the few Advanced Encryption Standard based systems that do multimedia encryption does not address the threats to data in the course of transiting from

source node to destination node. The existing research was not able to effect the integration of timing circuit algorithm that can disallow file or folder decryption before the scheduled time of decryption at the destination node. Monitoring agent to keep track of data was also lacking. Hence, this study seeks to bridge these gaps.

3 METHODOLOGY

This section is dedicated to laying out the methodology, the materials and resources used are discussed and the model the authors employed in analyzing the implementation of the proposed work.

In the research, none of the encryption softwares mentioned in chapter two can encrypt video, graphic or audio files with Feedback Artificial Agent (FAA) and a Time Circuit Algorithm (TCA) altogether. Most of the softwares were developed to encrypt text and text files, the few ones that can do the encryption of multimedia data do not have FAA and TCA. Therefore, the authors researched into encryption algorithms that can effectively be used as a scientific basis for implementing the aim and objectives of this study. This is where the Enhanced AES comes into the modeling of the File Encryption System for this work, using the FAA and TCA as the unique models for this work.

3.1 The Advanced Encryption Standard

The security and tracking of multimedia data on transition can be achieved by applying the Advanced Encryption Standard (AES), enhanced and modeled it into a file encryption system, thereby giving it the power to accept any data type such as text, video, graphics and audio. The existing encryption system mostly accepts text. The few that accept multimedia data do not have feedback artificial agent that monitor and notify the source of a data on transition of any attempt to compromise the confidentiality, integrity and the availability of the data and of course the decryption of the data by the authorized receiver. In this model, the real data is digitized into an 8-bit data element in matrix formation and then passed through the Enhanced Advanced Encryption Standard. M represent Multimedia data like; text, video, graphics and audio. Figure 7 shows that data M as a matrix function in which each data element is an 8bits (1byte):

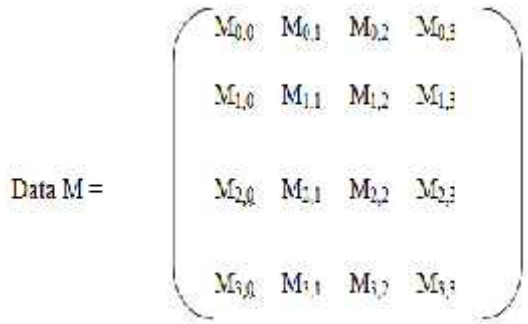

Figure 7. Data M in Matrix Formation.

In the transformation shown in figure 8, the data was converted to an encrypted bit value that is represented in machine language using the Advanced Encryption Standard. This explains the reason why cipher data is presented as a data file since it cannot be read naturally. It is only the deciphered data that has been converted back to normal language that can be read again. The decryption process is the inverse matrix function of the encryption processes.

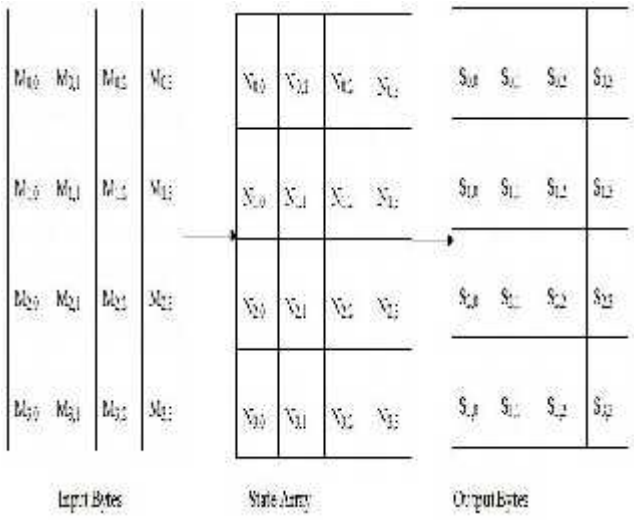

Figure 8. Matrix transformation of plain data in AES.

The internal operation of the AES adopts the concept of repetition called rounds as shown in Figure 8. The plain data M passes through the state array S, where substitutions, transposition and XOR bitwise operations occur to produce the

cipher data N. The inverse matrix of the cipher data N, gives back the original plain data.

3.2 AES Multimedia Encryption Algorithm

The pseudo code for the AES encryption algorithm is shown in capital letters below:

```
START
        SELECT MULTIMEDIA FILE
        ENTER AES ENCRYPTION PASSWORD
        GENERATE CIPHER USING
PASSWORD
        READ IN FILE
        FIGURE OUT FULL SIZE OF FILE
        ENCRYPT FILE DATA
        WRITE ENCRYPTED DATA TO NEW
FILE
STOP
```

3.3 AES Multimedia Decryption Algorithm

The pseudo code for the AES decryption algorithm is shown in capital letters below:

```
START
        SELECT MULTIMEDIA FILE
        ENTER AES DECRYPTION PASSWORD
        GENERATE CIPHER USING
PASSWORD
        READ IN FILE
        DECRYPT FILE DATA
        FIGURE OUT FILE SIZE
        WRITE DECRYPTED DATA TO NEW
FILE
END
```

3.4 Timing Circuit Algorithm (TCA)

The Timing Circuit algorithm is used to determine when a multimedia data encrypted can be decrypted in the file encryption system. It is to make sure that in the event where an attacker was able to hijack a sensitive multimedia data; he would not be able to decrypt it before the time programmed on it for its decryption. The structural model for the Timing Circuit Algorithm is in figure 9.

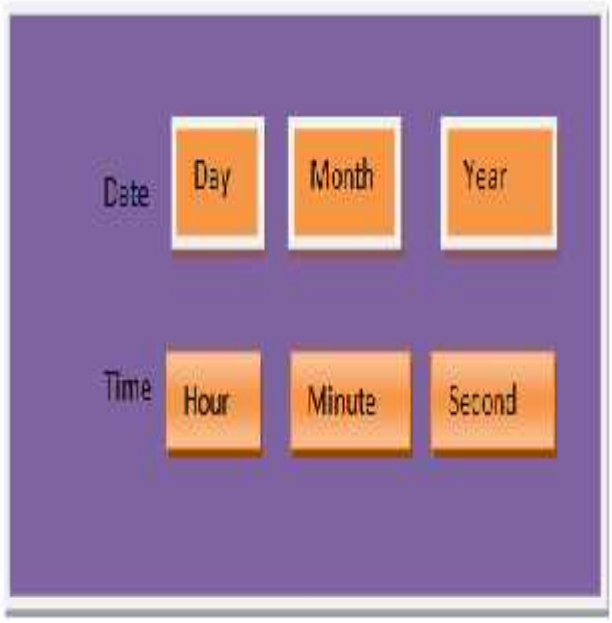

Figure 9. Model for Timing Circuit Algorithm.

3.5 The Timing Circuit Algorithm (TCA) pseudo code

The pseudo code for the Timing algorithm is shown below:

```
START
   GET ENCRYPTED FILE
    GET THE TIMING SECURITY DETAILS OF
         ENCRYPTED FILE
     SET Y=Decrypted due date Year
      H= Decrypted due Time Hour
      M= Decrypted due date Month    MIN=
         Decrypted due Time Minute
       D= Decrypted due date Day
       SEC= Decrypted due Time Second
       y= Current Date Year;  h= Current Time Hour
       m= Current Date Month;  min= Current Time
Minute
       d= Current Date Day;     sec=  Current  Time
Second
       SET                                  Boolean
is_Decryption_Date_Time_Due=x
       x = false
       IF Y > y
          x=false
        ELSE IF Y=y
          IF M>m
             x = false
          ELSE IF M=m
```

```
      IF D>d
        x=false
      ELSE IF D=d
      IF H>h
          x=false
       ELSE IF H=h
       IF MIN>min
          x=false
       ELSE IF MIN=min
       IF SEC>sec
          x=false
       ELSE
          IF SEC=sec
            x=true
          ELSE x=true
       ENDIF
    ENDIF
STOP
```

3.6 The Feedback Artificial Agent (FAA)

The Feedback Artificial Agent (FAA) is the system that monitors the encrypted multimedia data on transition by effecting the sending of short message to a registered phone number and an email address of the sender of data, whenever the holder of the decryption key decrypts the data or any attempt by an attack to hijack and decrypt the multimedia data. The structural model for the feedback algorithm is shown in figure 10. Clicking the process in the figure will trigger the sending of an alert to the phone number and email address registered with the modelled Feedback Artificial Agent for this study.

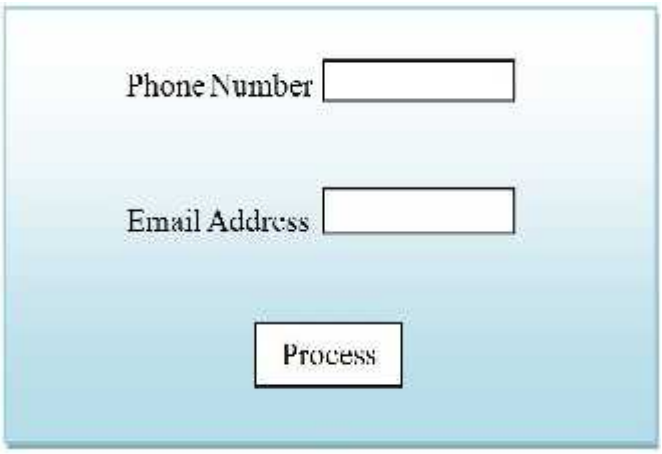

Figure 10. Model for Feedback Artificial Agent Algorithm

3.7 The Feedback Artificial Agent Algorithm

```
START
   IF (DECRYPTION DATE/TIME NOT DUE)
AND
          (PASSWORD IS INCORRECT) THEN
      SEND UNSUCCESSFUL DECRYPTION
      SMS/EMAIL FEEDBACK
   ELSE IF
       DECRYPTION DATE/TIME NOT DUE
AND
        PASSWORD IS CORRECT
        SEND UNSUCCESSFUL DECRYPTION
          SMS/EMAIL FEEDBACK
   ELSE IF
      DECRYPTION DATE/TIME DUE AND
PASSWORD
         IS CORRECT
        SEND SUCCESSFUL DECRYPTION
SMS/EMAIL
           FEEDBACK
    ENDIF
STOP
```

3.8 Algorithm for the Enhanced AES File Encryption System

```
START
   SELECT TARGET FILE
   ENTER ENCRYPTION PASSWORD
   WRITE DECRYPTION DATE/TIME SETTING
TO
         TARGET FILE
   ENTER FEEDBACK RECIPIENT PHONE
         NUMBER/EMAIL
   ENCRYPT FILE
STOP
```

3.9 Algorithm for the Enhanced AES File Decryption

```
START
  SELECT TARGET FILE
  ENTER DECRYPTION PASSWORD
  CHECK DECRYPTION DATE/TIME AND
PASSWORD
  IF DECRYPTION DATE/TIME NOT DUE
AND PASSWORD INCORRECT
```

SEND UNSUCCESSFUL SMS/EMAIL
ELSEIF DECRYPTION DATE/TIME NOT DUE AND PASSWORD CORRECT
SEND UNSUCCESSFUL SMS/EMAIL
ELSE IF DECRYPTION DATE/TIME DUE AND PASSWORD CORRECT
SEND SUCCESSFUL SMS/EMAIL
DECRYPT FILE
ENDIF
STOP

3.10 The Model for the Enhanced File Encryption System

This model developed for the Security of Multimedia Data on Transition using Enhanced AES File Encryption System, is discussed in comparison to the existing AES multimedia encryption system. Figure 11, shows the existing AES file encryption system that has a key generator inputted into the AES encryption of system. The original multimedia data is also inputted into the system resulting in a ciphered multimedia data, the reverse of the process gives back the original multimedia data.

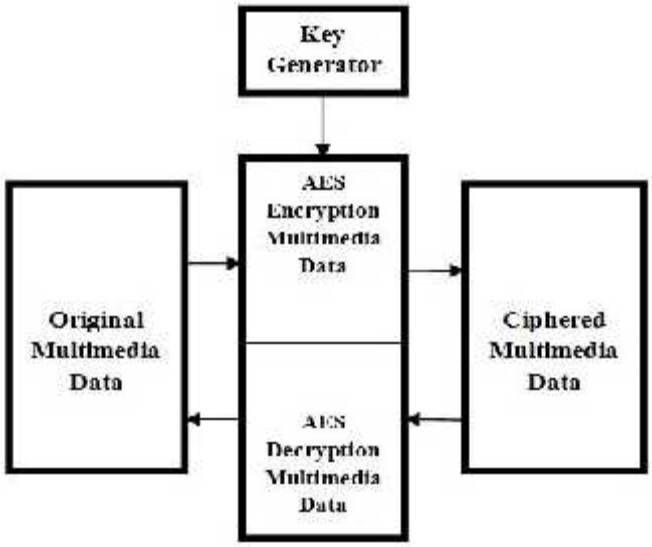

Figure 11. The Model of AES Multimedia Encryption system.

In figure 12, the authors enhanced the AES file encryption system by embedding the Feedback Artificial Agent that serves as a monitoring system for a multimedia data on transition, thereby executing the sending of reports whenever the encrypted data is decrypted and a Timing Circuit algorithm also embedded to the determine when an encrypted multimedia data on transition can be decrypted. The green section is the enhanced section.

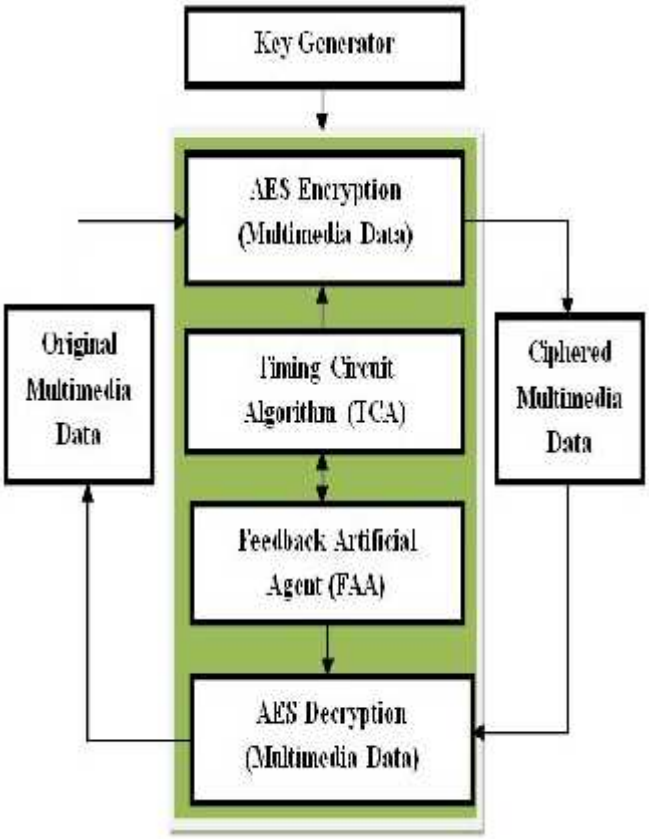

Figure 12. Structural Model for the Enhanced AES Multimedia Data Encryption System.

Figure 13. The Enhanced AES icon

4 MODEL IMPLEMENTATION AND TESTING

The authors discussed the implementation of the software simulation of the Enhanced AES With Time-Bound and Feedback Artificial Agent Algorithm for Security and Tracking of Multimedia Data on Transition.
As explained earlier, the implementation was effected using Java programming Language. This was achieved by some complex coding of the Timing Circuit Algorithm and that of the Feedback Artificial Agent into the existing AES codes to produce a single algorithm (AES Enhanced) for the software implementation of the objectives of this work.

4.1 Launching of the Software Simulation

This system can be accessed directly from the built-up module by double-clicking the Enhanced AES icon to launch or access it from the NetBeans IDE 8.0.2 environment. This is shown in figures 13 and 14 respectively.

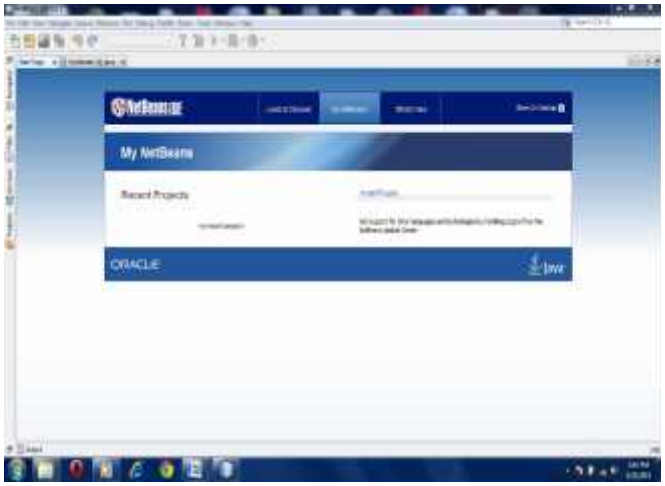

Figure 14. The NetBeans IDE 8.0.2 Environment

4.2 System Application Encryption Interfaces

Figures 15-20 shows the System Application Encryption Interfaces.
It is very important to provide quick step by step process on how to use the system as highlighted in figure 15

Figure 15. System Encryption Interface Displaying the Help Menu.

When the interface is launched, the date and Time security Checkbox can be checked to activate Timing Circuit Algorithm settings. This is shown in figure 16

Figure 16. System Encryption Interface with Date and Time Security Settings.

This interface shown in figure 17 represents the Feedback Artificial Agent (FAA) settings. A default email and phone number can be set here so that reports can always be sent to them by the FAA monitoring the multimedia transition from the source to the destination.

Figue 17. Default Feedback Artificial Agent (FAA) Settings.

Figure 18 represents the interface where a multimedia folder or file to be sent on transit is being access from its location on the computer system, then the expected date and time of decryption were set; also a phone number and an email address were specified where the Feedback Artificial Agent shall be sending its reports to. The ''process'' button is clicked for the encryption process to begin. The Feedback Artificial Agent will automatically be activated to starts its monitoring activities.

Figure 18. Accessing and Encrypting a Multimedia File from Folder

In figure 19, the FAA sends a report displaying the security details and demanding for confirmation before the system finalizes the encryption process.

Figure 19. Inputted Details Confirmation.

Upon the completion of the encrypting process, the FAA sends the report as shown in figure 20. Click the 'OK' to end encryption status.

Figure 20. Multimedia File Encrypted.

4.3 System Application Decryption and tracking Interfaces

Figures 21-29 shows the System Application Decryption Interfaces. The Decryption process involves the simultaneous actions of the Time-bound (Time Circuit Algorithm) and Tracking (Feedback Artificial Agent) mechanisms.

Figure 21 shows the decryption interface of the system. The encrypted multimedia folder has changed to ciphered multimedia folder and the key was entered to decrypt the multimedia folder; the 'process' button clicked to start the decryption process.

Figure 21. The Decryption Interface.

Figure22, represent the interface display the decryption in progress. The FAA is at this moment, monitoring the security details at the encryption stage in order to authenticate them.

Figure 22. Multimedia Folder or File Decryption in Progress.

The interface as shown in figure 23 displays a multimedia file decryption attempt failure because there was no internet connection. The FAA report also fails to deliver as the attempt failed.

Figure 23. Decryption Attempt Offline.

Figure 24 is the decryption interface displaying the message of an invalid password. The encryption and decryption keys used in this system is password based and hence displays 'invalid password' message when an attempt is made to on the multimedia file or folder on transition with wrong passwords.

Figure 24. Decryption Interface displayed attempted with invalid password

This interface shown in figure 25 was an attempt on an encrypted multimedia file on transit when the date and time was not due. Hackers may have succeeded in guessing the password though any method but the Timing Circuit Algorithm that is string to AES Algorithm blocked the decryption.

Figure 25. Decryption Attempted on Transit when time not due

The interface shown in figure 26 represents the successful completion of the multimedia data decryption process at the intended destination when the date and time were also due. The data is decrypted back to the original plain multimedia data

Figure 26. Multimedia Data File Decrypted Successfully.

The interface shown in figure 27 is the action of the Feedback Artificial Agent (FAA) which sends reports to the pre-set email address and phone number on the successful decryption of the multimedia data when the pr-programmed date and time is due.

Figure 27. Feedback Artificial Agent (FAA) Sends Report.

Figure 28 is the interface showing the report that the FAA sent to the administrator's mobile phone as an alert message from the FAA monitoring server.

Figure 28. Report of the Feedback Artificial Agent (FAA) on a Mobile Phone.

Figure 29 is the interface showing the report that the FAA sent to the administrator's e-mail box from the FAA monitoring server.

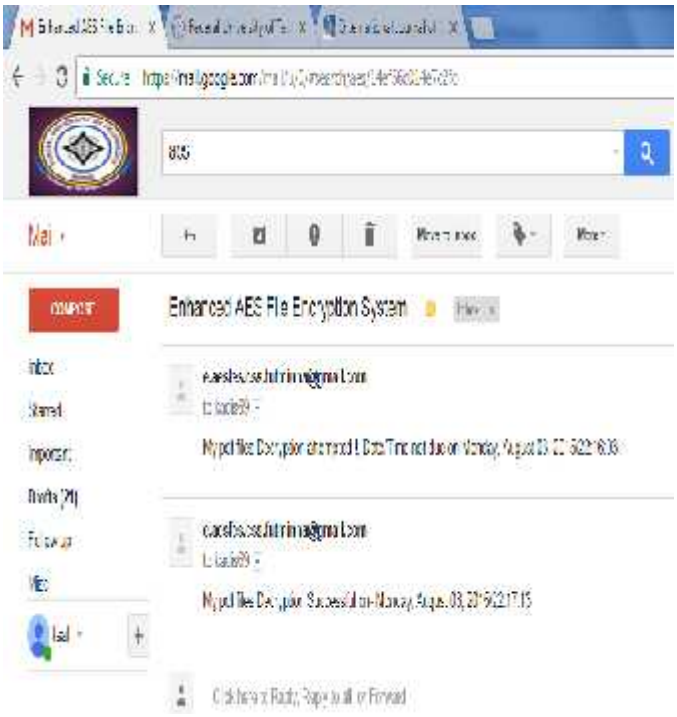

Figure 29. Report of the Feedback Artificial Agent (FAA) Delivered to an e-mail Address.

4.4 Discussion

The system model has been implemented as designed by the authors. Multimedia folder or file can be accessed from any location from the computer system and encrypted as such. This is one of the differences between this very model and most of the encryption system reviewed where the file content has to be copied and pasted or directly written to the text field of the encryption system. The enhancement of the AES with the FAA and TCA has been able to give high reliability to multimedia data transiting via network and also put the data administrator on guard.

5. CONCLUSION AND RECOMMENDATION

The work of this paper, Enhanced AES With Time-Bound and Feedback Artificial Agent Algorithm for Security and Tracking of Multimedia Data on Transition has been able to achieve the aims and objectives which are to design a model for secured multimedia data in transition from a source to destination and also the implementation of the enhanced AES algorithm using java programming language, Timing Circuit Algorithm and Feedback Artificial Agent to monitor encrypted multimedia data on transition. The testing of the performance of the designed model for secured multimedia data on transition was also successful.

The authors recommend further research on this work to enable the monitoring of multimedia data on transition to be tracked, to know the exact location on transit where the data was successfully decrypted or where an attempt was made to decrypt the data. So also, physical security should be taken seriously, as the breach of it can easily thwart all the effort made in securing confidential data.

REFERENCES

1. Avinash Kak "AES: The Advanced Encryption Standard lecture notes on Computer and Network Security" Lecture8: 2017, https://engineering.purdue.edu/kak/compsec/NewLectures/Lecture8.pdf
2. Apple, "Apple Introduces 10GB iPod-2,000 Songs in your pocket', Apple Press Release March 20, 2012. Retrieved from www.apple.com/pr/library/2002
3. Richard Taylor, "Sony cyber attack leaves many questions" BBC Business News, November 26, 2014. Retrieved from www.bbc.com/news/business
4. Olatunde A. Aworanti "Strategies for Managing Examination Malpractice in Public Examinations" 2012, retrieved from http://www.nabtebnigeria.org/wp-content/uploads/2012
5. Alan Yuhas (2014, December 19), Sony CEO insists 'we made no mistake' after US accuses North Korea of hack – as it happened. The Guardian Newspaper. Retrieved from www.theguardian.com/us-news/
6. Pooja Singh, Hardik Upadhyay, Mitesh Thakor, Krunal Suthar, "A Survey: A Hybrid Approach to Secure Transmitted Message by Combining Steganography and Asymmetric Cryptography", International Journal of Innovative Research in Computer and Communication Engineering Vol. 2, Issue 11, November 2014. ISSN (Online): 2320-9801.
7. Adarsh. R, Ganesh Kumar. R, Jitendranath Mungara ''Secure Data Transition over Multicast Routing in Wireless Mesh Network", International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-1, Issue-3, August 2012. Retrieved from www.ijitee.com
8. Reena J. Shah, Bhavna K. Pancholi, "Multimedia Security Techniques", International Journal of Innovative Research in Electrical, Electronics, Instrumentation And Control Engineering. Vol. 2, Issue 5, May 2014. Retrieved from www.ijireeice.com
9. Radha. S. Shirbhate, Anushree A.Yerawar, Ankur M. Hingane "Features Preserving Data Encryption Used to Secure Multimedia Data" International Journal of Emerging Technology and Advanced Engineering. ISSN 2250-2459, Volume 2, Issue 1, January 2012. Retrieved from www.ijetae.com
10. Renuka, M. Thangaraj, P "Reliable Data Security Architecture for Multi-Path Multimedia Streaming in MANET", International Journal of Electronics & Communication Technology
IJECT Vol. 3, Issue 1, Jan. - March 2012. Retrieved from www.iject.com
11. Agholor, S. Sodiya, A. S, Akinwale, A. T. Adeniran, O. J. and D. O..: A Preferential Analysis of Existing Password Managers from End-Users' View Point". The Society of Digital Information and Wireless Communications, (ISSN: 2305-0012)
International Journal of Cyber-Security and Digital Forensics, (IJCSDF) 5(4): 187-196 (2016).
12. Nithyabharathi, P. V. Kowsalya, T. Baskar, V. "To Enhance Multimedia Security in Cloud Computing Environment Using RSA and AES" International Journal of Science, Engineering and Technology Research (IJSETR), Volume 3, Issue 2, February 2014. Retrieved from
www.http://ijsetr.org/wpcontent/uploads/2014/02/IJSETR -VOL-3-ISSUE-2-341-345.pdf
13. Jamgekar, R. S. & Joshi, G. S. "File Encryption and Decryption Using Secure RSA" International Journal of

Emerging Science and engineering, 2013 1(4) 2319-6378. Retrieved from www.ijese.org

14. Harn, L., Chang, C. C. & Hsiao, L. W. "An Anonymous Multi-Receiver Encryption Based on RSA" International Journal of Network Security, 2013, 15(4) 307-312. Retrieved from www.ijns.femto.com.
15. Alireza Tamjidyamcholo and Rawaa Dawoud Al-Dabbagh. "Genetic Algorithm Approach for Risk Reduction of Information Security"
The Society of Digital Information and Wireless Communications, (ISSN: 2305-0012)
International Journal of Cyber-Security and Digital Forensics, 1(1): 59-66, (2012)