Digital Innovations & Contemporary Research in SCIENCE, ENGINEERING & TECHNOLOGY
Vol. 10. No. 1, 2022

Article Citation Format
Oghenekaro, L.U., Ikeobi, A. & Enyindah, P. (2022):
A Hybrid Text-Based Encryption System for Data Security
. Journal of Digital Innovations & Contemporary Research in Science, Engineering & Technology. Vol. 10 No. 1. Pp 39-48
DOI: dx.doi.org/10.22624/AIMS/DIGITAL/V10N1P4

Article Progress Time Stamps

Article Type: Research Article
Manuscript Received:11th Dec, 2021
Review Type: Blind
Final Acceptance:: 20th February, 2022

A Hybrid Text-Based Encryption System for Data Security

Oghenekaro, Linda Uchenna, Ikeobi, Adaobi & Enyindah, Promise
Department of Computer Science
University of Port Harcourt
Rivers State, Nigeria
E-mails: linda.oghenekaro@uniport.edu.ng, ikeobia@gmail.com, promise.enyindah@uniport.edu.ng

ABSTRACT

In recent years, everything is trending toward digitization, and with the development of the internet technology, digital media can be transmitted conveniently over the network there by leading to data theft among others. Cyber security encompasses a broad range of practices, tools and concepts are closely related to those of information and operational technology security used in securing data to avoid data theft (Amah, 2015). Data theft is the act of stealing information stored on computers, servers, or other devices with the intent to compromise privacy or obtain confidential information. Data theft is a growing problem for individual computer users as well as large corporations and organizations. Data theft has continued to grow and has risen to the extent where organizations are finding new ways to secure data in information systems. There are several reports of spammers, crawlers and hackers who break into people's privacy to gain illegal access to their data. This has posed greater challenges on people who use database, transact online, and internet users. Information is a valuable and costly asset that must be presented, controlled and planned just like other valuable assets within organizations. Many businesses have come to the realization that, in order to compete in the global market place, key business processes need to be fully secured. Data integrity affects the accuracy of information maintained in the system, based on validity, quality and security which affect the entire system's operations and desired outcomes. Different data security techniques has emerged such as cryptography, biometrics, pass-wording and 2fa Authentications. Cryptography has continued to gain momentum among researchers based on its level of security concept. The use of cryptography for securing data has been a great one which has help to guard against the vulnerability of data both in store format, auditing communication to wiretapping (spying) and accessibility especially in cloud computing environment. Encryption is a well-known technology for protecting sensitive data, the use of combination of Public and Private Key encryption to encrypt data into unreadable format which can be decrypted by users. Cryptography plays a vital role in the information security system against various attacks. The Advanced Encryption Standard (AES) is a strong symmetric key cryptographic algorithm which uses a number of tables look ups to increase its performance

Keywords: Advanced Encryption Standard, Encryption Algorithm, Cryptography, Database

1. INTRODUCTION

In recent years, everything is trending toward digitization, and with the development of the internet technology, digital media can be transmitted conveniently over the network there by leading to data theft among others. Cyber security encompasses a broad range of practices, tools and concepts are closely related to those of information and operational technology security used in securing data to avoid data theft (Amah, 2015). Data theft is the act of stealing information stored on computers, servers, or other devices with the intent to compromise privacy or obtain confidential information. Data theft is a growing problem for individual computer users as well as large corporations and organizations. Data theft has continued to grow and has risen to the extent where organizations are finding new ways to secure data in information systems. There are several reports of spammers, crawlers and hackers who break into people's privacy to gain illegal access to their data.

This has posed greater challenges on people who use database, transact online, and internet users. Information is a valuable and costly asset that must be presented, controlled and planned just like other valuable assets within organizations. Many businesses have come to the realization that, in order to compete in the global market place, key business processes need to be fully secured. Data integrity affects the accuracy of information maintained in the system, based on validity, quality and security which affect the entire system's operations and desired outcomes. Different data security techniques has emerged such as cryptography, biometrics, pass-wording and 2fa Authentications. Cryptography has continued to gain momentum among researchers based on its level of security concept. The use of cryptography for securing data has been a great one which has help to guard against the vulnerability of data both in store format, auditing communication to wiretapping (spying) and accessibility especially in cloud computing environment. Encryption is a well-known technology for protecting sensitive data, the use of combination of Public and Private Key encryption to encrypt data into unreadable format which can be decrypted by users. Cryptography plays a vital role in the information security system against various attacks. The Advanced Encryption Standard (AES) is a strong symmetric key cryptographic algorithm which uses a number of tables look ups to increase its performance

2. RELATED LITERATURE

Nishtha, et al. (2016) implemented a hybrid encryption algorithm, using Advanced Encryption Standard (AES) and Elliptical Curve Cryptography (ECC) with encrypted keys for secure key exchange and enhanced cipher-text security. Their study focused on verifying cache timing attack and investigated some of the countermeasures by implementing them. Their results showed the encryption performed on a text document as input using Advanced Encryption Standard 192- bit in which the key has been given by the user and the number of iterations used for the AES was 12. Jasleen, et al., (2016) introduced a hybrid algorithm of RSA as Digital Signature and Blowfish Algorithm which provided improved security to the data while being uploaded or downloaded from cloud. Their work focused only on providing security for data in motion, as there was no clear evidence of security while data was at rest. Radhika, et al., (2016) described a new architecture for security of data storage in multi-cloud. Their work made use of two mechanisms-data encryption and file splitting, every uploaded file, was encrypted using AES encryption algorithm, then was further divided into equal parts according to the number of clouds and stored into multi-cloud.

Their proposed system enhances the data security in multi-cloud. Li, et al., (2014), proposed a system for securing E- Business using Hybrid combination based on symmetric Key and RSA Algorithm. Both the encrypted secret key and the encrypted message are then sent to the Merchant.

The recipient decrypts the private key first, using his own private secret key, and then uses that secret key to decrypt the message. Tarakji, (2011) suggested a technique based on key encryption algorithm which uses ASCII values of input text to encrypt the data. Renu, (2013) evaluated the performance of three algorithms such as AES, DES, and RSA to encrypt text files under three parameters like computation time, memory usage, and output bytes. Encryption time was computed to convert plaintext to cipher text then comparing these algorithms to find which algorithm takes more time to encrypt text file. According to the results they have obtained RSA takes more time compared to other algorithms. For second parameters RSA needs a larger memory than AES and DES algorithms. DES and AES produce the same level of output byte whereas RSA has a low level of output byte. Nentawe (2013), in their work titled "Data Security in Cloud Computing using RSA Algorithm", reiterated that the RSA contains drawback like fake public key algorithm, complexity of key generation, security needs and low speed.

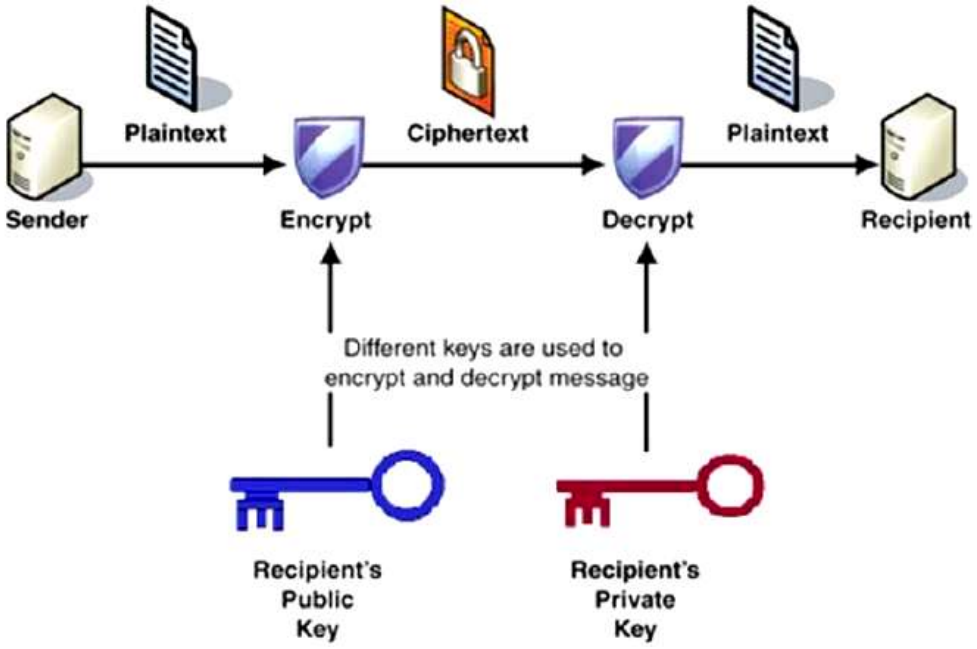

Fig. 1: A Typical Encryption Systems
Source: https://www.tutorialspoint.com/cryptography/public_key_encryption.htm

Jayasinghe, et al., (2010) proposed a new architectural method to reduce the complexity of AES algorithm when it is implementing on the hardware such as mobile phone, PDAs and smart card etc. The method consisted of integrating the AES encrypted and the AES decrypted to provide a perfect functional AES crypto-engine. This was achieved by focusing on some important features of AES especially Sub Bytes and Mix column module.

The existing system in this study was done by (Naphtha, et al., 2016), who proposed and implemented a hybrid system that uses AES Based Text Encryption using the key size of 192 bit and with 12 rounds of iterations for encrypting a plain text while Elliptic Curve Cryptography algorithm (ECC) was further used to encrypt the AES 192 bit key. Therefore, the proposed system applies a higher key size 256 bit with 14 rounds of iteration while achieving hybrid encryption using the AES algorithm and ECC encryption algorithm in encrypting the generated key and eliminating of possible vulnerability that tend to arise.

3. MATERIALS AND METHODS

The AES encryption process contains rounds and each round comprises of four sub-processes, these sub-processes convert the plain text data into cipher text through the use of a secret key. Figure1shows the process of plain text going through the aes encryption rounds, the key length designed is 256-bit, which reflects the number of rounds to be performed - 14 rounds. The more rounds to be executed, the more time consumed. The four types of AES operations involved in the encryption process are as follows:

3.1 Key Expansion and AddRoundKey

As mentioned earlier, the key size determines the number of rounds that will be performed. AES encryption uses the Rjindael Key Schedule, which derives the sub keys from the main key to perform the key expansion. The AddRoundKey operation takes the current state of the data and executes the XOR Booleanoperation against the current round sub key. XOR means "Exclusively Or," which will yield a result of true if the inputs differ (e.g. one input must be 1 and the other input must be 0 to betrue). There will be a unique sub key per round, plus one more (which will run at the end).

3.2 SubBytes

The SubBytes operation, which stands for substitute bytes, will take the 16-byte block and run it through an S-Box (substitution box) to produce an alternate value. Simply put, the operationwill take a value and then replace it by spitting out another value.The actual S-Box operation is a complicated process, but just know that it's nearly impossibleto decipher with conventional computing. Coupled with the rest of AES operations, it will doits job to effectively scramble and obfuscate the source data. The "S" in the white box in theimage above represents the complex lookup table for the S-Box.

3.3 ShiftRows

The ShiftRows operation is a little more straightforward and is easier to understand. Based offthe arrangement of the data, the idea of ShiftRows is to move the positions of the data in theirrespective rows with wrapping. Remember, the data is arranged in a stacked arrangement andnot left to right like most of us are used to reading. The image provided helps to visualize thisoperation.The first row goes unchanged. The second row shifts the bytes to the left by one position withrow wrap around. The third row shifts the bytes one position beyond that, moving the byte tothe left by a total of two positions with row wrap around. Likewise, this means that the fourthrow shifts the bytes to the left by a total of three positions with row wrap around.

3.4 MixColumns

The MixColumns operation, in a nutshell, is a linear transformation of the columns of thedataset. It uses matrix multiplication and bitwise XOR addition to output the results.

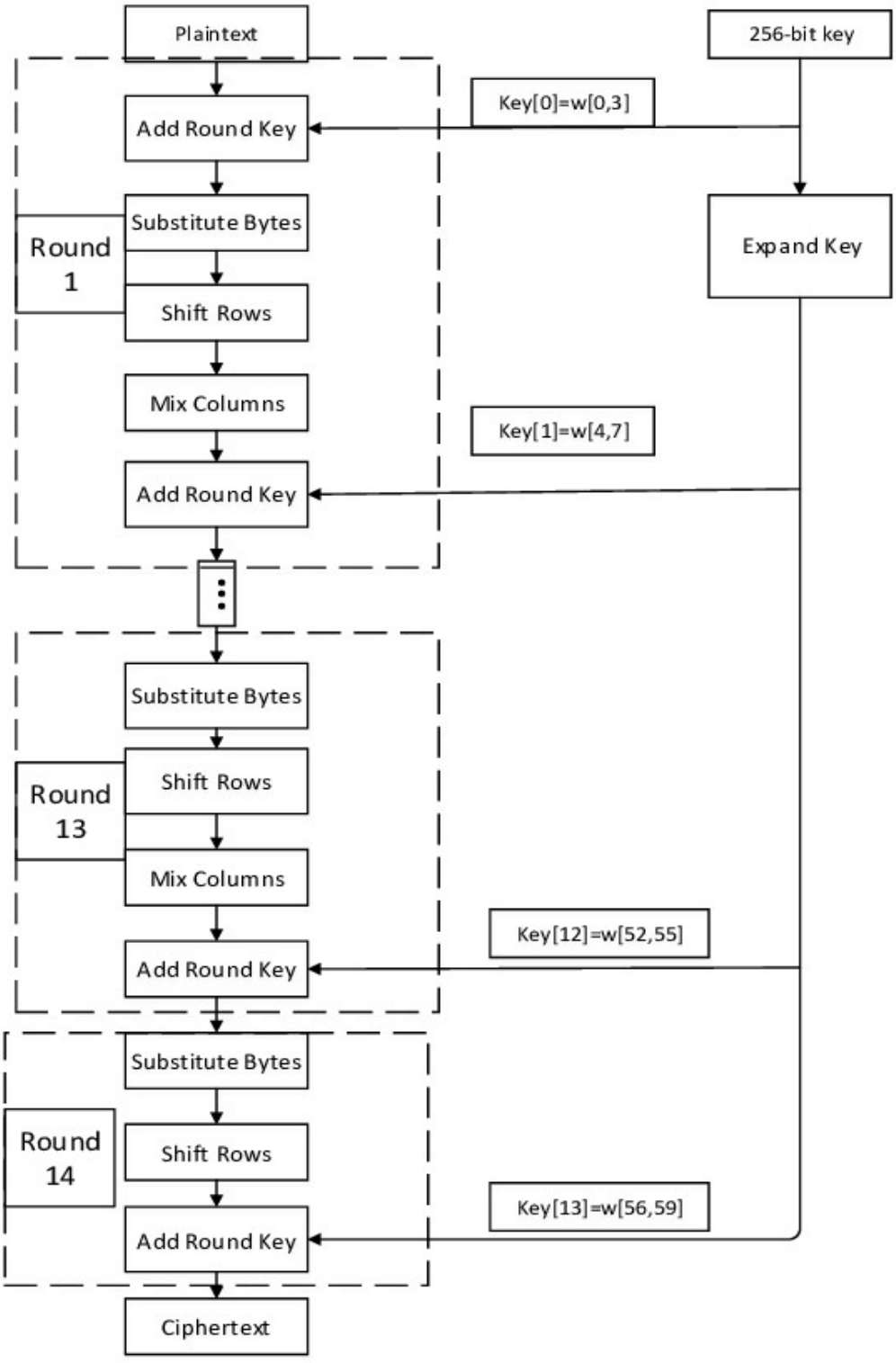

Figure 2: AES encryption with 256-bit of Key Length

4. IMPLEMENTATION

The system was implemented using PHP 5 object-oriented programming paradigm and MySQL relational database for storage. The proposed system is a hybrid model of AES encryption and ECC encryption. From the system architecture as seen in figure 2, the data to be encrypted is uploaded by the user into the system where it is stored in the database created for the encrypted files, AES algorithm, as seen in algorithm 1, generates an encryption/decryption key to encrypt plain text and is further encrypted with ECC algorithm, as seen in algorithm 2, to increase overall security of thesystem by implementing software based countermeasures to prevent possible vulnerabilities.The encrypted AES key is provided to the user which will be used to decrypt the AES keyblock at the time of decryption into its original format for the user to access.

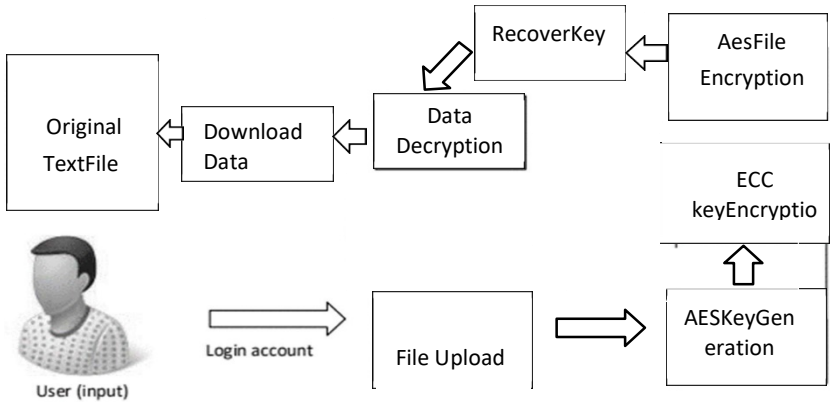

Figure 3: Architecture of Proposed System

Algorithm 1: AES Algorithm of 256 Bits Key and 14 Rounds ofIteration

Input: Uploaded Text File
Output: AES Encryption Key

a) Determine the set of round keys from the cipher key.
b) Initialize the state array with the block data (plaintext).
c) Add the initial round key to the starting state array.
d) Perform 13 rounds of state manipulation.
e) Perform the 14 and final round of state manipulation.

Algorithm 2: Elliptic Curve Cryptography

Input: AES Encryption key
Output: ECC encrypted key

a) Input AES generated key
b) ECC encrypts Key
c) Store Key in Database

5. RESULTS AND DISCUSSIONS

The results showed the encryption process performed on a text based file using the AES 256 encryption and ECC algorithm. Figure 3 shows the user login interface through which a user can gain access to the system. The main interface in figure 5 shows the program main interface which presents to the user two options either to upload a file or download a file. Figure 5 shows the data upload input form, through which data is uploaded to the database. The AES encryption algorithm is implemented at this point, which makes it possible for the data to be encrypted before uploading to the cloud storage. Everything including the file is encrypted on the process, it generates encryption key that will be used to also decrypt the file by recipient.

In order to enhance security, the encryption key generated by AES algorithm is also encrypted by ECC. Figure 6 shows the encrypted data which is loaded from the data base, each file present, has a unique identifier and also a decryption key generated by the AES algorithm during the time of upload, files without the decryption key become useless. The decryption button which is been used to select a particular data to be downloaded, here the ECC key encryption is being fully integrated to the AES encryption algorithm which will increase the security level, the encryption AES key is also encrypted by ECC on the file during the upload. The file was eventually decrypted to human readable form then it can be downloaded.

Figure 4: User Login Interface

.

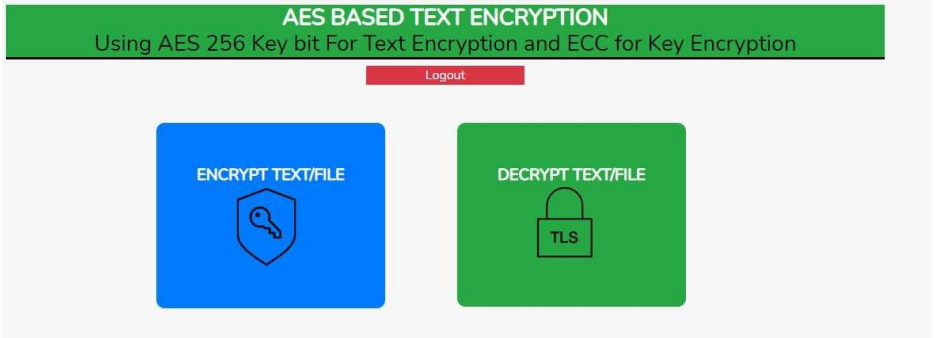

Figure 5: Main Interface

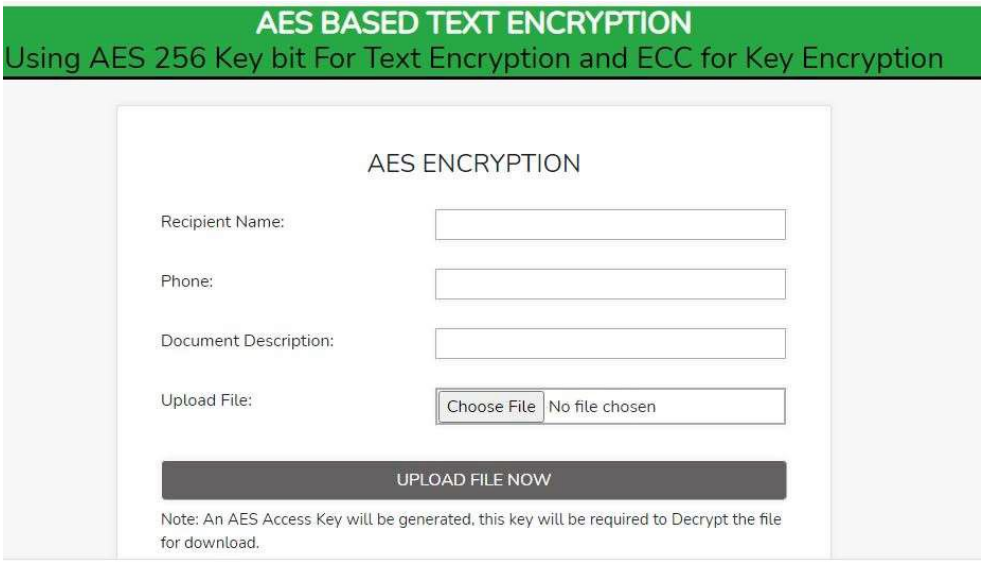

Figure 6: Upload Data (File) Interface

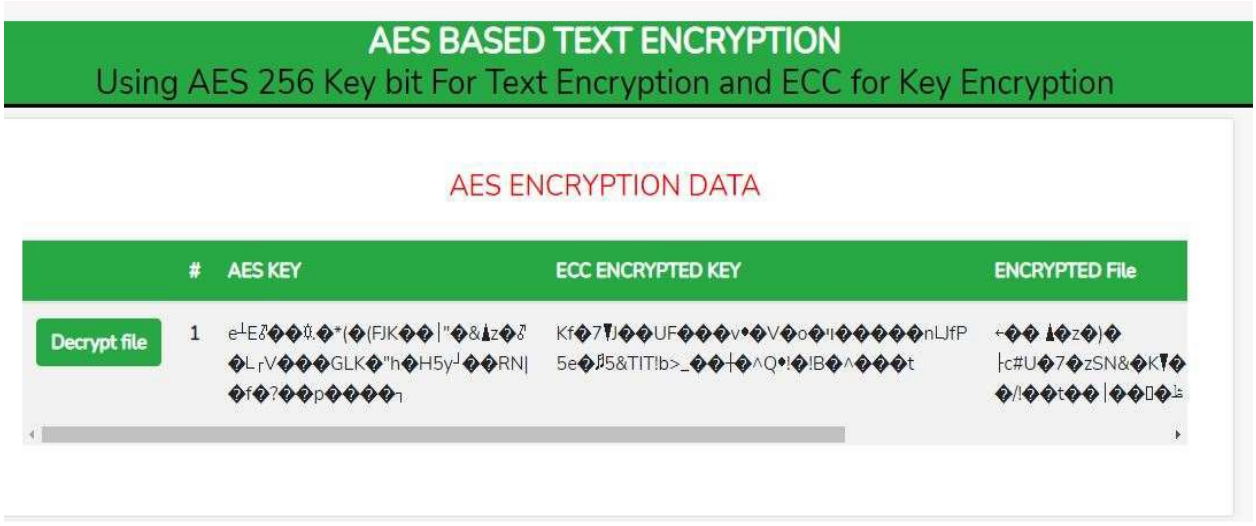

Figure 7: Data Encryption Interface

6. CONCLUSION

Without proper attention to data security, organization's information technology can become a source of significant mission of risks. Security of data has become a way of life within organizational context, thus the work presented a big data security system using hybrid techniques in cloud computing environment. The hybrid system comprised of Advance encryption standard (AES) algorithm gives more security to the data due to its encryption pattern thus serves as the first security level.

In the second security check, the ECC key encryption was adopted to improve security level across the network. The system proposed, provide better security model on big data management in cloud computing environment. This work will collaboratively increase the focus of the research and development community towards the trending data security using AES Encryption and Decryption techniques and also integration of ECC into cloud hosted applications where big data is been managed, which will ultimately lead to greater security and privacy in respect big data platforms in cloud computing environment.

In conclusion, data security plays an important role in the success of any organization. Hence, security of information is the security of an organization, thus a big data security using hybrid techniques has been developed.

REFFERENCE

1. Hayes. E, (2008). A Model for Cost-Benefit Analysis of Cloud Computing. Journal of International Technology & Information Management Electronic, 22(3),93–117.
2. Ilbert, M. (2015). Big Data for Development: A Review of Promises and Challenges.Development Policy Review. Retrieved from http://www.martinhilbert.net 1(3-6).
3. Jasleen Sushil & Rashmi (2015) "A Compound Algorithm Using Neural and AES for Encryption and Compare it with RSA and existing AES", Journal of Network Communications and Emerging Technologies (JNCET), 3(1).
4. Jayasinghe, D J Fernando, R Herath and R Ragel,(2010) "Remote Cache Timing Attack on Advanced Encryption Standard and Countermeasure," in IEEE International Conference on Information and Automation for Sustainability 1(2)177-182.
5. Jun Li, Q Dinghu, Y Haifeng, Z Hao and M Nie, (2011) "Email encryption system based on hybrid AES and ECC," in IET International Communication Conference on Wireless Mobile and Computing. 347 - 350.
6. Laney, D. (2001). 3D Data Management: Controlling Data Volume, Velocity and Variety, Information Systems International Journal of Advanced Research in Computer and Communication Engineering 47: 116-124.
7. Li X, J Chen, D Qin and W Wan, (2010) "research and realization based on hybrid encryption algorithm of improved AES and ECC"in IEEE International Conference on Audio Language and Image Processing 1(3) 396-400.
8. MacKenzie, T. (2002) Threshold password-authenticated key exchange. In, Advances in Cryptology, volume 2442 of Lecture Notes in Computer Science, pages 385400, Santa Barbara, CA, USA. Springer, Berlin, Germany 23-31.
9. Mannan, M. and P. Van Oorschot (2007). Using a personal device to strengthen password authentication from an untrusted computer. 1(2), 67-72.

10. Naveen Kumar, B. VenuGopal (2012) VLSI Implementation of Data Encryption Standard Algorithm. International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075,1(6)
11. Nentawe Y. Goshwe, (2013). Data Encryption and Decryption Using RSA Algorithm in a Network Environment. IJCSNS International Journal of Computer Science and Network Security, 13(7).
12. Nishtha Mathura and Rajesh Bansodeb (2016) "AES Based Text Encryption Using 12 Rounds With Dynamic Key Selection" in 7th International Conference on Communication, Computing and Virtualization 2016.
13. Radhika D.Bajaj and Dr. U.M. Gokhale (2016) " AES ALGORITHM FOR ENCRYPTION" in International Journal of Latest Research in Engineering and Technology (IJLRET) ISSN: 2454-5031. 2(5)
14. Renu Bhandari. (2013). Data Encryption and Decryption Using RSA Algorithm in a Network Environment. IJCSNS International Journal of Computer Science and Network Security. 13(7)
15. Tarakji, A. (2011). A Survey of Risks, Threats and Vulnerabilities in Cloud Computing. In: Proceedings of the 2011 International conference on intelligent semantic Web- services and applications. Amman, Jordan, 1–6.