Design of Multimedia Data Security System using Hybrid Cryptography

Gautam Kumar Jha [#1], Dr. R. R. Sedamkar [*2]

[#1, *2] Department of Computer Engineering, Mumbai University, TCET, Kandivali, India.

[#1] gautamjha229@gmail.com

[*2] *rrsedamkar@thakureducation.org*

ABSTRACT:

In the recent trend, information are increasing hugely everyday thanks to its usage. The data used can be in any format, it may be a text, image, audio and video etc. Securing data is one of the main challenges nowadays, as data passes through different medium where the medium is not secured. To prevent confidential knowledge from an unauthorized access there are variety of approaches. The way of centrosymmetric key cryptography and uneven key cryptography is getting used for changing information into completely different format for securing the multimedia system files.

This paper generally focuses on a technique used for encoding and decoding multimedia data like text, images and audio. Through this hybrid model which is formed on the assemblage of Deffie Hellman Key Exchange Algorithm, RSA Algorithm and Advanced Encryption Standard Algorithm. This hybrid method generates a collective secret key by exchanging keys between two users where the communication take place for sharing their facts thru the usage of Deffie Hellman Key Exchange algorithm then passes it to input data. This model focuses on the facts which is in a text format. The data which is not in a text format is first converted into a text form. The input data is rehabilitated into a text form and are encrypted through the assistance of RSA algorithm and further with AES algorithm. The encrypted facts will be decrypted first with an AES algorithm and at that time with RSA algorithm. The process involves encoding and decoding of data.

The advantage of this hybrid model is that it will provide security to the multimedia data and also fill the gap of storage, speed and security. Here data used are in diverse arrangements like it may be a text, image or audio. It is even used for societal for communication of data over the network.

KEYWORDS:

Security, Multimedia, Cryptography, DES (Data Encryption Standard), AES (Advanced Encryption Standard), Encryption and Decryption.

I. INTRODUCTION

In a communication system, security of information is a most important worry nowadays. There are bags of techniques like hashing, stegnography, cryptography that make available as for the safety of essential information. Confidential facts can be protected by the application of Encoding and Decoding systems as it takes an important part. In the primordial times, through the learning of past events the data were made unreadable by scrambling the contents of information to keep it secret. Cryptography algorithms like DES, AES, Blowfish, RSA and Deffie Hellman provides a higher level of security by using a duo of key in cooperation for encryption and decryption.

Deffie Hellman is an algorithm in which exchanging of keys takes place, in which keys are used for communication to exchange facts in an open network. It involves principally five steps as follows:

- Global Public elements
- User 'A' Key generation
- User 'B' Key generation
- Generation of secret key by user 'A'
- Generation of secret key by user 'B'

Initially the two global public elements are used, one is a prime number element and another is a number that is used as a primitive root of that prime number. In the following step, user 'A' choices a casual number which is slighter than the prime number and it is used as a private key. In the subsequent step user 'B' chooses a unplanned number which is smaller than the prime number and it is used as a private key. In the fourth step user B shares his private key with user A and then user A generates a secret key for switching data. Similarly, user B generates a secret key for switching data. In the last two steps we get the same result which is castoff as a common secret key.

AES is a centrosymmetric key algorithm where the plain text size is similar to a block size of 128,192,256 bits and the measurement of the key is alike as the size of the plain text i.e. 128,192,256 bits. It involves basically four steps as follows:

- Byte Substitution
- Shifting of rows
- Mix columns
- Add a round key

It has total rounds of 10, 12 or 14 to encode data liable to the plain text size of 128,192 and 256 correspondingly.

Initially bits are converted into bytes and organized in a matrix form. After which, data are replaced from the substitution box and are arranged again in a matrix form. In the further step shifting of rows take place provisional on the offset used, i.e. offset 0, offset 1, offset 2 and offset 3. Offset 0 means data will remain on the unchanged position there will not be any shifting of data whereas offset 1 means data will be shifted by one position and respectively. In the subsequent step columns are mixed in alike approach as of rows shifting. At the last, Addround key is added after the mixing of columns and the method repeats till the last rings contingent on the plain text size.

The result provided by Advanced Encryption Standard is much better and more rapidly than any other algorithm corresponding Data Encryption Standard. Deffie Hellman Key Exchange algorithm exchanges their reserved key and unrestricted key to prepare a common shared key for switching the data.

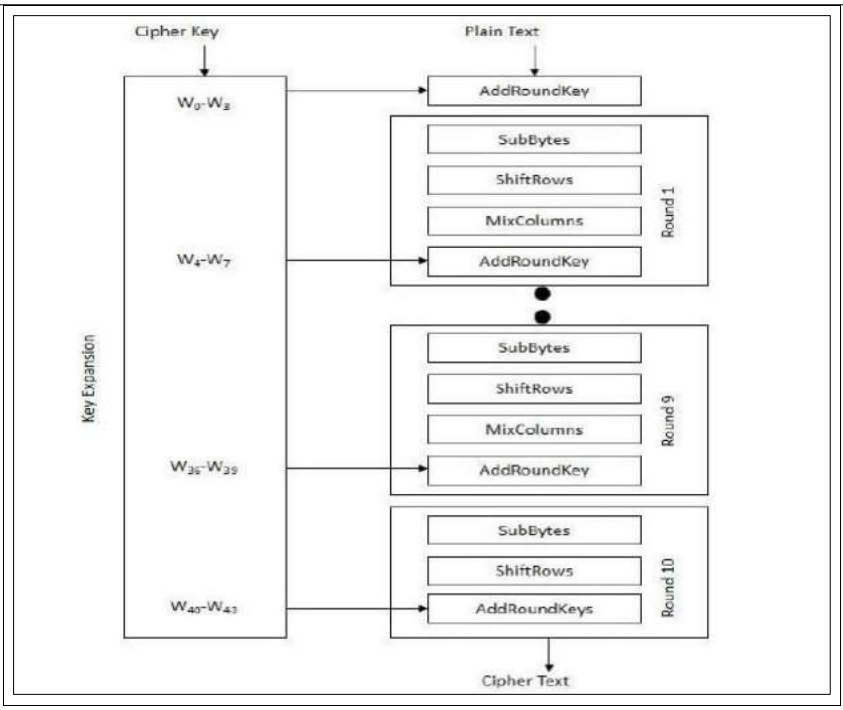

Figure 1: AES Process[8]

RSA is a disproportionate key algorithm where encryption of facts then decryption of facts are done with different key. It involves basically three steps as follows:

1. Key Generation.
2. Encryption.
3. Decryption.

In the initial stage, dualistic keys are generated one is a public key 'e' and other is a private key 'd'.

Key Generation

1. Select dual prime numbers p and q.

2. Calulate, Modulus n = p*q and then φ(n)=(p-1)(q-1).

3. Choose 'e' as a public key which lies in between 1<e<φ(n) and e and φ(n) necessarily be co-prime.

4. Calculation of 'd' which is a private key is done on the derivation of 'demodφ(n)=1'.

Encryption

Here 'C' is a cipher-text, 'M' is a plain text, n is multiplication of two prime numbers and ‘e’ is a public key used for encryption.

$$C=M^e \bmod n$$

Decryption

Here 'M' is a plain text, 'C' is a cipher-text, n is multiplication of two prime number and ‘d’ is a private key used for decryption.

$$M=C^d \bmod n$$

This amalgam algorithm is intended by combining DHM, RSA and AES to translate the multimedia data by converting it into a text, equivalent to reduce the overall time constraint and deliver a high level of security.

II. MOTIVATION

The safekeeping of multimedia data in an efficient manner to cope the perils associated with it and maintains the security requirement.

Security of data to avoid, the loss of information by most convenient methods in a extra secure way.

III. OBJECTIVE

The objective of this work is to boost the security of multimedia data.

It also fills the breach of storage, speed and security along the communication of facts over the network.

IV. LITERATURE SURVEY

A. Multiple layer Text security using Variable block size Cryptography and Image Steganography

In the cryptography large amount of research has been done to keep the data secured. The techniques of cryptography and steganography are castoff to secure a text by multiple layer approach. In this approach, the text is renewed into cipher text using cryptography methods of flexible block size and that cipher text is secreted in an image using steganography approach. These methods deal only with the image files. The future scope can be providing Security for Multimedia files like image, audio and video can be done. [2]

B. DES, AES and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis

DES (Data Encryption Standard) is a symmetric key algorithm, where the unchanged key is castoff for encryption and decryption of facts and it started to demoralize because of its natural limitations. It uses 64-bit plain text message along with 56 bits of key for encrypting it into a 64-bit cipher text. Because of the usage of small key length, it makes it susceptible to brute force attack as cipher is simple and straightforward.

These limitations were overcome using Triple DES which means three times DES is carried out by a duo of key of size 112 or 168-bit. The encryption method of transmuting plain text into cipher text in 3DES takes relatively more time as compared to simple DES. To overcome the limitations of DES, a new cryptographic proposal AES or subset of Rijndael cipher was given by two Belgian cryptographers, Joan Daemon and Vincent Rijmen. In AES, its liable on the amount of rounds i.e. 10, 12 or 14 rounds it uses a single key of size 128, 192 or 256-bit which is identical as the size of the plain text. AES has been classified into four stages of Byte substitution, shifting of rows, mix columns and add a round key for all round excluding the last round to provide the equivalent cipher-text. DES is sooner in performance comparison than AES, but it deficiencies in standings of security. The asymmetric key-based encryption algorithms use the couple of keys; a unrestricted key and a reserved key which is mathematically bounded to each other. The future scope is to increase the extent of key to get better results.[3][4]

C. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems

RSA is an asymmetric key based encryption technique which is used widely and for sharing the statistics through the communication channels it uses 1024-bit key stream. Message confidentiality in RSA is solely dependent on huge prime number then discrete logarithm problem. It is highly secured and provides safety to online operation data over the communication network. In a research article by Boneh, specified the limitations in RSA and the various possible attacks happening to RSA

cryptosystem. It is stress-free to recognize the private key if planned properly by using a scheduling attack.

In just 10 repetitions an author has claimed to obtain 508 bits of 512 bits RSA. The scope can be to increase the Usage of both Pubic Key and Private Key. [5]

D. Stegnography for Inserting Message on Digital Image Using LSB and AES Cryptographic Algorithm

In this data are scrambled with the assistance of AES algorithm. The data which is to be converted are in text format. It practices Least Significant Bit method for inserting data on a digital image to make it extra secure. The system is not much secure as it uses only Least Significant Bit. It deals only with the image files. Scope can be by providing Security for Multimedia data like image, audio and video can be done. [6]

E. Securing Data in Cloud Using AES Algorithm

Data in file format are scrambled by encryption technique. The files are encrypted with the AES Algorithm. The proposed system will work only when there is a stable internet connection. AES Algorithm's steps are followed in it, which store data on the cloud in the encrypted format will be downloaded or decrypted with usage of concepts of keys. The proposed system can be applied in numerous arenas like Voice communication, Network appliances and Virtual Private Network. Future scope can be increased by implementing for other data like images, audios etc. [7]

F. Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data

In this paper, it describes all the processes of AES. The procedure used for encoding data along with decoding data for making dataA. Multiple layer Text security using Variable block size Cryptography and Image Steganography

V. PROBLEM DEFINITION

After studying the restrictions of the present existing system, and sensing that there is a need of a more effective system to secure multimedia data in various terms as follows:

Time Complexity, as in many approaches the system contains complex parts which increases the time complexity but the simple systems has less time complexity. So the compromise between two is must needed.

Memory Efficiency, the text encryption method require less memory as equated to the multimedia data encryption. Therefore the compromise between two is must needed.

Input supported, the system used till now only deals with the text in the direct form or taken from some files. Multimedia files uses image, audio, graphical contents require large memory for storage and the time required for the determination of encoding and decoding is also high.

VI. DESIGN AND METHODOLOGY

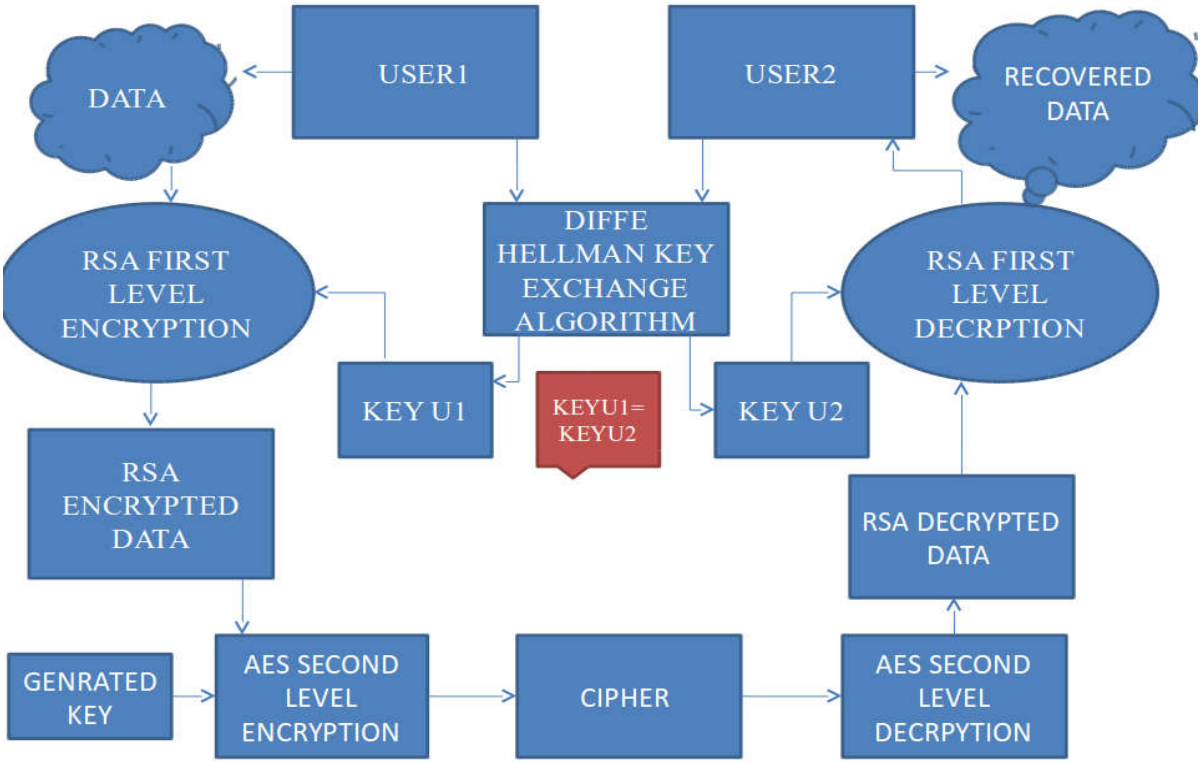

Figure 2: System Model

The system model provides security to the multimedia data by compounding three algorithm viz. DHM algorithm, RSA and AES.

DHM algorithm create a shared secret key by exchanging their keys between the two users. This common secret key is basically used for communication between two users. The data will go for first stage of encryption with RSA which gives RSA encrypted data. This encrypted data will go for second stage of encryption with AES algorithm and provide a cipher text. This cipher text will go for first stage of decryption which provide a RSA encrypted data. This encrypted data will further go for second stage of decryption with RSA which results into the plain text data.

The facts in a text form will work as the process shown in the system model. The facts in an image form must be converted into a text form and the method will be followed for further process of encryption and decryption. The data in an audio form must be converted into a text form. The multimedia facts like text, images and audio are encrypted with the assistance of RSA and AES algorithm.

VII. IMPLEMENTATION AND RESULTS

This papers shows a hybrid encryption system for securing the multimedia data type like any file, images, audios etc.

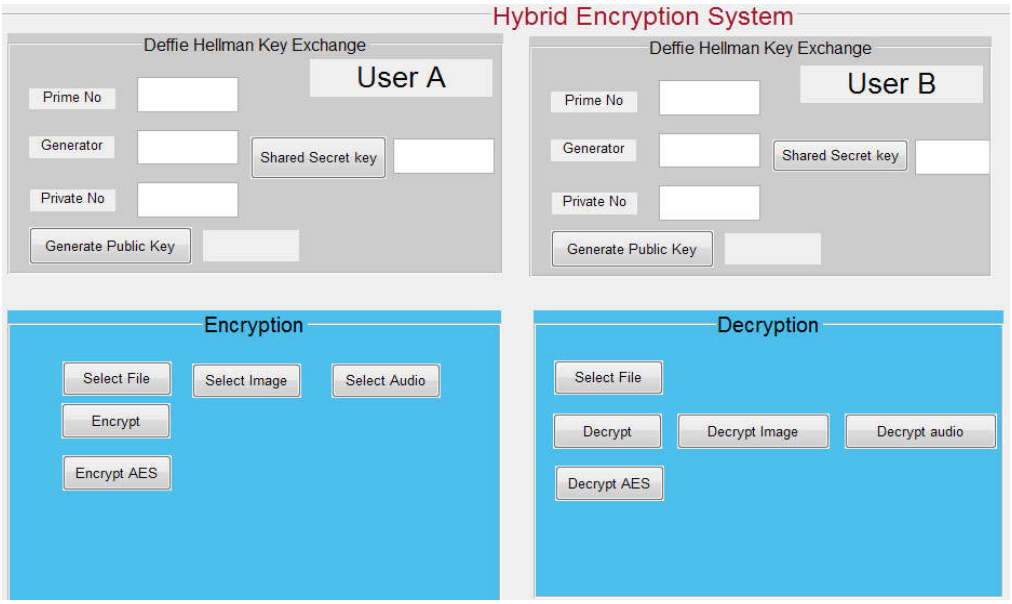

Figure 3: Hybrid System Model

Process of Deffie Hellman key exchange algorithm where keys are shared between two users for sharing their data with the help of shared secret key.

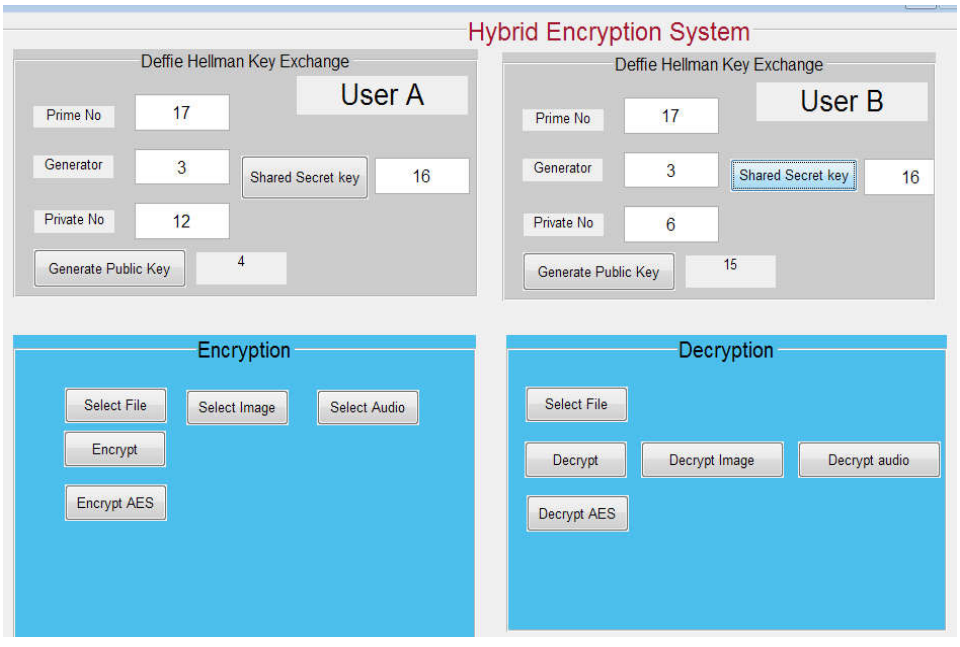

Figure 4: Process of Deffie Hellman

Here User A generates a Public key and similarly User B generates a Pubic key. Later it generates a shared secret key for communication purpose.

In the procedure of encryption first choose the file which is in a text layout will go for encryption

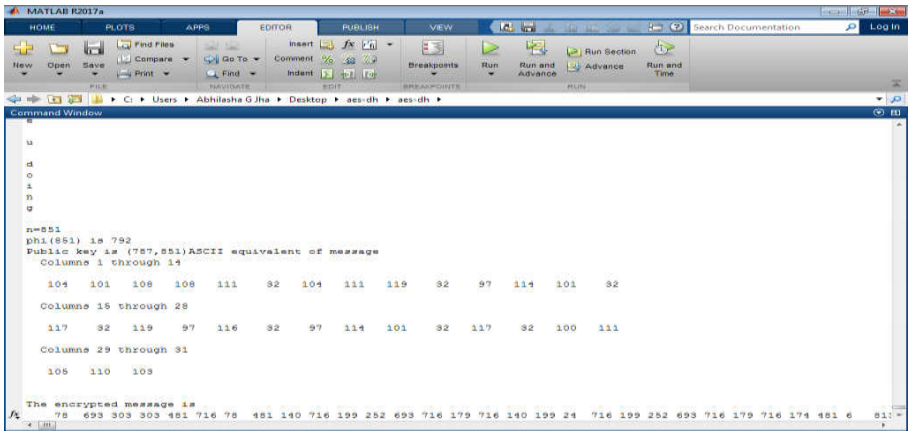

Figure 5: Encryption of data using RSA

After encryption with RSA, it goes for encryption with AES algorithm.

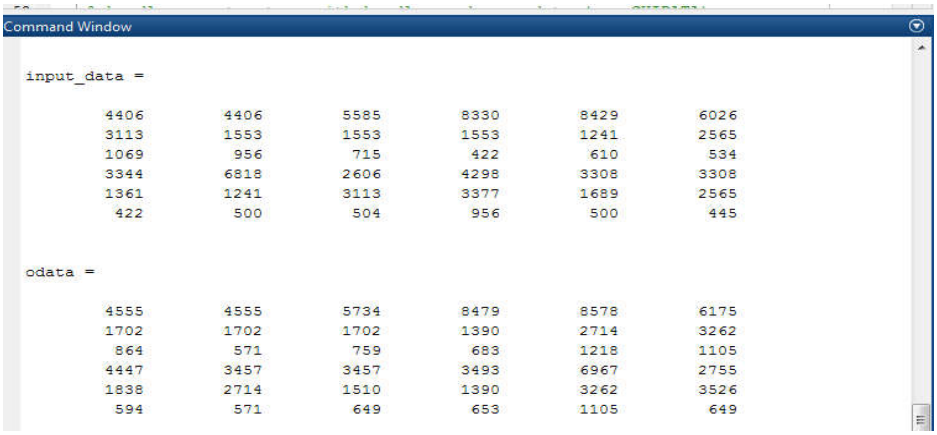

Figure 6: Encryption of data using AES

It will go for decryption with AES algorithm

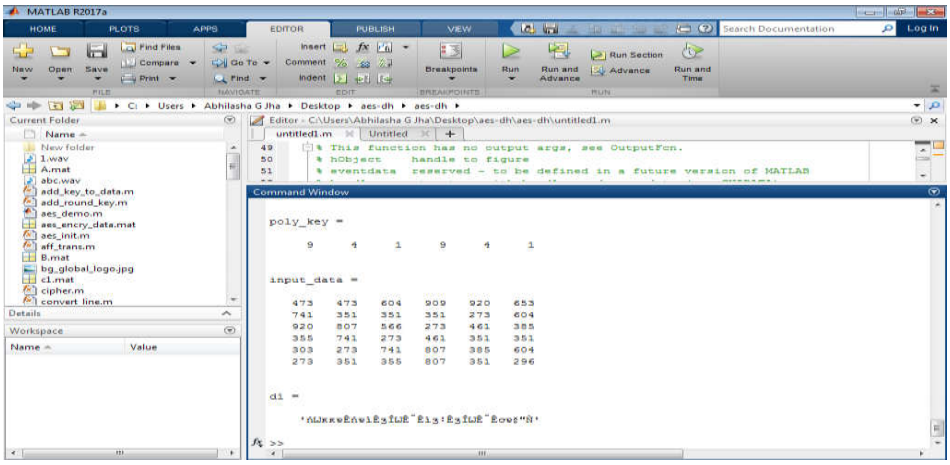

Figure 7: Decryption with AES

Result generated after decryption of data with RSA algorithm

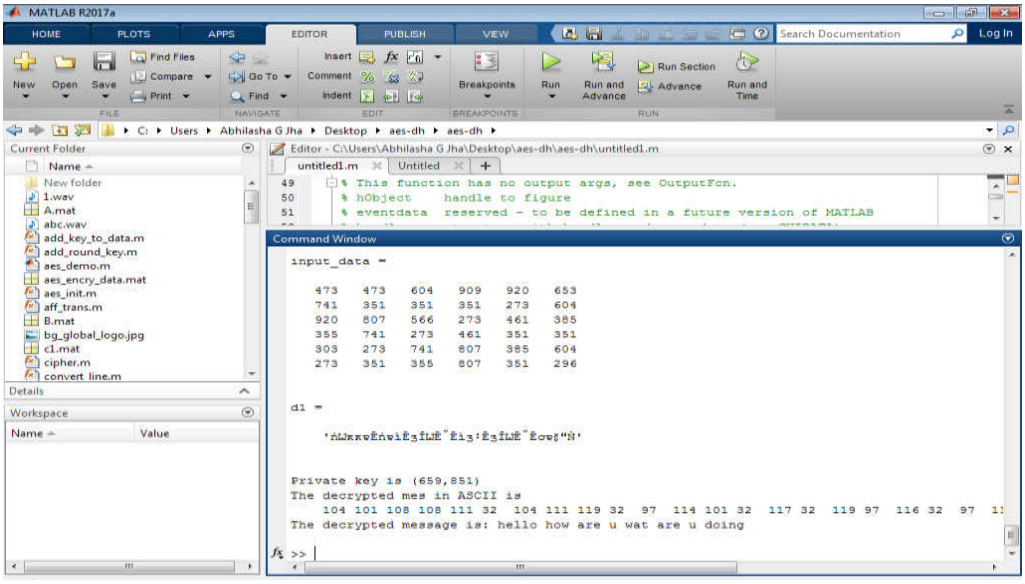

Figure 8: Decryption with RSA

In the encryption of image, it is first resized into 256*256 image. The image is first converted into text format and the process involves as encryption with RSA and AES algorithm. Decryption involves with AES and RSA.

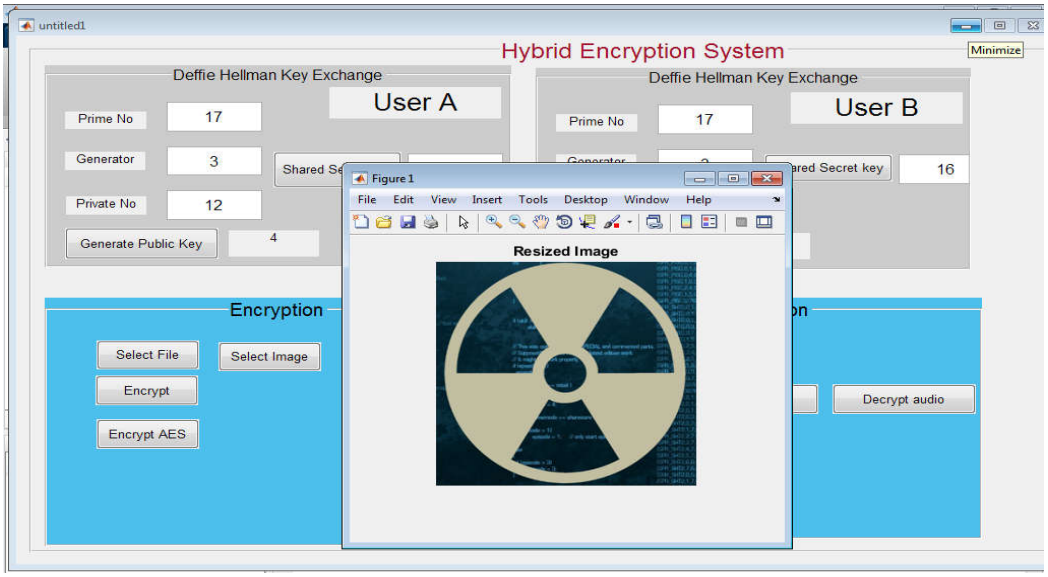

Figure 9: Select image

The image after converting into text and applying encryption process.

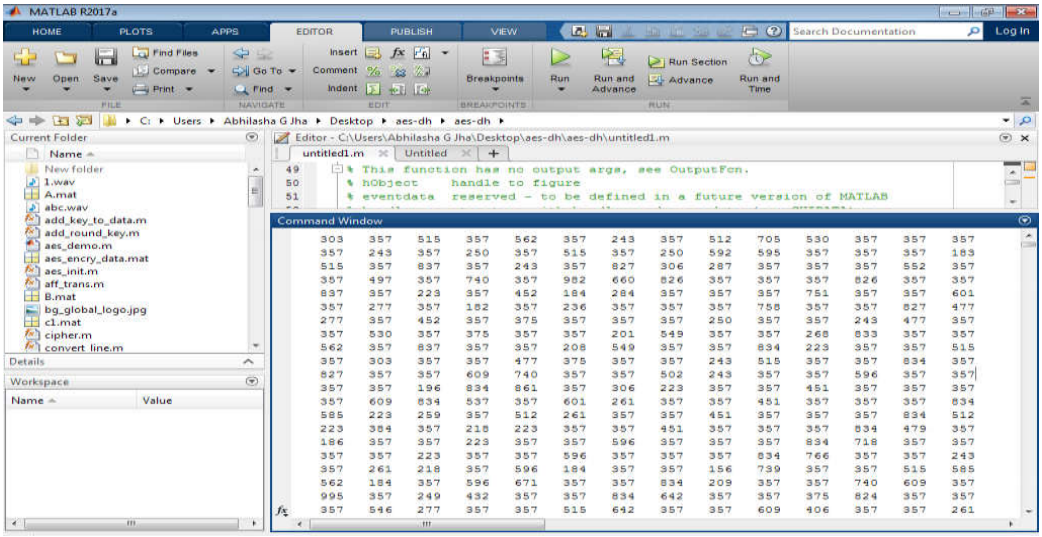

Figure 10: After Encryption

After the encryption, we apply the decryption of data with AES and RSA

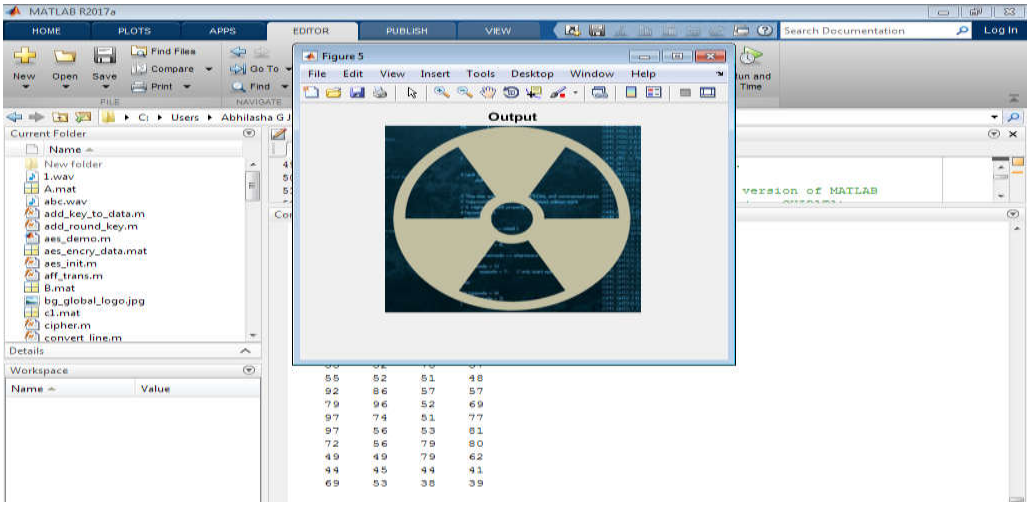

Figure 11: Image after Decryption

The process is similarly carried out for the audio file, where an audio is converted into text arrangement first. Now this data which is in text format will go for encoding with RSA algorithm and AES algorithm and similarly it goes for decoding.

VIII. CONCLUSION

The hybrid model is prepared by combination of three cryptography algorithms viz Deffie Hellman Key Exchange algorithm, RSA algorithm and AES algorithm. It provides result faster and in efficient manner. The data in the text format provides the result faster. The data in an image format and in audio format must be first converted into text format. Here matters the size of data as data size is small result is very fast and if the size of data is high it takes comparatively time to secure the data. It provide better results by providing high level of security to the multimedia data then the current existing system. It will

be used to secure the multimedia data in the form of a file, image, audio etc. and also provide better memory efficiency.

VII. REFERENCES

[1] W.Stallings, "Cryptography and Network Security: Principles and Practices, fourth edition", pp.592, November 2005.

[2] *Shivani Chauhan, Jyotsna, Janmejai Kumar, Amit Doegar, Multiple layer Text security using Variable block size Cryptography and Image Steganography, 3rd IEEE International Conference on "Computational Intelligence and Communication Technology" (IEEE-CICT 2017).*

[3] Daemen, Joan, Rijmen, Vincent. (March 9*)*, AES Proposal: Rijndael. *National Institute of Standards and Technology* 2003; p. 1. Retrieved 21 February 2013.

[4] Jawahar Thakur, Nagesh Kumar. DES, AES and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis. *International Journal of Emerging Technology and Advanced Engineering* December 2011; vol 1(2), p.6-12.

[5] R.L. Rivest, A. Shamir, and L. Adleman. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems.*Communications of the ACM* 1977; p. 120-126.

[6] Nurhayati, Syukri Sayyid Ahmad, Steganography for inserting message on digital image using least significant bit and AES cryptographic algorithm. IEEE Conferences 2016.

[7] Prasoon Raghav , Rahul Kumar , Rajat Parashar, Securing Data in Cloud Using AES Algorithm. International Journal of Engineering Science and Computing, April 2016;Volume 6 Issue No. 4. ISSN 2321 3361 © 2016 IJESC.

[8] Ako Muhammad Abdullah, Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data; Research Gate.

[9] wikipedia.org,"Deffie Hellman Key Exchange Algorithm", https://en.wikipedia.org/wiki/Diffi%E2%80%93Hellman_key_exchange

HYPERLINK "https://en.wikipedia.org/wiki/Advanced_Encryption_Standard"https://en.wikipedia.org/