SECURE AND SCALABLE VIDEO TRANSMISSION

Damini Sharma[1], Pradnya Dhepe[2], Vinaya Mane[3], Priti Giri[4], Prof. Poonam Pate[5]

[1] Student, Computer Engineering, Sinhgad Academy Of Engineering, Maharashtra, India
[2] Student, Computer Engineering, Sinhgad Academy Of Engineering, Maharashtra, India
[3] Student, Computer Engineering, Sinhgad Academy Of Engineering, Maharashtra, India
[4] Student, Computer Engineering, Sinhgad Academy Of Engineering, Maharashtra, India
[5] Professor, Computer Engineering, Sinhgad Academy Of Engineering, Maharashtra, India

ABSTRACT

.In modern world use of Internet and multimedia transmission has become popular. Hence, it has become important to protect the confidentiality and security of this data which is being transmitted over wide networks. This paper is based on the security and scalability of video transmission. In order to protect the video content from being accessed and misused by malicious attackers and unauthorized users we are using graphical as well as graphical text based passwords for secure authentication. Then we are using AES (Advanced Encryption Standard) for standard encryption and decryption of video content. These two entities make our transmission system highly secure.

Keyword : - *AES, Encryption, Graphical passwords, etc….*

1. Introduction

While transmitting multimedia data we need to secure the data. For securing the data while transmitting we have implemented security measures especially for login. We have implemented security for logging so that only authenticated person can login for accessing the video and multimedia data. We have used graphical as well as graphical text based password which is more secure than traditional text password. This two-level authentication process prevents shoulder surfing attacks which are common in traditionally used text passwords. Malicious attackers cannot hack these kinds of passwords easily. While transferring the video content we have used compression technique so as to reduce the size of video and transfer it in a faster way. After compressing we have encrypted the video so as to keep the data secure. Same procedure is followed on the receiver side. Authenticated person logins using the same technique of graphical and graphical text based password. The video which is received on the receiver side is decompressed and then the video is decrypted for further usage.

2. Literature Survey

Lei Yuan, Huaan Li. has proposed schemas which can address the challenging task of multimedia transmission in wireless packet network. Multimedia transmission is a tedious task due to time-varying channel characteristics and heterogeneity of end-user devices like laptop, tablet and mobile phone. In this paper, the author has discussed Layered media coding schemes, such as scalable video coding (SVC), extension of H.264/MPEG-4 AVC and progressive image coding which are proposed to meet the complex multi-platform requirements of the multimedia and Internet era[1].

Nentawe Y. Goshwe. RSA algorithm allows a message sender to generate a public keys to encrypt the message and the receiver is sent a generated private key using a secured database. An incorrect private key will still decrypt the encrypted message but to a form different from the original message**.** RSA algorithm converts the information to a not understandable form by the intruder hence protecting unauthorized users from having access to the information[2].

Gurpreet Singh. analyzed the three popular encryption algorithms DES, RSA and AES, and gave their comparative study in terms of various factors like various encryption and decryption methods, their computational issues and security. Due to the rapid development of multimedia technology (internet and mobile devices) the security of video in the communication field has become the major concern. Use of multimedia data transmission has become more and more popular due to the wide use of internet all around the world which makes it necessary to implement various video protection techniques to keep that information secured from irrelevant malicious attackers. This paper, focuses on how to choose which encryption algorithm can be used to exchange video safely, and maintain the balancing between the security and computational time[3].

Mandeep Singh Narula. presents the design and the implementation of the Triple Data Encryption Standard (DES) algorithm. Triple-DES (TDES) is basically used in various cryptographic applications and wireless protocol security layers. A much more secure version of DES is called Triple-DES (TDES). It is equivalent to using DES three times on plaintext with three different keys. Consequently, it is three times slower than the original form of DES but it is way more secure. In this paper a complete examination of full procedure of implementing a DES and Triple DES algorithm using a high-level hardware description language Verilog[4].

Md Imran Alam. has discussed efficiency analysis and performance of various block cipher algorithms such as (DES, 3DES, CAST-128, BLOWFISH, IDEA & RC2) of Symmetric Key Cryptography. Here, block cipher algorithms have been compared based on the following factors, viz. input size of data (in the form of text, audio and video), encryption time, decryption time, throughput of encryption and decryption of each block ciphers and power consumption. On performing experiments it can be found that, if throughput value of a block cipher is increased then power consumption value of that cipher is decreased which helps in performance analysis of algorithms[5].

Pooja Deshmukh. has proposed a modified AES based algorithm for heavy-weight encryption of MPEG video data. The MPEG video stream is quite different from the normal program code or textual data because there are interframe dependencies and redundancy factors present in MPEG video structure. Therefore, special MPEG video encryption algorithms are required because of their special characteristics which are coding structure, large amount of data and real-time constraints. The algorithms like RSA, DES, IDEA involve complex computations. This paper provides a modified AES algorithm which can provide secure encryption of high quality videos[6].

Dhananjay M. Dumbere. has introduced various approaches based on which video encryption can be done. These approaches provide a proper classification in terms of what is selected for encryption which can be based on the content to be encrypted or the various characteristics or the structures of the content to be encrypted securely. In order to protect unwanted interception and viewing of any video while in transmission over the networks, this paper focuses on implementing AES algorithm for encrypting and decrypting the video securely over Internet and multimedia technology[7].

Guang-liang Guo. has proposed a detailed study about the different optimized designs and implementations of AES algorithm. It tests the fast implementation of AES algorithm and the performance has been improved by about 50 times when compared to the standard AES algorithm; It also explains how by using the Intel AES-NI extended instruction sets, the performance has been improved by about 50 times compared with the fast implementation of AES algorithm; Lastly, how by using CUDA and GPU to execute the AES in parallel can improve the performance by about 18 times compared with the fast implementation of AES algorithm[8].

Hung-Min Sun. has introduced Pass Matrix which protects users from becoming victim of shoulder surfing attacks and it uses one-time login indicator. Login indicator expires as the session ends. In Login indicator user uses a dynamic pointer to point out the position of their passwords instead of clicking on password directly. Attackers can observe directly or use external recording devices to collect users' credentials. Pass Matrix was introduced to resolve the problem based on graphical passwords to resist shoulder surfing attacks[9].

D. D. Walanjkar. has introduced graphical passwords to overcome the defects of text based password. Graphical Password contains images which when selectively clicked in a certain sequence creates a desired password. We have chosen this over traditional text based password so as to avoid dictionary attacks which is major security threat in online applications. In text based password attacks like eavesdropping attack, dictionary attacks, denial of service attacks may take place. To overcome the disadvantages of text based password, graphical password are used. Click based graphical password schemes offer a good approach to images and password such as Pass Points, that often leads to weak password choices[10].

Bin B. Zhu. has proposed CarP. CaRP(Captcha as gRaphical Passwords) is obtained by clicking on image to obtain the password. A new captcha is generated at every login attempt. Graphical password systems was introduced on enhancement of Captcha technology, termed as Captcha as graphical passwords (CaRP). CaRP is both a Captcha and a graphical password scheme. CaRP addresses a number of security problems such as online guessing attacks, relay attacks. CaRPs conists of text Captcha and image recognition Captcha. One of them is a text CaRP wherein a password is a character sequence like a text password, however it is entered by clicking the right character sequence on CaRP images[11].

Shraddha M. Gurav. has focused on the adoption of graphical passwords. We have bundle of images on screen through which the user selects the password. It is very difficult for hacker to make the combination of images i.e password and for every time images are different for each case. Graphical password is one of the alternative solution to alphanumeric password as it is very tedious process to remember alphanumeric password. According to human mind it is easy to remember the images than text based password[12].

Amish shah. Has described the use of graphical passwords in modern day applications and how they prevent various security threats and attacks. Graphical passwords are not easy to guess and they also prevent brute force attacks. Text based passwords have its own flaws and are highly vulnerable to attacks. One of the attacks is shoulder surfing attack in which the person is watching the password over the user's shoulder when the user is entering the password. Shoulder surfing attack is also called as peeping attack[13].

Mrs. Aakansha S. Gokhal . has given a detailed study on the types of graphical passwords and the performance efficiency of each type. Basically the types of Graphical Passwords are Recognition based and recall based. Recognition based: In this, user is presented with a set of random images during registration. The user has to select the number of images from this to set as a password. At the time of authentication, user has to recognize those preselected images in a correct sequence. Images are presented on screen for user and the user has to click on right images and in a right sequence. Recall based: In this, during login phase user is asked to recall (reproduce) something that he/she has created or selected during the registration phase. While registering the user has chosen images, so in this the user has to reproduce something that the user has chosen[14].

3. PROPOSED SYSTEM

3.1 SYSTEM ARCHITECTURE

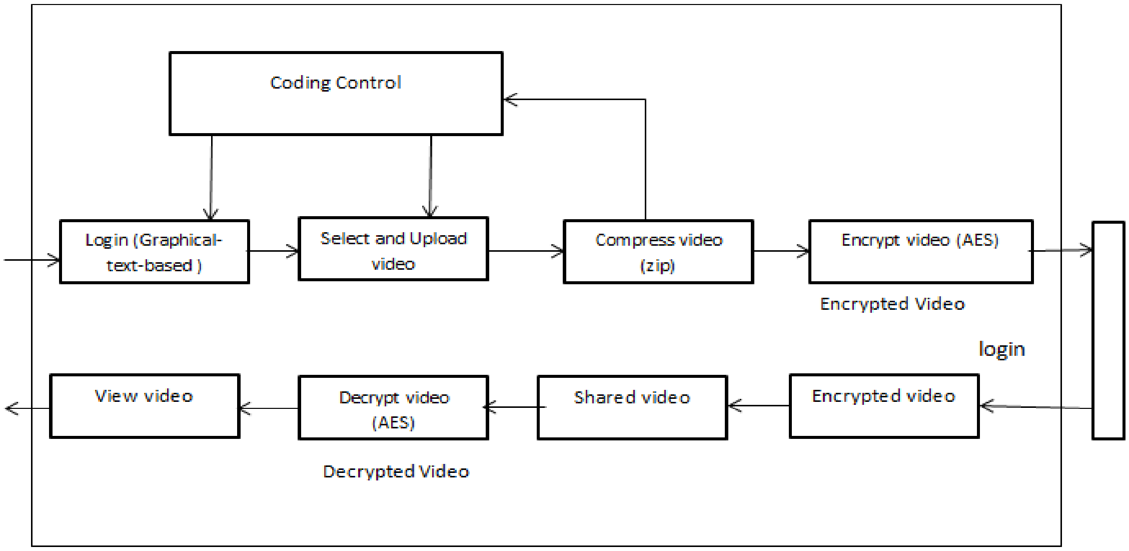


Fig -1: System Architecture

3.2 AES (Advanced Encryption Standard):

This AES algorithm has been used for standard Encryption and Decryption of multimedia data for transmission over a wide network. It has various versions according to the length of key that is used in a particular application, viz. they are 128-bit, 192-bit and 256-bit. We will be using AES for 128-bit key size in our application. AES goes through 10 rounds and four major operational steps in each round before producing the final encrypted data. All the steps in AES algorithm and their complete working is explained as follows:-

❖ **AES CBC Encryption and Decryption Algorithm:**

This algorithm provides the following cryptographic functionalities

- Encryption using AES
- Decryption using AES

1. Generate a AES key (specify the Key size during this phase)
2. Create the Cipher
3. To Encrypt : Initialize the Cipher for Encryption
4. To Decrypt : Initialize the Cipher for Decryption
    - **Step 1.** Generate an AES key using Key Generator. Initialize the key size to 128 bits (16 bytes)
    - **Step 2.** Generate an Initialization Vector (IV)

      a. Use Secure Random to generate random bit. The size of the IV matches the block size of the cipher (128 bits for AES)

      b. Construct the appropriate IvParameterSpec object for the data to pass to Cipher's init() method.
    - **Step 3.** Create a Cipher by specifying the following parameters.

      a. Algorithm name - here it is AES
      b. Mode - here it is CBC mode
      c. Padding - e.g. PKCS7 or PKCS5
    - **Step 4.** Initialize the Cipher for Encryption
    - **Step 5.** Encrypt the Data

      a. Declare / Initialize the Data. Here the data is of type String

      b. Convert the Input Text to Bytes

      c. Encrypt the bytes using doFinal method
    - **Step 6.** Decrypt the Data

      a. Initialize a new instance of Cipher for Decryption (normally don't reuse the same object). Be sure to obtain the same IV bytes for CBC mode.

      b. Decrypt the cipher bytes using doFinal method.

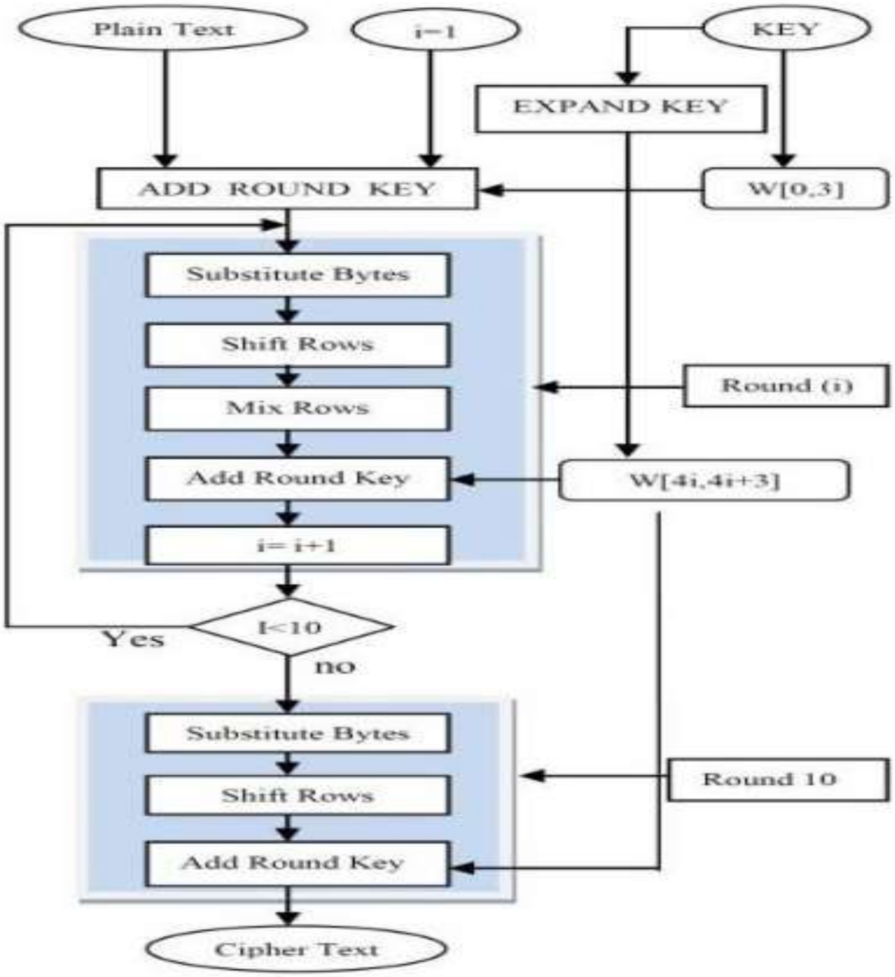


Fig -2: AES (Advanced Encryption Standard) process [3]

3.3 Graphical Password:

This has been used over text based password. It contains multiple images in a grid format. The user has to select the sequence of images to set as password. These images are set as password during the registration process. Then when the user login into the system he/she can directly enter that particular sequence of images which have been set as password during registration.

Ps
FEEDBACK

Fig -3: Graphical Password

3.4 Graphical Text Based Password:

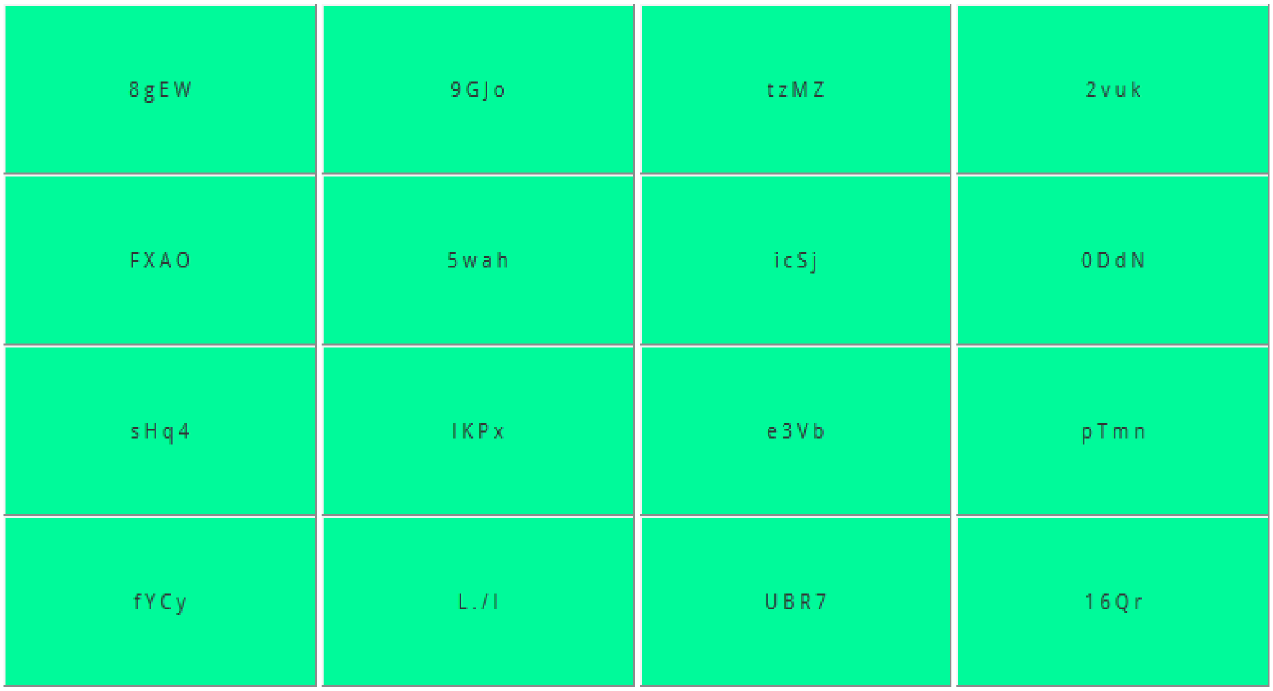
In this, in each block of the grid there is a combination of alphabets (upper and lower case), numbers and symbols. The password that we have set in text based is selected from a combination of alphabets, numbers and symbols from the block and every time the combination is generated randomly. The combination does not repeat any pattern.

- **Algorithm of Graphical Text Based Password**:

Input: 64 character a to z=26, A to Z=26, 0 to 9=10 and ". /"=2

Output: Random Printing Algorithm:

Step 1. To generate the matrix with row and column 8*8.
Step 2. Put 0 to 63 numbers into matrix.
Step 3. Select one random number from 0 to 63.
Step 4. For putting number into matrix system check number is already parent or not.
Step 5. If number is present then perform Step 3.If not present then put into a matrix and go to step 3.
Step 6. Do step 5 repeatedly up to 0 to 63 inserted into matrix.
Step 7. Print The Matrix.
Step 8. Now Get string which have 64 character " a to z=26, A to Z=26, 0 to 9=10, and. /=2".
Step 9. Get number present into matrix sequentially [0][0] to [8][8] i.e., total 64 character .
Step 10. Select index of string from 64 char. put into that Current location.
Step 11. Do step 9 and 10 repeatedly up to [8][8] number.
Step 12. Print Current Matrix With String Char.
Step 13. Display a matrix With Random Printing
Step 14. Stop.



8gEW	9GJo	tzMZ	2vuk
FXAO	5wah	icSj	0DdN
sHq4	IKPx	e3Vb	pTmn
fYCy	L./I	UBR7	16Qr

Fig -3: Graphical - Text based Password

4. CONCLUSION

In this paper, we have proposed a secure and scalable video transmission scheme for multimedia transmission over a huge network like Internet. The system is protected with highly secure graphical text based password authentication for valid users. The data will be transferred securely over the network since it will be encrypted with highly secure AES algorithm. AES prevents the attacks of malicious users on the video and multimedia data being transferred from one secured system to another system.

4. FUTURE SCOPE

- **Live video Conferencing:** There can be transmission of live video conferences.
- **Size of video:** There will be no limitations on larger size videos.
- Make transmission compatible with lower bandwidth/slow internet connections.

5. REFERENCES

[1] Lei Yuan, Huaan Li, “A Novel UEP Fountain Coding Scheme for Scalable Multimedia Transmission”, IEEE Transactions on Multimedia, Vol. 00, No.00, August 2015.

[2] Nentawe Y. Goshwe, “Data Encryption and Decryption Using RSA Algorithm in a Network Environment”, IJCSNS International Journal of Computer Science and Network Security, VOL.13 No.7, July 2013.

[3] Gurpreet Singh ,Supriya, “A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security”, International Journal of Computer Applications (0975 – 8887) Volume 67– No.19, April 2013 .

[4] Mandeep Singh Narula, Simarpreet Singh, “Implementation of Triple Data Encryption Standard using Verilog”, Volume 4, Issue 1, January 2014, International Journal of Advanced Research in Computer Science and Software Engineering.

[5] Md Imran Alam, Mohammad Rafeek Khan, “Performance and Efficiency Analysis of Different Block Cipher Algorithms of Symmetric Key Cryptography”, Volume 3, Issue 10, October 2013, International Journal of Advanced Research in Computer Science and Software Engineering.

[6] Ms. Pooja Deshmukh, Ms. Vaishali Kolhe, “Modified AES Based Algorithm for MPEG Video Encryption”, ICICES2014 - S.A. Engineering College, Chennai, Tamil Nadu, India.

[7] Dhananjay M. Dumbere, “Video Encryption Using AES Algorithm”, 2nd International Conference on Current Trends in Engineering and Technology, ICCTET’14, IEEE Conference Number - 33344, July 8, 2014, Coimbatore, India.

[8] Guang-liang Guo, Quan Qian*, Rui Zhang, “Different Implementations of AES Cryptographic Algorithm”, 2015 IEEE 17th International Conference on High Performance Computing and Communications (HPCC), 2015 IEEE 7th International Symposium on Cyberspace Safety and Security (CSS), and 2015 IEEE 12th International Conf on Embedded Software and Systems (ICESS).

[9] Hung-Min Sun, Shiuan-Tung Chen, Jyh-Haw Yeh and Chia-Yun Cheng, “A Shoulder Surfing Resistant Graphical Authentication System”, IEEE Transactions on Dependable and Secure Computing, 2015.

[10] D. D. Walanjkar, Prof. Vaishali Nandedkar, “User Authentication Using Graphical Password Scheme: A More Secure Approach Using Mobile Interface” International Journal of Innovative Research in Computer and Communication Engineering, Vol. 2, Issue 12, December 2014.

[11] Bin B. Zhu, Jeff Yan, Guanbo Bao, Maowei Yang, and Ning Xu, “Captcha as Graphical Passwords—A New Security Primitive Based on Hard AI Problems “IEEE transactions on information forensics and security, vol. 9, no. 6, june 2014.

[12] Shraddha M. Gurav, Leena S. Gawade , “Graphical Password Authentication”, 2014 International Conference on Electronic Systems, Signal Processing and Computing Technologies.

[13] Amish Shah, Parth Ved, “Shoulder Surfing Resistant Graphical Password system” , International Conference on Advanced Computing Technologies and Applications (ICACTA -2015).

[14] Mrs. Aakansha S. Gokhalea, Prof. Vijaya S. Waghmareb, “The Shoulder Surfing Resistant Graphical Authentication Technique”, 7th International Conference on Communication, Computing and Virtualization 2016.