International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 3 | ISSN : 2456-3307

Enhanced Video Transmission Using Binary Conversion

M. Roja Shree, V. Akilandeswari

K.L.N College of Engineering, Pottapalayam, Madurai, Tamil Nadu, India

ABSTRACT

With the rapid development of data outsourcing services,advanced security measures has to be taken to secure the outsourced Multimedia datas.Securing data is an big challenging task for the server .To maintain security and data confidentiality video data must be encrypted using advanced cryptographic scheme before outsourcing.Here new Method is proposed to maintain data integrity that is binary conversion algorithm.Index is created for every video data and it is encrypted using Blowfish algorithm then the Encrypted data is converted to binary values of 0's and 1's using BCA algorithm.Performance evaluation is made by comparing most advanced AES algorithm and Blowfish algorithm to improve throughput and time efficiency.

Keywords : Blowfish Algorithm, Binary Conversion Algorithm, Data Confidentiality, Data Security

I. INTRODUCTION

With the development of data outsourcing and mobile network user tends to access the data stored in the public server in a secured manner from the remote storage services .Some recruipted public centers allows some external user to upload the data in a storage services,For instances Unencrypted data stored at a public center can be vulnerable to external attacks initiated by unauthorized outsiders and internal attacks initiated by untrustworthy cloud service providers.

Several researchers addressed the issues of ensuring confidentiality and privacy of outsourced data without compromising user functionality.Here confidentiality means securing the stored data from attackers so that clent only can read the exact stored data.To solve the problem of confidentiality data encryption scheme should be handled to provide secrecy of stored data .

The advances cryptographic scheme should be used like to encrypt the video data,Time and throughput should be maintained higher to increasing the efficiency of cryptographic system.To improve the security and dta confidentiality the encrypted data is transformed to binary values of 0's and 1's using ASCII values. Cryptography plays a very vital role in keeping the message safe as the data is in transit. It ensures that the message being sent at one end remains confidential and should be received only by the intended receiver at the other end.Cryptography converts the original message in to non-readable format and sends the message over an insecure channel.The people who are unauthorized to read the message try to break the non-readable message but it is hard to do it so.The authorized person has the capability to convert the non-readable message to readable one. Cryptographic algorithmis classified into two categories: (I) Symmetric Key Cryptography where one key is used for both encryption and decryption. (ii) Asymmetric Key Cryptography where two different keys are used one for encryption and other fordecryption. Symmetric key cryptography is divided into two types on the basis of their operations : (I) StreamCipher: A stream cipher is one that encrypts a digital data stream one bit or one byte at a time. (ii) Block Cipher: Ablock cipher is one in which a block of plaintext is treated as a whole and used to produce a cipher text block of equal length .Blowfish is a symmetric block cipher designed by Brute Schneider in 1993. Blowfish is a replacement ofDES or IDEA . Blowfish algorithm is a symmetric block cipher with a 64-bit block size and variable key lengthfrom 42 bits to 448 bits.A network is a series of individual elements transmitting and receiving various data. Whenever sensitive or confidential information is transmitted,

there is a possibility of an unauthorized third party "eavesdropping" on a transmission andlearning contents of the sensitive message. This possibility is unacceptable in many scenarios. Cryptography is the process of translating a message into a form which is unreadable to everyone except the intenderecipient. This istypically done with use of keys. A cryptographic key is roughly equivalent to the concept of a physical which can unlock the correct lock. In cryptography, keys are used to encrypt the message into a format which would appear as unreadablerandom information to an unauthorized third party.

II. LITERATURE REVIEW

On the basis of analyzing the various transmission of video securely through encryption/decryption, compression techniques and caching mechanism this chapter describes the survey of existing research papers. The literature provides various techniques of video encryption/decryption and compression with reduced ratio-distortion performance and better efficiency with high quality video delivery.

This paper(3) was proposed by John Singh and Manimegalai,a new algorithm is implement by the author called Fast random Bit Encryption Techniques(FRBET).First take the video as input and video is subjected to lossless compression to reduce the size of the video for better encryption. Carefully video should be compressed otherwise there will a seen of degradation in video quality. To encrypt the video ,advanced encryption standard (AES)algorithm is implemented. Here the key is divided into four parts and encrypted using random number. If the bits are not present with 8 bits then it is padded with 0's to increase the key strength. Then both sender and receiver should be given with same random key number to avoid issues. The bit 0's and 1's are padded to get a fixed length hash data; it is given by hash function. Then it is subjected to salt algorithm to create salt for hash function. The AES encrypted data should be converted in to frames before applying salt alg.key based password is created to generate key from salt alg. key is separated into four parts and XOR_{ed} with random number and then PKCS7 is padded with key to generate a secured key function.

This paper (4) Vino1, Logashanmugam proposed a new standard algorithm for H.264 standard to decrease the overhead. It will be secured against cipher-text only and known plain text attack. Error tolerance is initiated with the secret sharing method.DC's coefficients are shared among Ac's and DC's coefficient. It is not helpful is recognizing full object but it can identify the object which is in motion. Leakage of information may do by P and B frames of I block. This leakage can be decreased by encrypting this I block also but to encrypt I block it takes some time to encrypt those data. It is not suitable for enlarge and sensitive video.

This paper(5) WANG Li-feng, NIU Jian Proposed a new lightweight scheme called Luminance Transform Coefficient Encryption exploit the important features of H.264 standard.To provide security and efficiency with limited power, high processing speed with bandwidth capabilities in wireless platorm.The residual data co efficiency are encrypted by stream ciphering. This algorithm mainly encrypts the luminance transform coefficient due to high effect on visibility than chrominance. To eliminate propagation error stream ciphers are concentrated than block cipher. Security is ensured by conventional encryption algorithm.Bitrate is adjusted by selecting the specific parameter.

This paper(6) Zhang Qian, Wu Jin Proposed a new encryption algorithm for better video conferencing purpose. It introduced a new permutation code and DESalgorithm with three schemesFor H.264 standards. This scheme engage the technique of encrypting part of motion vector and chrominance and luminance of residual data of DCT coefficient and intra prediction of motion vector are encrypted.Intra prediction codeword encryption makes more confusion due to I and P frames of inter prediction mode. It incredibly reduces the compression rate.

This paper(7) varalaxmi.l proposed a new encryption for the real time video transmission. Main scheme is that videos are converted into DCT coefficient and encrypted using secret sharing. Secret sharing is used to determine that there is no formation of groups which discover secrets. Motion vectors are transformed or jumbled using pseudo random generator. Next proposal is used to do discrete wavelet transform on the coefficients using secret sharing mehtod.Intraprediction encryption is done using a method called PRNG with secret sharing of DWT, then it is followed rest of previous process. In last scheme the algorithm called ACCordin is used do spatial correlation of frames and

it is used to transform group of pictures in to single group using interframe redundancied.It fight against cipher-text only and known pain-text attacks.

III. PROPOSED WORK

A SYSTEM ARCHITECTURE

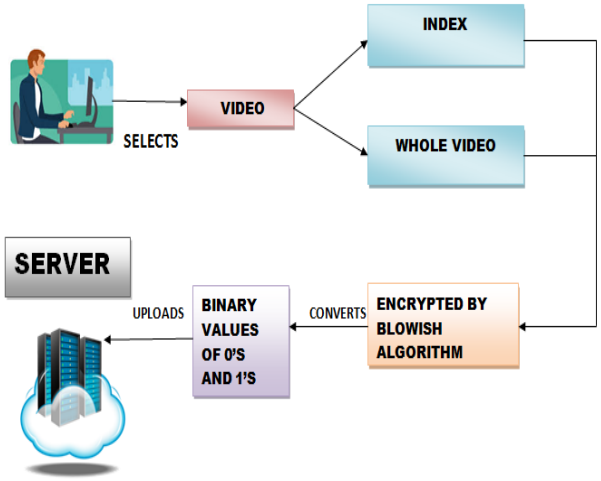


Figure 1. System Architecture

Data owner: The data owner is basically referred as a video provider who stores the data in a server .The video provider encrypts the video data before uploading the video to the server. The index and meta data of the video must be encrypted using cryptographic algorithms that enables the secure searching capabilities.

Data user: Data user are called as subscribers who gets the data by sending encrypted query to the server for subscribing the video data at user end securely.

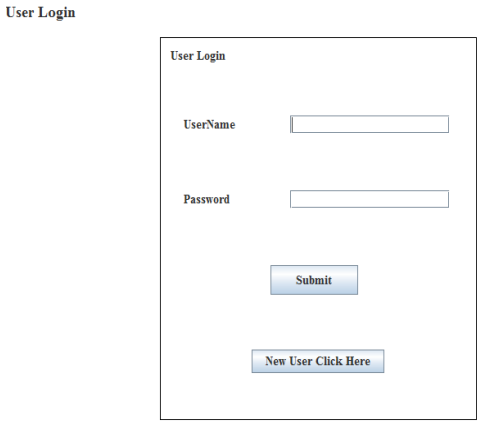
Server: They are the premise server which stores the massive amount of Multimedia data for the user to subscribe at any time without having any risk.

B MODULES

- **User Authentication**
- **Video Indexing**
- **Video encryption and binary conversion**
- **Video storing**

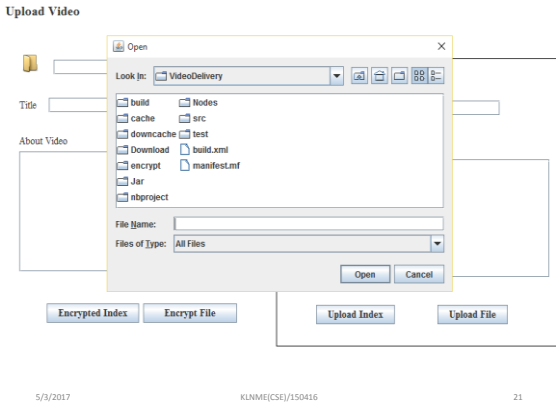
C. USER AUTHENTICATION

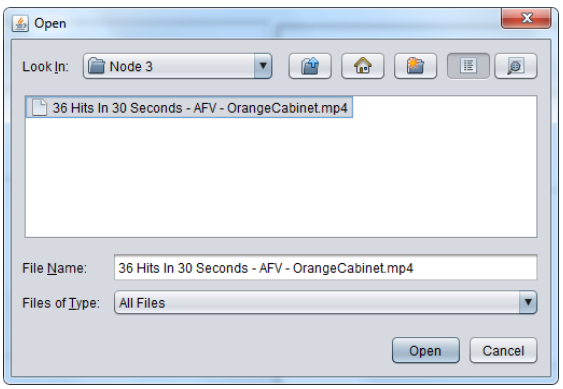
- Only authorized user can upload the video to the public centre.
- Video providers are Provided with unique user Id and Password to login .
- New user can register their id and get new user Id and password to login.

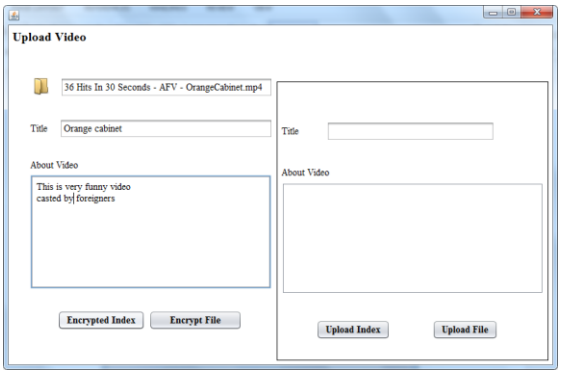


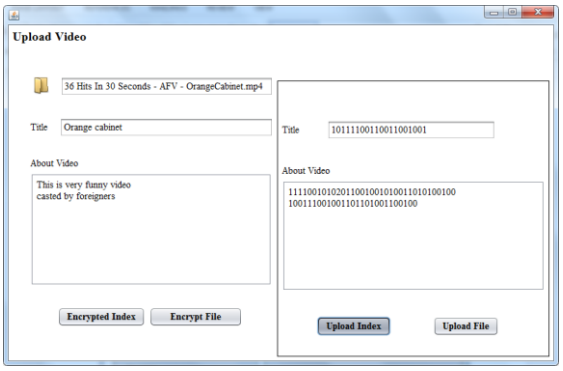
D. VIDEO INDEXING

- Providers can select the video which they want to store in server.
- After selecting the video ,Providers has to give title and describe something about the video.



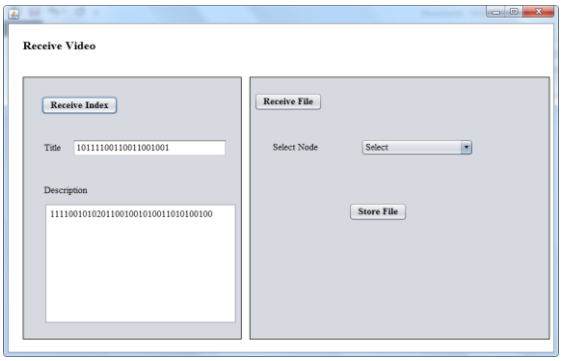


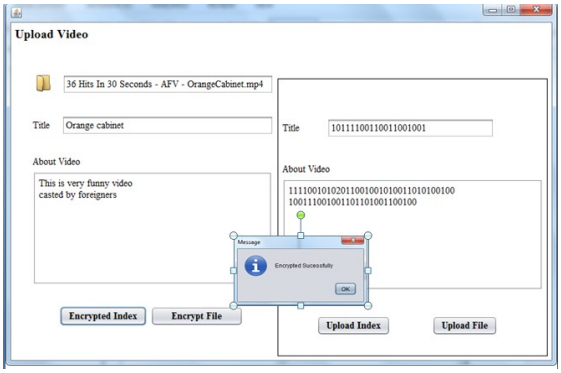


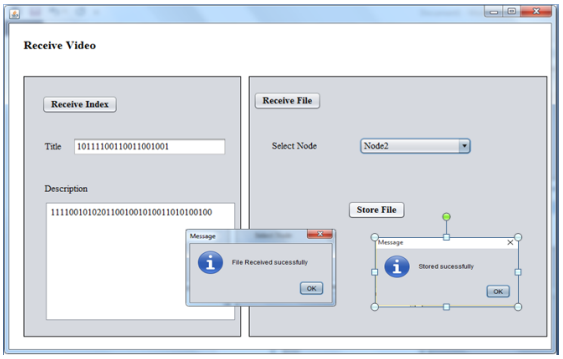


E. VIDEO ENCRYPTION AND BINARY CONVERSION:

- Title and description about the video is encrypted using AES encryption algorithm.
- Then whole video content is divided into frames and encrypted individually.
- After encryption, Encrypted data and index is converted in to binary form of 0's and 1's.







F. VIDEO UPLOADING

- Encrypted index and whole video content is uploaded into the server by video provider.
- Server receives the index and entire encrypted video content from the provider and stores in the separate database in encrypted binary form.
- Videos are retrieved by matching index and whole video content using location sensitive hashing technique.

G. COMPARISON TABLE

TABLE I

ELEMENTS	AES	BLOWFISH
KEYSIZE	128,256	32-448BITS
BLOCKSIZE	128	64BITS
STRUCTURE	SUBSTITUTION/ PERMUTATION	FIESTAL OR BLOCK CIPHER
FLEXIBLE	YES	YES
SECURITY	GOOD SECURITY	EXCELLENT SECURITY OVER MULTIMEDIA DATA
THROUGHPUT	LOW	HIGH
TIME	HIGH	LOW

IV. RESULT ANALYSIS

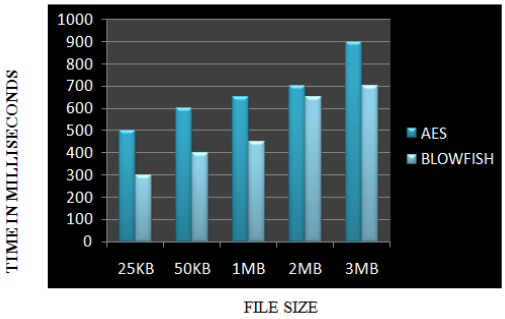


Figure 2. Comparing AES and Blowfish in file size

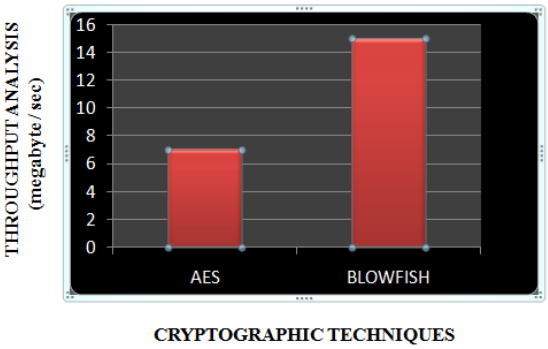


Figure 3. Throughput Analysis

V. CONCLUSION

The Proposed methodology of securing data in public centre is better than any other security measures mentioned in literature survey. To ensure better security an everlasting secured Blowfish Algorithm to increase throughput and time efficiency in encrypting and decrypting the file and to enhance security the encrypted data are converted stored in binary format at public centre. It ensures that our proposal maintain data confidentiality over data transmission and it assures that storing data in binary format helps in retrieving similar data at minimum time.

VI. REFERENCES

[1]. Xingliang, Xinyu Wang, jinfan Wang, "Enabling Secure and Efficient Video delivery through Encrypted In-network Caching", in IEEE journal on selected areas in communication, 2016.

[2]. Qian Wang,Meiqi He,Minxin Du, "Searchable Encryption over Feature-Rich Data", in IEEE Transaction on Dependable and Secure Computing, VOL. 13,NO. 9,Sep 2014.

[3]. PoojaYadav,NishcholMishra,SanjeevSharma,"A secure video steganography with encryption based on LSB technique", IEEE International Conference on Computational Intelligence and Computing Research,2013

[4]. Bonny Raj,Frank, " A Secure data transfer through DNA Cryptography using Symmetric Algorithm",IEEE 2012 7th International Conference on Electrical and Computer Engineering ,NO 20-22 December, 2012

[5]. Shunjun Li, Guanrong Chen, Albert Cheung, Bharat Bhargava, and Kwok-Tung Lo, "On the Design of Perceptual MPEG Video Encryption Algorithm", IEEE Transactions on Circuits and Systems for Video Technology, vol. 17, No. 2, 2007, pp. 214-223

[6]. Zhang Qian, Wu Jin-mu, Zhao Hai-xia, "Efficiency Video Encryption Scheme Based on H.264 Coding Standard and Permutation Code Algorithm", IEEE World Congress on Computer Science and Information Engineering, 2009, pp. 674-678

[7]. WANG Li-feng, NIU Jian-wei, MA Jian, WANG Wendong, XIAO Chen, "A Lightweight Video Encryption Algorithm for Wireless Application", Fifth IEEE International Symposium on Embedded Computing, 2008

[8]. K. John Singh, R. Manimegalai, "Fast Random Bit Encryption Technique for Video Data", European Journal of Scientific Research, Vol.64, No.3, 2011, pp. 437-445

[9]. R. R. Igorevich, H. Yong, D.Min, E. Choi "A study on multimedia security systems in video encryption," in proceeding of IEEE 6th International Conference on Network Computing. 2010, pp. 1-5

[10]. Shiva Krishna Reddy, k. Srimathi, R. Rajalakshmi," The Indexing Algorithm for scrambled frames in video encryption", International Journal of Advanced Research in Computer Science and Software Engineering ,vol. 4, pp. 651-655, February – 2014.