End to End Guaranteed Secure and Efficent Video Delivery Through Encrypted in- Network Caching

M. Roja Shree
PG Scholar
Dept of Computer science
K.L.N College of Engineering
Pottapalayam,India

V. Akilandeshwari
AP(Sr.Gr)
Dept of Computer science
K.L.N College of Engineering
Pottapalayam, India

***Abstract*— In today's world most of the communication will be video based .To scale the immense delivery of video, various novel network design like In-network caching of Information centric networking(ICN) is used. In-network caching have been grown as an hopeful method to grip the exponential growth of video traffic. Alternatively due to the increase of vast attacking surfaces, caching of video content should be done. Accessible protocols like HTTPS also fall short of fully leveraging in network caching and there also chances of taking place man in the middle attack. To facilitate competent video delivery a new network system architecture is developed. To Provide guaranteed security videos are alienated into chunks, and these chunks must be encrypted. Then these chunks are recognized by the finger print index. To assist fast and secure video delivery a secure redundancy elimination protocol is introduced. Cache enabled router is worn to achieve the benefits of caching mechanism and to eliminate redundancy**

***Keywords*--Video network traffic, Redundancy elimination, Assymetric Searchable Encryption, Pseudo random function**

I. INTRODUCTION

Videos have been increasingly dominating today's Internet traffic and Cisco projected that 75% of all network traffic in 2018 will be video based. To balance the massive delivery of videos, a new network architectures with optimizations for content-intensive applications have been proposed,Such as network caching of ICN and it has been a natural trend to leverage some of the benefits like storing the content in advanced network devices like cache-enabled routers, efficient and scalable content distribution, and redundant network traffic elimination.Network content caching plays a vital role in raising security and privacy concern among the un trusted network environment .

For users, it is crucial to ensure their private data, like video access history, subscription details, or even personal videos, not to be exposed unwillingly and For content providers, strong protection against unauthorized content access or copyright infringement is a commercial imperative so we propose and implement a new networked system that aims for secure and efficient encrypted video delivery while preserving the benefits of encrypted in network caching. The proposed designs are presented via a systematic integration of emerging network architectures for content intensive applications, cryptographic building blocks, novel encrypted data structures, and secure and practical network protocols.

Section i shows the basic introduction about video delivery section ii shows the survey work section iii delivers our proposed work and system initialization section iv tells about security techniques used in proposed work section v tells

about the experimental setup section vi discuss about the result section vii conclusion part.

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.

Michalos (2012) discussed about the performance of DASH, DASH is regarding delivering video to the internet user in an adaptive mode. This means that the stream is being deliver to the client by recognizing and adjust to network's capacities every time a new request takes place. As soon as the request is taking place DASH chops the video files in to segments and download it in a active way but streaming does continuously without any disruption in playback mode it doesn't care about which part of the stream is being watched while the rest is being downloaded. DASH effortlessly changes the stream to low quality video which is also stored in the server whenever there is insufficient and undesirable breaks interrupt in network. DASH runs using HTTP protocol and contains the evident file in xml like MPD file. Media Presentation description is a manifest file responsible for shipping information about video piece and to convey it in a secure manner. To promote the service of dash, the user should download the dash in the recruit operating system.

Ujwala (2010) proposed perceptual encryption this design is a universal version of VEA for perceptual encryption, by selectively encrypting FLC information elements in the video stream. In fact, encrypting FLC data elements is the most natural and possibly the simplest way to maintain all needed features, especially the need for firm size maintenance. To sustain format compliance , only last four FLC data elements are considered, that are divided into three categories i) intra DC coefficient
ii) sign bits of non intra DC coefficients and AC coefficients iii) sign bits and residuals of motion vectors. Based on this separation, three control factors Psr, Psd and Pmv in the range [0, 1] are used to manage the visual quality in three special scope like low degree spatial view, high resolution spatial details and temporal motions. Recognized and chosen plaintext attack are ensured with four special measures by implementing block cipher, using a cipher with plaintext/ciphertext feedback, with a key executive system and a stream cipher and using a stream cipher with unique ID.

Deshmukh (2014) proposed a new encryption scheme a Modifies AES algorithm for MPEG video encryption. To conquer the problem of high computation and totaling overhead, analysis of Advanced Encryption Standard (AES) is made and modifies it, to recover the encryption performance and speed .The alteration is mainly focused on Shift Row Transformations. In the Shift Row Transformation, the value in the first row and the first column is constant, then the first and fourth row is unaffected, and each and every byte in the second and third row of the state is on a regular basis shifted right over different number, else the first and third row is unaffected, then each and every byte of the second and fourth row of the state is regularly shifted left over different number of bytes. This modification allows for greater security and increased performance.

Nazar Al-Hayani(2013) proposed a new concept of simultaneous video compression and encryption for securing a video during real time transmission. Here encryption and compression are performed simultaneously to inherit the efficient video transmission. To retain the original size and exact quality of the video the compression is based on Discrete wavelet transform, Discrete cosine transform and vector quantization .The compression algorithm follows two steps reference frame encoding and current frame encoding based on reference frame. Encryption algorithm utilizes two Linear feedback shift register seeded with three secret key is generated to scramble the significant wavelet coefficients multiple times. These algorithms are applied simultaneously in the wavelet domain. Videos are divided into frames and these frames are applied to the 3rd level of wavelet transform. Here each frame is divided into 16x16 blocks of high frequency sub bands and DCT is applied for each blocks. Each block is considered as vector based on vector quantization method and these vectors are used to construct code books. After applying quantization method, the code books are compress and send through the transmitter. After performing these functions reference frames are founded. To enhance the video quality RF will be send to every 25 frames at each frame.

Gul Boztok Algin(2011) proposed a syntax compliant encryption algorithm is proposed for H.264/AVC. Encryption is inserting within the encoder. Using the projected method allows to add the encryption mechanism inside the video encoder, as long as a secure transmission which does not alter the transmission process. Then the bits “selected for encryption” are chosen with esteem to the considered video standard according to the following rule: each of their encrypted configurations generate a non-desynchronized and fully standard compliant bit stream. This can in particular be completed by encrypting only parts of the bit stream which have no or a negligible impact in growth of the decoding process, and whose impact is consequently purely a visual one.

Fuwen Liu (2012) proposed a new compression-independent video encryption algorithm called puzzle. Here compression and encryption are carried out separately. It consists of two ways to reduce the computational overhead for video encryption. one ways is to apply selective encryption principle i.e the only a portion of the compressed video streams is encrypted with conventional algorithm ,The other ways is that entire video stream is encrypted with a lightweight algorithm. Puzzling consists of three steps i)partitioning-dividing the blocks into sub blocks, a compressed video frames is puzzled by partitioning the frames into n blocks and it is arranged by reordering all the bocks ii)obscuring means all the blocks are subjected to encryption with the help of light weight algorithm with pseudo random generator.

Pradeep pai(2014) proposes a new a time selectively video encryption methodology for enduring the concept of row-column permutation and shuffles the video data to ensure faster delivery of data and better encryption of video data. Here Meta data are sent to a retrieved data and in retrieved data field a set of audio and video files are distinguished. Then these data are encrypted by RC permutation then it is followed by AES/DES method.

Florence(2011) proposes an efficient selective encryption scheme to enhance the security in H.264/scalable video coding. Encryption procedure is implemented in Network abstraction layer. Encryption scheme are proposed at three domains at Intra prediction mode, motion vector and at residual data. To improve security and guaranteed transmission both base layer and enhancement layer of the video are encrypted. In Base layer IPM are encrypted using fixed length encryption scheme, IPM and MV are encrypted using Exponential-Golomb encryption then residual data are encrypted using texture encryption. In Enhancement layer encryption are done at three levels to ensure better temporal scalability, spatial scalability, SNR scalability.

Shiva Reddy (2014) proposes a new threshold encryption, by using this enc. Videos are separated in to frames and each frame of a video is encrypted. Then the encrypted frames are set with an index number. The index number is also veiled. The encrypted frames are twisted and send through the network in a arbitrary manner. Completely all the in order is hidden. The threshold method is used for encrypting the frames. The threshold method converts the data into a binary data. The threshold value is recognized. The repeating pixel value is taken as a threshold value. The pixels superior than or equal to the threshold is taken as 1, and the values lesser than the threshold value is taken as 0.The receiver is providing with the decrypting algorithm. The original frames are obtain and rearranged with the help of key numbers

Abomhara (2010) discussed about some of the video encryption techniques that are fully layered encryption, selective encryption, Perceptual encryption, Permutation encryption. In Fully layered encryption: whole content of video is first compacted and then encrypted using typical ritual algorithms like DES, RSA, IDEA, AES etc. This technique is not suitable in real time video applications due to heavy computation and slow speed.

III. PROPOSED WORK

System Initialization

It consists of four parties: video application servers, request handlers, cache-enabled routers, and users.

A. Users

They are the promising user with authorized Private key to get the original video data.video consumer may act as paid user or free consumer .on the account of paid status user will give some amount to video providers for authorized access.

B. Video application servers

This is brilliant server which is used for providing service as video aggregator like you tube and video streamer like Netflix .It can be applicable only for authenticate user.

C. Request handlers

They can be devoted servers with computing and storage ability, which identify, locate, and manage the chunks in-network cache. In our system, those dispersed request handlers are assumed to be wholly- honest. They are used to transfer and store the video content and encrypted index to have secure communication. In practice, a request correspondent may be requisite to dispense the arriving requests to different request handlers. For ease, we consider the dispatcher as a single logic unit, and focus on how one request handler handles the request.

D. Cache-enabled routers

New network devices is implemented to store, match and forward the content in network environment. In Proposed design cache enabled router play a major role to store the encrypted video frame temporarily and each chunks are presented with the unique Pseudonyms. It has the main role in routing the video content to the authorized user

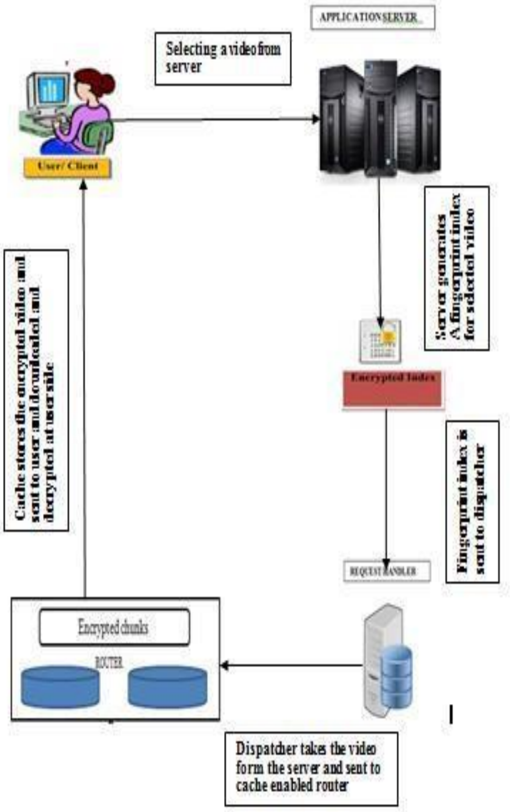

APPLICATION SERVER
Selecting a video from server
User/ Client
Server generates A fingerprint index for selected video
Encrypted Index
Fingerprint index is sent to dispatcher
REQUEST HANDLER
Cache stores the encrypted video and sent to user and downloaded and decrypted at user side
Encrypted chunks
ROUTER
Dispatcher takes the video form the server and sent to cache enabled router

Fig.1 System Architecture

IV. SECURITY TECHNIQUES

A. MD5 hashing algorithm

MD5 algorithm was built by Professor Ronald L. Rivest in 1991. According to RFC 1321, “MD5 message-digest algorithm takes as input a message of random length and gives a output of 128-bit "fingerprint" or "message digest" of the input .The MD5 algorithm is projected for digital signature applications, where a large file must be "compressed" in a secure manner before being encrypted with a private (secret) key under a public- key cryptosystem such as RSA.

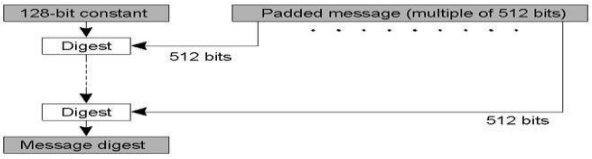


Fig.2 MD5 Structure

”It consists of four implementation: steps i) Appending Padding bits ii) Append length Iii) Initialize MD Buffer iv)Process messages in 16-words blocks.

Algorithm (for generating finger print index)

Step 1: MD5 process over a length of message up to 128 bits (name of the video)

Step2: The i/p message is broken in to chunks of 521 bits (16 32-bit words)

Step3: Message is padded and then length is divisible by 512 bits

Step4: Padding work as follows

Step4.1: First single bit,1 is appended to end of message

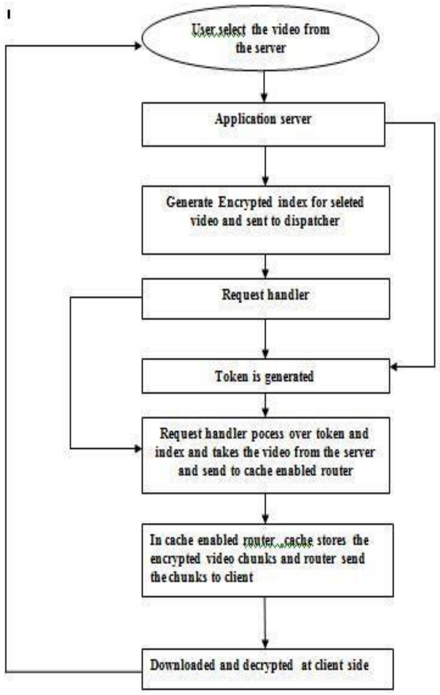
Step4.2: Then it is followed by zeros as required to bring up to 64 bits fewer than multiple of 512 bits

Step5: The remaining bits are filled up with 64 bits.

B. Secure Redundancy Elimination (RE) Protocol

The secure RE protocol is conducted in the following steps: 1) The video application server generates a secure token from the fingerprint of user’s requested video; 2) The request handler processes the token over the encrypted index, and obtain the chunk pyns for the requested video only;

3) From pyns, the request handler looks up the addressing table D, and returns a manifest L with hpyn,addri pairs; 4) For chunks in the network, the request handler will send pyns and the user’s addresstotargetedrouter.5)If(pyn,Null)is found in L, the application servers will be notified to send the chunk pyn directly to the user, and place it in some router along the path. Then the router will update hpyn, addr to the request handler.


User select the video from the server
Application server
Generate Encrypted index for seleted video and sent to dispatcher
Request handler
Token is generated
Request handler pocess over token and index and takes the video from the server and send to cache enabled router
In cache enabled router, cache stores the encrypted video chunks and router send the chunks to client
Downloaded and decrypted at client side

C. Searchable Encryption (SE)

During Encryption the search token is generated from keyword search. Search token represents the encrypted query. Encrypted data is generated with the help of query with the help of key.SSE is normally based on two components i.e keyword based and non keyword based. Keyword based is used to search the document using index concept.Non keyword based concept is used to Search word by word scanning process.The cryptographic algorithm is implemented by symmetric key or Asymmetric key

D. Asymmetric searchable encryption algorithm (AES):

The encryption are totally depends on asymmetric key or public key. Functionality is the key advantage of AES and inadequacy is the chief problem of AES. Searchable Symmetric Encryption Searchable Symmetric Encryption (SSE) provide high security that enables the data to be stored in negotiator for privacy preservation .The symmetric encryption is the cryptographic algorithm based on symmetric key or private key. It deploy a same key for encryption and decryption. The solutions of SSE are swap among efficiency, security and confidently data is updated and encrypted before uploading .The Principle goal of SSE is practical concern. The SSE is compared to the homomorphic encryption / multiparty computation to provide high security without any drawback.

Effectiveness is the key advantage of SSE and all SSE schemes are totally depends on PRF and block ciphers. This ability is the main drawback of SSE.

E. Cuckoo hashing:

The cuckoo hash table contains the array of buckets with hash function. Cuckoo hashing is an open addressing format. The hash table hold the Key value pair or key. Cuckoo hashing is used to resolve the hash table collision. To avoid collision it uses two hash table. Each key is tracked by hash function. Every key provides the exact location of hash table. The hash table is separated in to two and filled with hash function on either side. Index is provided to identify the hash table. Insertion, Deletion and search operation is implemented by cuckoo technique : The items are searched in either side of table at the same time and each bucket is checked whether it contains the item or not using look up protocol. The items are inserted into hash table with the help of greedy algorithm . cuckoo hashing is helpful in balancing the load factor. Failure can be handled by restructuring the data structure with less time. Membership details are presented in hash table. It will provide optimized performance with the usage of partial key software based Ethernet switches and it achieves improved performance by cuckoo hash table.

Advantage of cuckoo hash function

- Table allocation is not recommended for rehashing.
- It follows the general procedure for deletion.

F.Cuckoo Filter

A cuckoo filter is a compressed deviation of a cuckoo hash table. The cuckoo filter store a bit string for each item insert into table instead of key value.

Advantage of cuckoo filter

- Dynamic insertion and deletion are intervened.
- It provides better performance than bloom filter.
- Simple Implementation is required.

G. Pseudo random function (PRF)

Pseudo Random Function (PRF) is a cluster of computable functions. Pseudorandom functions plays a major role in forming primitive structure of cryptographic and encryption technique. PRF is a random function that choose the function from same value set or same sector. The pseudorandom generator (PRG) builds the pseudo random function. PRF is defined by deterministic function of (Key, Message and Output) and return the random sequence output .i.e. F: Key x N > Out. All the outputs are appeared randomly in PRF. PRF is a deterministic function that maps the domain distinct set and range distinct set and produces the real random function.

Encryption mode

□ ECB - Electronic codebook.

□ CBC - cipher block chaining.

□ OFB - Output Feedback Mode.

Merits

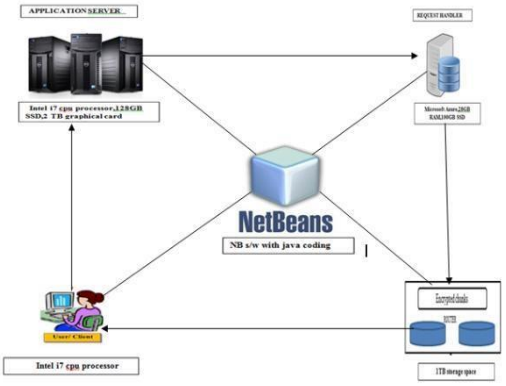
□ General setup is implemented.
□ security is ensured with the help of using random function.
□ Mapping is done.

Limitation

□ Same key is used for both input and output.

V. EXPERIMENTAL SETUP

We implement a system prototype for the performance evaluation. The video application server and request handler are deployed at Microsoft windows 10 Hp notebook which servers 8GB RAM 2 GB graphical cards 1TB and 100GB SSD. We use three servers at local side to stimulate cache enabled router. Each server has an Intel i7-CPU, 16GB RAM, 2GB graphical card. Then net beans tool is installed and programmed with java coding. I used intel-i7 processor as both server and client. The cryptographic building blocks in the request handler and the user client are implemented by open SSL and .NET framework.



VI. RESULT AND DISCUSSION

Fig.3 states that delivery time increases with the size of the video .it is estimated between video size and delivery time. Delivery time is evaluated with encrypted in-network caching and bandwidth is set as 10 mbps for application server and 1000mbps is set for cache to store. The overall delivery time is estimated.

Fig.4 shows that security overhead increases with different bandwidth and delivery time. If the bandwidth of the cache increases then cache can store more mb videos so delivery time increases with the video size.

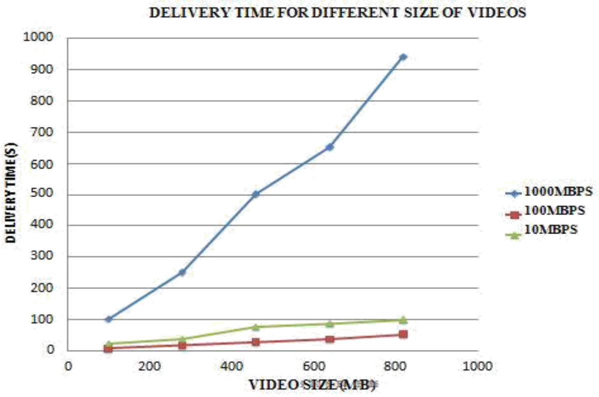


Fig.3 Delivery time for diverse volumes of video

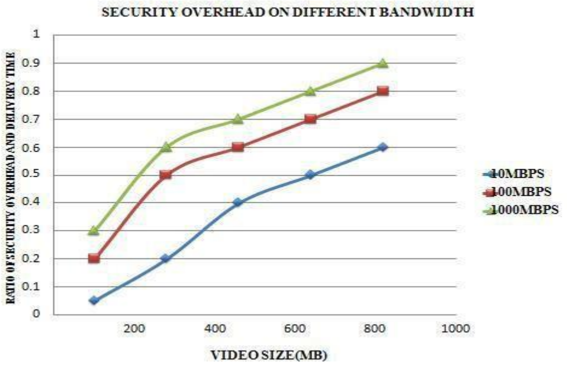


Fig.4 Security transparency on different caching ratios

VII. CONCLUSION

An emerging new system architecture is designed to enable secure video delivery with encrypted chunks through network caching. High performance and security is achieved to some extent by using encrypted fingerprint index in developed architecture and Redundancy of video data is reduced by implementing secured RE Protocol. The system prototype and evaluation is made to verify the secured architecture.

The Experimental result revealed that the secured index is processed over the network caching with minimum latency of intermediate server and the delivery time is massively reduced with enormous video content.

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] Ahlgren B, Dannewitz C, Imbrenda C, Kutscher D, and ohlman B(2012), “A survey of information-centric networking,”
IEEE Communications Magazine,vol. 50, PP. 26-36

[3] Arianfar S, Nikander P, and Ott J(2010), “On content-centric router design and implications,” in Proc. of the ACM Re-Architecting the Internet Workshop.

[4] Boztok Algin E, Turhan Tunali(2011), “Scalable video encryption of H.264 SVC Codec” ELSEVIER journal of visual communication and image representation, vol 22,PP 353-364.

[5] Misra M, Tourani R, and Majd N E(2013), “Secure content delivery in information- centric netwoks: design, implementation, and analysis,”,in Proc. of the 3rd ACM SIGCOMM workshop on information centric networking.

[6] Manfredi S, Oliviero F, and Romano S P(2013), “A distributed control law for load balancing in content delivery networks,” IEEE/ACM TON, vol. 21, no. 1, PP. 55-68.

[7] Nazar Al-Hayami, Naseer Al-Jawad, Sabah Jassim (2013), “Simultaneous video compression and encryption for real-time secure transmission”,IEEE Internation symposium on Image and signal Processing.

[8] Pradeep Pai T, Raghu M E, Ravishankar K C(2014),” Video Encryption for Secure Multimedia Transmission - A Layered Approach, IEEE 3rd International Conference on Eco-friendly Computing and Communication Systems (ICECCS),vol. 6,PP. 18- 21.

[9] Pooja Deshmukh, Vaishali Kolhe (2014), “Modified AES based algorithm for MPEG video encryption”, IEEE international conference on information communication and Embedded system(ICICES).

[10] Psaras I, Chai W K, and Pavlou G(2012), “Probabilistic in-network caching for information-centric networks,” in Proc. of the second edition of the ACM ICN workshop on Information- centric networking.

[11] Perino D, Varvello M, and Puttaswamy K P(2012), “ICN-RE: redundancy elimination for information-centric networking,” in
Proc. of the second edition of the ICN workshop on Information- centricnetworking.

[12] Shiva Krishna Reddy A, Srimathi K, Rajalakshmi R(2014), “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. [13]So W, Narayanan A, and Oran D (2013), “Named data networking on a router: fast and dos-resistant forwarding with hash tables,” in Proc. Of ACM/IEEE ANCS.

[13] Zhang X(2011) “Lossy compression and iterative reconstruction for encrypted image,” IEEE Transactions on Information Forensics Security, Volume 6, No 1, pp. 53–58. [15]Zheng Y,Yuan X, Wang X, jinag J, Wang C, and Gui X(2015), “Enabling encrypted cloud media center with secure deduplication,” in Proc. of AISACCS.