IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 10, October 2016

A Survey on Secure Video Delivery through Encrypted in- Network Caching

S. Jeyalakshmi[1], P. Murugeswari[2]

PG Scholar, CSE, Srividya College of Engineering and Technology, Virudhunagar, India[1]

Professor, CSE, Srividya College of Engineering and Technology, Virudhunagar, India[2]

Abstract: With the dramatic increase the video application, security is becoming a major problem of the network. Intruders on the network are increasing day by day. The attackers are easily access the video content. This problem is recovered by In-network content caching. In-network content caching is new emerging network architecture that effectively handles video traffic in network. At present many technologies (like HTTPs) to effectively handle the video traffic but the main drawback is end to end security. In-network caching provides the encryption method for secure video delivery. This paper presents a survey on different method for secure and efficient video delivery through in network caching.

Index terms: Video traffic, attackers, in-network content caching, encryption, Http.

I. INTRODUCTION

In network caching[13] is the latest research area in content centric network or context of information. In-network caching is differentiate from co –operative caching approach, web caching. In-network caching is the caching techniques to uncoordinated and decentralized environment. The main aim of in-network caching is reduce redundancy of cache and utilize the cache resource along the delivery path of content.

In-network cache management manages the cache capacity and estimate the amount of cache traffic per unit time, to make decision on whether the cache content is incoming or not.

Design of In-network caching

In-network caching is a key function of ICN architectures [13]. The contentplacement and contentreplacement is the significant two dimension of In-network caching.

Contentplacement

A contentplacement approach[5] decides the object cache across routers along the path request. The specific strategies of content placement: (1) Leaving a copy in all places. (2) The immediate downstream router leaves the copy when there is upstream router hit. (3) Leave the random chosen router along the path request. (4) Stable probability of each router caching. (5) The router has the largest value use centrality based measure. (6) Use hybrid method for router cache object function.

Contentreplacement

The contentreplacement[5] approach provides the object rejection function while the cache is full. The five function of content replacement is: 1) LRU (recently used) 2) FIFO (first-in first-out)3) LFU (least frequently used) 4)TTL (time to live) 5)Size of the item.

The content placement and content replacement strategies are different from content staging. It determines the cache steady state behavior.

II . NEW NETWORK ARCHITECTURE

Information Centric Network

Information centric networking[10] is the current research topic of future internet. The objective of future internet is enforcement of security and mobility management. ICN caching is the best approach for video workloads that improve the quality of video –centric.

ICN analyze [11][12]the relationship between information and video. ICN depends on connectivity and end to end architecture to network. HTTP is a protocol of choice that provides the cache content delivery.

The operation of ICN is storage, caching, multicast and information delivery to the users. ICN[15] request the content to network that depends on two activities: i) request is directly respond when the data is cached. ii) The data is not cached, the content is request to peers then the content is cache. This caching is called universal.

ICN use any type of protocol for caching and deliver the content is called single uniform caching. The contents are applied to all users. The universal caching is implemented by all nodes and construct the node is persistent. The security ICN is content-oriented model.

In content oriented model the ICN does not receive the content from server. It receives the content from content provider and verifies the content by signature. The communication of ICN is hop by hop between the elements of content router, resolution handler.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 10, October 2016

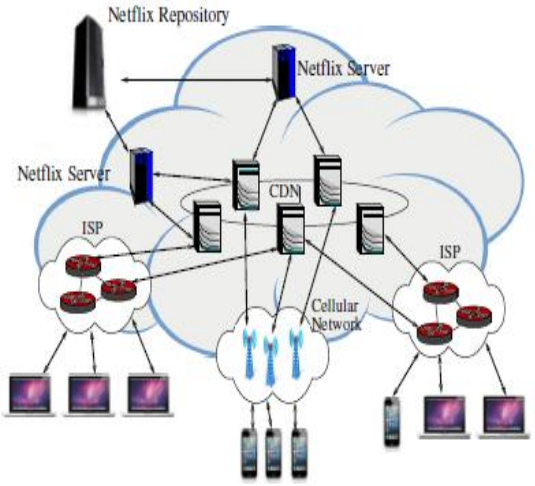

Figure 1. Information centric network architecture.

Content Delivery Network

Content delivery network[7][17] is a distributed network of system that provide the proficiently deliver the web content to users. The main aim of CDN is reduce the internet inherent and latency of web site access. The CDN security method protects the DDoS and WAF (Web Application Firewall) attacks. CDN is composed by number of surrogate servers that distribute to world. The web site content is replicated by push or pull method.Request routing is the key element of CDN. The technique of Request routing is i) URL rewriting: It modifies the URL content in the website. The advantage of URL rewriting is Fine grained redirection control modifies the web site content. The drawback of URL rewriting is : not protect the DDoS or WAF attacks. Domain level redirection is required. This drawback is overcome by Domain hosting and CNAME. ii) Domain hosting: It is authorized name server for web domain. The web domain name is restricted by CDN provider. iii) CNAME: It is type of DNS record that relates the domain name. The domain name and CDN domain name are related by CNAME record.

III. ALGORITHM FOR IN-NETWORK CACHING

ProbCache

The probabilistic algorithm is ProbCache. ProbCache distribute [13] the cache content along the cache path. ProbCache ultimate goal is reduce the cache redundancy and manage cache resource. ProbCache has less Received Request and more Cache Hits. The efficient resource management of ProbCache by Cache hits and Received Request, the result is staying the content in cache for longer. ProbCache is the multiply of Cache Weight and Times In. ProbCache probability depends on TSB value and TSI value.

Redundancy Elimination (RE)

In the network traffic, the similar byte streams are detected and eliminated by Redundancy Elimination (RE). RE [12] [20] is achieved when the conditions are satisfied: Cache the recent packets and 2) synchronize the cache. RE is a primitive service of IP-layer on network router. 10 % to 60 % of redundant data is eliminated by trace driven analysis method.

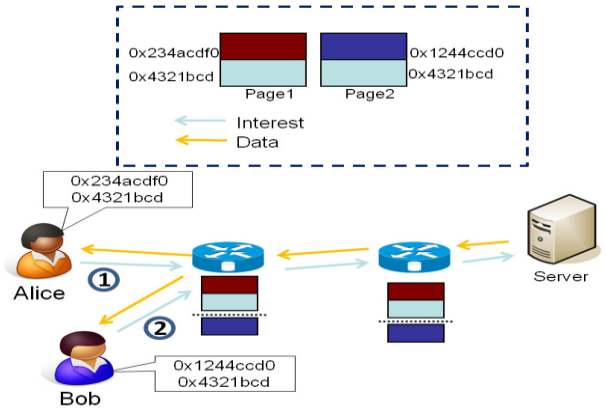

Figure.2 Example of RE

IV. TECHNIQUE OF ENCRYPTION

Broadcast encryption

Broadcast encryption [33] is the problem of cryptographic. The content is transformed into encrypted format and delivers to broadcast channel. Only the authorized user can access the concept. i.e. The broad channel secretly transmit a packet to all privileged subset members. The working principle of Broadcast encryption based on key management block. At the beginning the key management block is sent to the all user. The receiver receives the key management block and reads the key to continue the process based on the key management block.The algorithm of broadcast encryption is a triple of scheme (setup, Broadcast, Decrypt).Setup constructs the private information of receiver. Broadcast list the authorized user and send the key block and broadcast message. The user decrypts the content with Decryption algorithm.

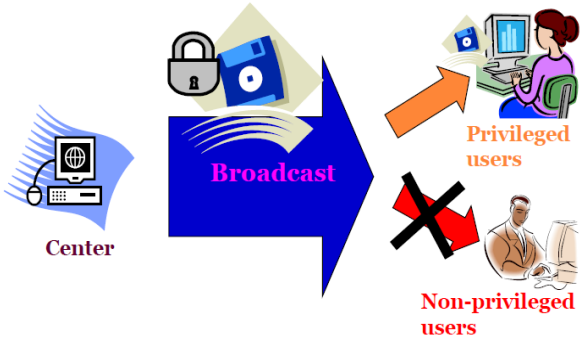

Figure 3. Broadcast encryption

Broadcast Encryption Techniques

1) Traitor tracing[31][32] – minimize the unauthorized user key assessment by random decryption keys assigning to the user.
2) Multicast Encryption.
3) Secret sharing - Its revocation of one-time scheme.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 10, October 2016

4) Tree-based - It's a subset difference construction scheme of encryption.

Attribute – based Encryption

Attribute-Based Encryption (ABE)[21][30] is a category of public-key encryption. The user secret key and cipher text are attributes dependent. ABE is the general technique of functional encryption and collusion –resistance. Attribute based encryption uses a log encryption for reduce the number of key usage.

The log encryption encrypts the log attribute instead of encrypting the key of receiver. The decryption is achieved by user key attribute math with cipher text attribute.

Attribute – based Encryption scheme

1) Key – policy scheme (KP-ABE)
2) Cipher text policy scheme (CP-ABE).

KP-ABE

The user's keys are constructed by tree access that defines the user privilege scope .The encryption is based on attribute set.

CP-ABE:

The encryption is based on tree access and the user's keys are constructed by attribute set. The set of attribute is defined by user's private key and specifies the access policy of the attribute. The decryption is done by user when the attribute satisfy the policy. The policies are conjunctions, disjunctions or threshold.

Drawback of ABE

1) Non –efficiency of attribute revocation.
2) Non – existence of attribute revocation.
3) Co- ordination of key.

AES

Symmetric encryption algorithm is called as Advanced Encryption standard. The operation of AES[23] is iterative that depends on substitution permutation network. It contains the number of linked operation.

In Substitution the input is replaced by corresponding outputs. In Permutation bit shuffling is involved. AES computation is based on bits instead of bytes. Plain text use 128 bits as 16 bytes. The bytes are set in four rows and columns for matrix process.

Advantage of AES

1) Symmetric block, Symmetric key cipher.
2) Key size is 128/192/256 bit, Data size is 128 bit.
3) AES is Quicker than Triple-DES.
4) Provide the full requirement e and detailed design.
5) Implementation is C and java.

Drawback of AES

- The proper implementation and best key management is guaranteeing the AES security.

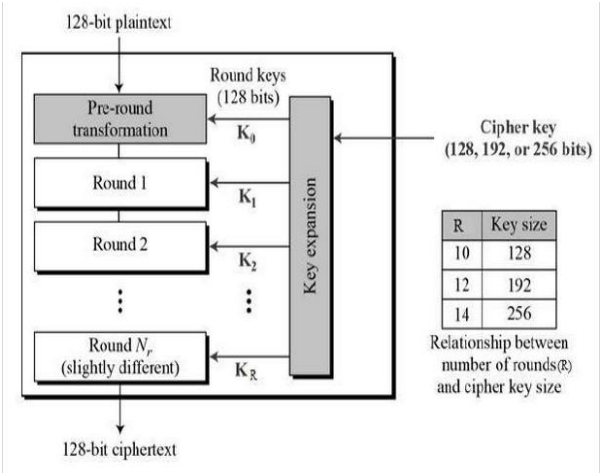

Figure.4 overview of AES.

Searchable Encryption

Searchable encryption produces the search token from keyword search. Encrypted query is represented by search token. The query generates the encrypted data with help of key. Searchable encryption design based on keyword based or non keyword based. Keyword based model use index concept that provide the easiest document search. Non-Keyword based model use word by word scanning process. In the cryptographic algorithm the SE is implemented by Symmetric key or Asymmetric key.

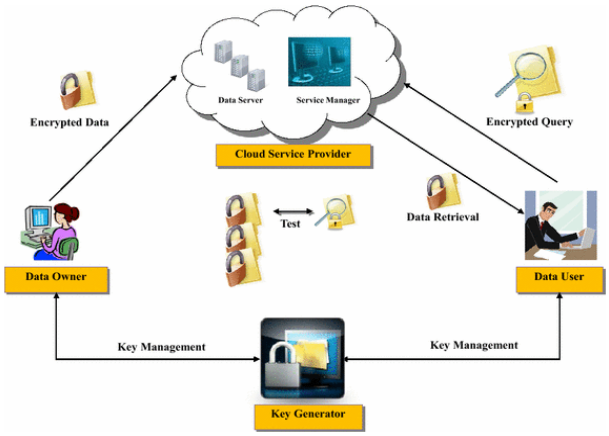

Figure.5 SE encryption.

AES (Asymmetric searchable encryption) algorithm

The encryption depends on asymmetric key or public key. Functionality is the advantage of AES and inefficiency is the major drawback of AES.

Searchable Symmetric Encryption

Searchable Symmetric Encryption (SSE) [2] provides the high security that allows the data is stored in third party for privacy maintenance. The symmetric encryption is the cryptographic algorithm. The encryption is based on symmetric key or private key. It uses a same key for encryption and decryption. The solutions of SSE are trade - off between efficiency, security and confidently update the data and finally this information is encrypted then

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 10, October 2016

uploaded. The main aim of SSE is practical competence. The SSE is compare to the homomorphic encryption / multiparty computation that provide the high security but one draw is not expected for well-organized practical. Efficiency is the advantage of SSE since all SSE schemes depends on PRF and block ciphers. The functionality is the drawback of SSE.

Cuckoo Hashing

In general the cuckoo hash table[16] contains the array of buckets that determine the hash function. Cuckoo hashing is an open addressing format. The hash table holds the Key value pair or key. Cuckoo hashing is resolving the hash table collision[27]. It use two hash table for avoid the collision. Each key location is determined by hash function. Each key provide the possible location of hash table. The hash table divides into two equal size of table and has hash function. Two hash functions provide the index to single table. The Operation of Cuckoo hashing is Insert, Delete, and Search: The element is searched in two locations at same time. The lookup procedure check if the bucket contain the item or not. The greedy algorithm is used for insert the element into hash table. The main aim of cuckoo hashing is improving the space by load factor. The failure rate is reduced by rebuild the data structure with less frequent. The cuckoo hash table presents set membership information for application. Software based Ethernet switches internal data structure as cuckoo hash table. Cuckoo hash table performance improved by partial key cuckoo hashing. It also called optimization.

Advantage of cuckoo hash function

1) New table allocation is no need for rehashing.
2) Deletion operation done by general Insertion procedure instead of finding the position of element.

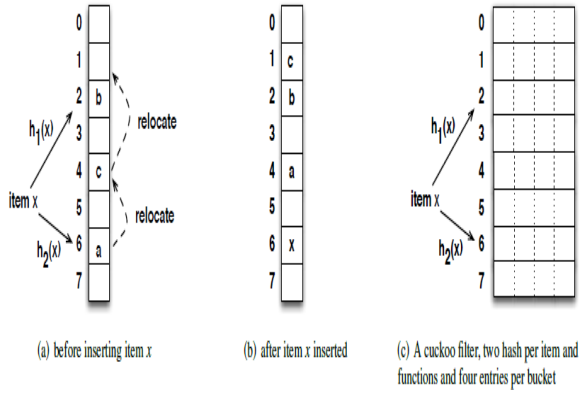

Figure 6 .Operation of Cuckoo hashing.

Cuckoo Filter

A cuckoo filter[6] is a crushed 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

1) It supports dynamic insertion and deletion.
2) It offers high lookup performance than bloom filter.
3) Easy to implement.
4) Less space and less than 3% of false positive rate.

Pseudo Random Function

Pseudo Random Function (PRF)[24][29] is group of computable functions. Pseudorandom functions are essential tools for primitive structure of cryptographic and encryption technique. PRF is a random function that selects the function from same value set or same domain.The pseudorandom generator (PRG) [25]constructs the pseudo random function. PRF is defined by deterministic function of (Key, Message, Output) and return the random sequence output .i.e. F: K x M -> O.All the outputs are appeared random in PRF but PRG the single output is appeared randomly. 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 code book.
- CBC - cipher block chaining.
- OFB - Output Feedback Mode.
- Counter mode.

Merits

- Use general principle.
- Random functions provide the more security to the system.
- Set of functions are mapping from n bit strings to n bit strings.

Limitation

- Input ,output and key has same size.

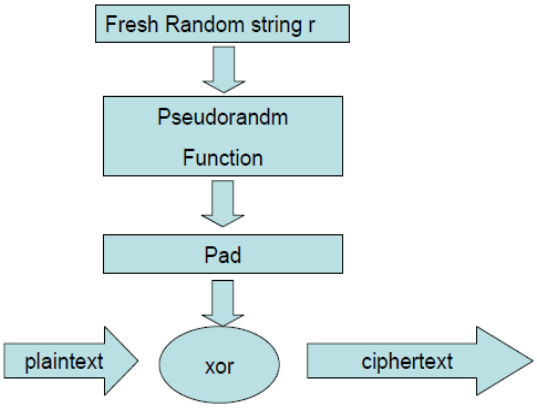

Figure 7. Encryption with PRF

IV. ADAPTIVE VIDEO STREAM

At present, increasing the growth of on line vides delivery that requires the high quality of video stream. One of the famous methodology is HAS (HTTP – based adaptive streaming)[4][5]. The contents are separated into small chunks. Each chunk video bit is dynamically allocated in real time by HAS client. The drawback of HAS is: i)

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 10, October 2016

Application layer's rate adaption is conflict with congestion control of TCP's. ii) The downloading suffers from chunk period of on/off. These problems are overcome by another video streaming technology as DASH ,MMT (MPEG Media Transport). The client rate adaption logic is neglects the caching server transparent that over estimate the current bandwidth. This is the incorrect selection of chunk video bit rate.

DASH

The technology of adaptive bit rate streaming is called Dynamic Adaptive Streaming over HTTP (DASH)[19][26].It also called MPEG-DASH. DASH delivers the high quality of streaming content to web servers. The contents are divided into small file segment [HTTP –based file]. The segment contain the interval time, various bit rate. Dash accepts the network condition and provides the play back with high quality and minimum stalls. The first adaptive bit rate solution of HTTP –based streaming is DASH. The transport protocol of DASH is TCP. DASHEncoder is content generation tool of DASH. DASHEncoder encode the DASH content. The working principle of Dash is the video file is encoded with different versions. It has a different resolution / rate called media presentation or representation. Video representation has the same content but content quality is different. The representation is further divided into segments based on time. Each segment has equal time or length (e.g. 5 seconds). All the segments are stored in content server. MPD (Media presentation Description) identifies the video resolution, representation, rate of playback and store in the location. The different Product of Adaptive video are Adobe HDS (HTTP Dynamic Streaming) , Apple HLS (HTTP Live Streaming) and Microsoft smooth streaming.

MMT

MMT video delivery[8] use Content-Based Caching (CDC).Caching proxy of CDC place between clients and MMT server. The video content is delivered by MMTP protocol. MMT manage the online distribution video. The drawback of DASH is overcome by MMT.The major drawback of MMT[14] is scalability of server while the number of client increases. This drawback is overcome by MMT caching middle boxes (MMT-CMB). The MMT-CMB[22] is placed between the server and client. The two main role of MMT is i) CMB is close to client, it act like a MMT-server and perform the perfect video rate adaption and monitor the congestion of network. ii) Proficiently utilize the server-side bandwidth by caching video chunks. The media format of MMT is logical structure. It also called package that contain the Composition Information (CI) and multiple assets. The assets are media data encryption, CI and logical structure.

MMT caching middle box of adaptive video Stream

The adaptive video streaming of MMT-CMB is positioned near to the clients and monitor the network congestion that suffers from bottleneck. The video playback buffer is eliminated by reducing MFUs.

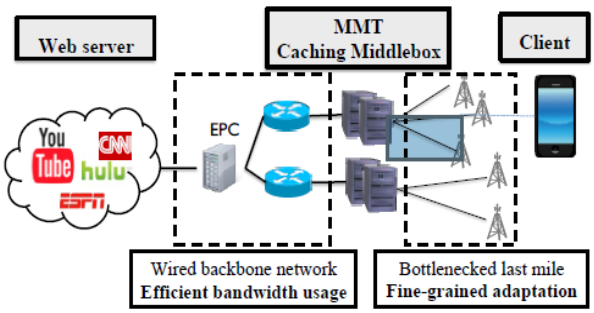

Figure.9 overview of MMT-CMB.

Protocol of MMT-CMB

Table 1. Different protocol for MMT-CMB

Sl. no	Format	Purpose
1	X - MPU RANGE : N-M	Request MPU IDs from Nth MPU to Mth MPU.
2	X – MPURequest : N	Request full content of Nth MPU.
3	X – MPU HeaderRequest : N	Request only metadata part of Nth MPU.
4	X-HTML Request	Request HTML file of package.
5	X- CIRequest	Request CI file of package.

V. CONCLUSION

This paper presented a survey on secure video delivery through encrypted In-network caching. This enables the effective and secure video delivery in the network, to develop a secure architecture as information centric network, Content delivery network and In-network caching. And discuss the different encryption techniques, algorithm, Hashing function and adaptive video stream protocol for securely deliver the video content.

REFERENCES

[1] SomayaArianfar, PekkaNikander and Jorgott,"On Content-Centric Router Design and Implications", in ACM, November -30-2010.
[2] Reza Curtmola, NJIT Juan Garay and Seny Kamara ," Searchable Symmetric Encryption: Improved Definitions and Efficient Constructions ",13th ACM Conference on Computer and Communications Security-2006.
[3] Abhishek Chanda and Cedric Westphalyz,"Content Flow: Mapping Content to Flows in Software Defined Networks " ,arXiv:1302.1493v2 [cs.NI] Feb-7- 2013.
[4] Ruoyu Wang, Yan Shoshitaishvili, Christopher Kruegel, and Giovanni Vigna, "Steal This Movie - Automatically Bypassing DRM Protection in Streaming Media Services", in SEC'13 proceeding of the USENIX conference on security ACM - Aug 14-2013.
[5] Yi Sun, Seyed K. Fayaz, Yang Guo, and Vyas Sekar," Trace-Driven Analysis of ICN Caching Algorithms on Video-on-Demand Workloads ", ACM -2014.
[6] Bin Fan, David G. Andersen, Michael Kaminskyy, and Michael D. Mitzenmacher," Cuckoo Filter: Practically Better Than Bloom ", ACM -2014.

[7] S. K. Mehertaj, K. V. Subbaiah, P. Santhi, and T. Bharath Manohar,"An Efficient Distributed Control Law for Load Balancing in Content Delivery Networks "International Journal ,of Modern Engineering Research (IJMER)", Vol. 3, Issue. 4, pp-2514-2521, Jul - Aug. 2013.
[8] Justine Sherry, Shaddi Hasan and Colin Scott," Making Middle boxes Someone Else's Problem: Network Processing as a Cloud Service", ACM-2012.
[9] Nachikethas A. Jagadeesan, Ranjan Pal and Kaushik Nadikuditi," A Secure Computation Framework for SDNs ", ACM -2014.
[10] George Xylomenos, Christopher N. Ververidis, Vasilios A. Siris, Nikos Fotiou, and Christos Tsilopoulos, Xenofon," A Survey of Information-Centric Networking Research", IEEE -2012.
[11] Satyajayant Misra, Reza Tourani and Nahid Ebrahimi Majd," Secure Content Delivery in Information-Centric Networks: Design, Implementation, and Analyses", ACM -2013.
[12] Diego Perino, Matteo Varvello and Krishna P. N. Puttaswamy," ICN-RE: Redundancy Elimination for Information-Centric Networking ", ACM-2012.
[13] Ioannis Psaras, Wei Koong Chai and George Pavlou," Probabilistic In-Network Caching for Information-Centric Networks ", ICN 12 workshop on information-centric networking ACM -2012.
[14] Justine Sherry, Chang Lan, Raluca Ada Popa, ETH Zürich and Sylvia Ratnasamy," Blind Box: Deep Packet Inspection over Encrypted Traffic ", ACM -2015.
[15] George Xylomenos, Christopher N. Ververidis, Vasilios A. Siris, Nikos Fotiou, and Christos," A Survey of Information-Centric Networking Research", in communications surveys and tutorials, vol. 16, no. 2, 2014.
[16] Won So, Ashok Narayanan and David Oran," Named Data Networking on a Router: Fast and DoS-resistant Forwarding with Hash Tables ", IEEE -2013.
[17] Jinjin Liang, Jian Jiang, Haixin Duan, Kang Li, Tao Wan , Jianping Wu," When HTTPS Meets CDN: A Case of Authentication in Delegated Service ", IEEE -2014.
[18] Ali Ghodsi, Teemu Koponen, Scott Shenker, and James Wilcox," Information-Centric Networking: Seeing the Forest for the Trees ", ACM -2014.
[19] Stefan Lederer, Christopher Müller, and Christian Timmerer," Dynamic Adaptive Streaming over HTTP Dataset ", ACM-2012.
[20] Ashok Anand, Vyas Sekar and Aditya Akella," SmartRE: An Architecture for Coordinated Network-wide Redundancy Elimination ", ACM -2009.
[21] Yongdong Wu, Zhuo Wei, and Robert H. Deng," Attribute-based Access to Scalable Media in Cloud-assisted Content Sharing Networks ", IEEE-2012.
[22] Sangwook Bae, Giyoung Nam and KyoungSoo," case for caching middle boxes for scalable MMT video delivery", IEEE -2015.
[23] www.tutorialspoint.com/cryptography/advanced_encryption_standard.htm.
[24] www.crypto-it.net/eng/theory/prf_and_prp.html.
[25] Crypto.stackexchange.com/questions/22318/difference-between-pseudorandom-function-vs-randomly-chosen-function.
[26] WIKIPEDIA.ORG/WIKI/DYNAMIC_ADAPTIVE_STREAMING_OVER_HTTP.
[27] WWW.lkozma.net/cuckoo_hashing_visualization.
[28] Ioannis Psaras, Wei Koong Chai, and George Pavlou," In-Network Cache Management and Resource Allocation for Information-Centric Networks ", IEEE transactions on parallel and distributed systems, MAY 2013.
[29] Pseudo-random Generators (PRG): Introduction to Cryptography.
[30] John Bethencourt, Amit Sahai and Brent Waters," Cipher text-Policy Attribute-Based Encryption ", in SP '07 proceedings – IEEE symposium of security and privacy -2007.
[31] J. Staddon, D. R.Stinson and R. Wei," Combinatorial properties of frame proof and traceability codes ", IEEE Transactions on Information Theory – 2001.
[32] A. Silverberg, J. Staddon and J. Walker," Efficient traitor tracing algorithms using list decoding", Asiacrypt- 2001.
[33] en.wikipedia.org/wiki/Broadcast_encryption.