International Journal of Contemporary Research in Computer Science and Technology (IJCRCST) e-ISSN: 2395-5325
Volume3, Issue 7 (July '2017)

SECURE AND EFFICIENT VIDEO DELIVERY THROUGH USER INDEX IN-NETWORK CACHING

T.T.Mathangi,
Assistant Professor,
Department of Computer Science & Engineering,
K.L.N. College of Information Technology,
Pottapalayam, Sivagangai Dist, Tamil Nadu.

S.Dhivya,
Assistant Professor,
Department of Computer Science & Engineering,
K.L.N. College of Information Technology,
Pottapalayam, Sivagangai Dist, Tamil Nadu.

S.Jeniba,
Assistant Professor,
Department of Computer Science & Engineering,
K.L.N. College of Information Technology,
Pottapalayam, Sivagangai Dist, Tamil Nadu.

Abstract: This paper, we present a new in networked system for efficient encrypted video delivery while preserving the benefits of in-network caching. As video chunks are encrypted before distribution, we first design a compact, efficient, yet encrypted video user index to empower the network with a fully controlled capability of locating the cached encrypted chunks for given encrypted requests. We then explain how to deploy the encrypted design in our proposed architecture, and present a secure redundancy elimination protocol to enable fast video delivery via leveraging cached encrypted chunks. We further discuss the full support of cache management, adaptive video delivery, and video access control. Rigorous analysis and prototype evaluations demonstrate the security, efficiency, and effectiveness of the design.

Keywords: Video Delivery, Encryption, MD5 Public Key Algorithm

I.INTRODUCTION

Videos have been increasingly dominating today's Internet traffic, with Cisco projecting that 75% of all network traffic in 2018 will be video based [1]. To scale the delivery of massive volumes of videos, various new network architectures with optimizations for content-intensive applications have been proposed, such as information-centric networking (ICN) and others as surveyed in [2]. Among these proposals, one natural trend is to leverage in-network caching, i.e., storing the content in advanced network devices like cache-enabled routers[3].The related benefits, like efficient and scalable content. distribution, redundant network traffic elimination, etc., are well understood in the literature [6]–[9]. Despite being promising, in-network content caching would also raise new security and privacy concerns, due to the increasingly un trusted networked environments [10], where the network caching devices are not necessarily in the same trusted domain as the content users or under the full control of content providers [11]. 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 .For content providers, strong protection against authorized content access or copyright infringement is a commercial imperative.

We note that directly encrypting the videos before distribution does not address the issues completely. It would diminish the benefits of in-network caching by preventing the cache enabled routers from accessing the data they need to inspect for their job. Encrypted protocols that secure end-to-end transmission channels, like HTTPS, are also not satisfying in fully leveraging the complete benefits of in-network caching [14]. Solutions that resort to decrypting the traffic some wherein the middle, e.g., public caches in CDNs,would fall short of guaranteeing the end-to-end security [16], vulnerable to the possible man-in-the-middle attacks [13].

In order to address the aforementioned limitations and challenges, in this paper we propose and implement a new networked system that aims for secure and efficient encrypted video delivery while reserving 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.Similar to existing standards of adaptive video delivery, like DASH [17], our system first segments the video files into smaller chunks. But for confidentiality, all video chunks are encrypted before distribution and remain in encrypted forms during their lifetime in cache-enabled network devices. We use content user index for chunk identification, and propose an encrypted fingerprint index to empower the network with a fully-controlled capability of securely locating and leveraging the cached encrypted chunks for efficient video delivery.

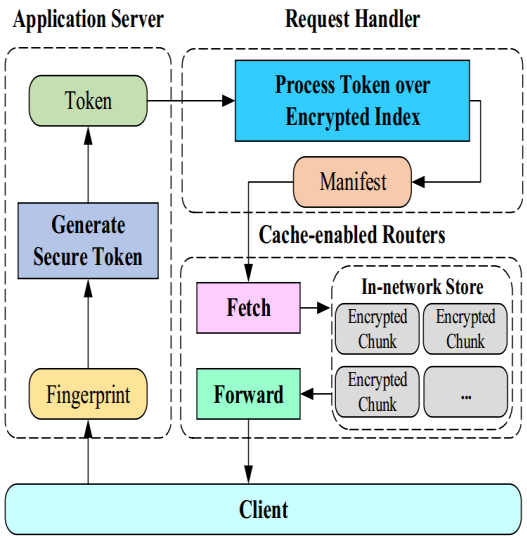
The proposed encrypted index achieves both security and efficiency. It follows the practical cryptographic framework called searchable symmetric encryption [18], [19], but also incorporates he latest design philosophy from high

performance in-memory indexing [20]. Different from prior arts, this new encrypted design is built from the ground up, and achieves optimal secure processing time, secure dynamic update, high throughput, and low memory consumption with high load factors, simultaneously.

In our proposed architecture, we deploy the encrypted index on a bunch of semi-trusted in-network request handlers, which serve as network middle boxes to locate and manage the encrypted in-network caches upon encrypted requests for video applications. Under such settings, we give a carefully designed protocol for secure redundancy elimination (RE),a crucial functionality for high performance video delivery, which can be instantiated over cached encrypted chunks. Specifically, the proposed protocol ensures that without a secure token generated from a valid user index, the entire network learns nothing about video content or the user index.

For further practical considerations, we also show how our system functions compatibly with known cache management strategies [6], inherently supports adaptive video delivery [17], and readily provides fine-grained access control restrictions for encrypted video distribution [14].We emphasize that the proposed system is not limited to secure and efficient video delivery. It can be applied for general content delivery with strong data protection, e.g., documents, music, images, etc. It also fits in the generic contexts of semi-trusted network middle boxes, which could be offered as a "service" by un trusted public cloud [23]. meanwhile, the proposed encrypted index and the secure RE protocol can flexibly work for encrypted data with different size granularity.

II. SYSTEM ARCHITECTURE



III.EXISTING SYSTEM

To scale the delivery of massive volumes of videos, various new network architectures with optimizations for content-intensive applications have been proposed, such as information-centric networking (ICN) and others as surveyed. Encrypted protocols that secure end-to-end transmission channels, like HTTPS, are also not satisfying in fully leveraging the complete benefits of in-network caching. Solutions that resort to decrypting the traffic somewhere in the middle, e.g., public caches in CDNs, would fall short of guaranteeing the end-to-end security vulnerable to the possible man-in-the-middle attacks. Standards of adaptive video delivery, like DASH, our system first segments the video files into smaller chunks. But for confidentiality, all video chunks are encrypted before distribution and remain in encrypted forms during their lifetime in cache-enabled network devices.

IV.PROPOSED SYSTEM

To leverage encrypted in-network caching, we then design an encrypted user index, and propose a secure RE protocol to identify and locate the encrypted chunks with a controlled capability. As a result, the users can securely obtain the videos from cache-enabled routers to avoid redundant transmission from video application servers. we show that our design works compatible with existing caching management policies, and further introduce secure dynamic operations for video addition and deletion. Our system works compatibly with known cache management policies for content placement and eviction. The performance of encrypted DASH videos to show the system feasibility in existing media streaming standards. The decryption takes less time than the encryption, because we use the AES-CBC model. This system provide End – to – End security.

V.IMPLEMENTATION

Video consumers who have legitimate private keys to decrypt the videos. They pay video content providers for authorized video access. User can select video and get encrypted user index. Send the request to the application.
Get the video chunks and combine the video, then decrypt the video chunks. They deal with user authentication and key management, and encrypt all the video chunks before distribution .It generate the token for the requested user. Send the secure token to the request handler They can be dedicated servers, or network middle boxes with computing and storage abilities, which identify, locate, and manage the in-network chunks. It process the token over encrypted index. Send request to cache enable routers They are the network devices that are able to store, match, and forward content. It Check the requested video is exist or not Chunks and encrypt the video .Send the video to the user.

VI.METHODOLOGY

MD5-PUBLIC KEY ALGORTHIM:

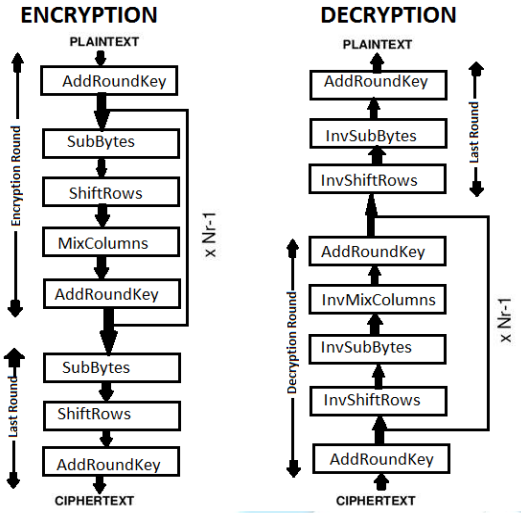
The primary threat to the security of a fingerprint is a pre image attack, where an attacker constructs a key pair whose public key hashes to a user id which matches the victim's user id. The attacker could then present his public key in place of the victim's public key to masquerade as the victim. In practice, most user index commonly used today are based on non-truncated MD5 or SHA-1 hashes. As of 2006, collisions but not pre images can be found in MD5, and although no practical attack yet exists against SHA-1, it has been partially broken. The future therefore likely to bring increasing use of newer hash functions such as SHA-256. However, user index based on SHA-256 and other hash

functions with long output lengths are more likely to be truncated than (relatively short) MD5 or SHA-1 user index.

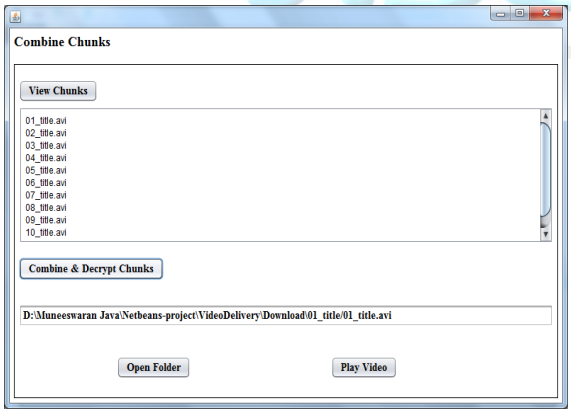
AES ALGORITHM:

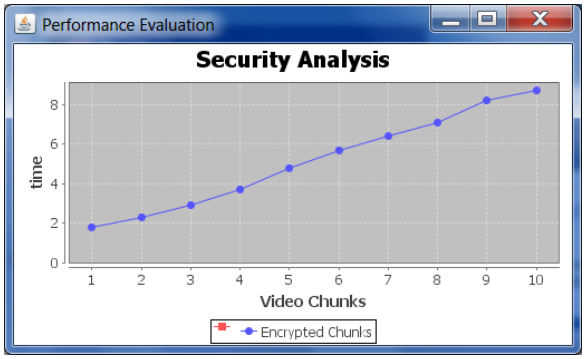
AES is a symmetric block cipher. However,AES is quite different from DES in a number of ways. The algorithm Rijndael allows for a variety of block and key sizes and not just the 64 and 56 bits of DES' block and key size. The block and key can in fact be chosen independently from 128,160,192,224,256 bits and need not be the same.

AES ALGORITHM:



EXPERIMENTAL RESULTS





The proposed RE protocol reduces the video delivery time greatly via encrypted in network caching with marginal security overheads introduced.

VII.CONCLUSION

In this paper, we presented a system that enables secure RE over encrypted video chunks. The system architecture is built on the emerging network architectures towards content intensive applications. We designed an encrypted and high performance user index, and proposed a secure RE protocol to leverage encrypted in-network caching for video delivery without knowing the underlying video content and fingerprints. Besides, our system also supports encrypted dynamic cache management, adaptive video streaming, and one to-many access control protocols. We have proven that our system is secure against adaptive chosen-keyword attacks.

We implemented the system prototype, and conducted comprehensive evaluations. The results show that the proposed index processes secure content requests with millisecond latency on a commodity server. Besides, the proposed RE protocol reduces the video delivery time greatly via encrypted in network caching with marginal security overheads introduced. The evaluation on a real DASH dataset demonstrates that our system adaptively delivers encrypted videos with comparable performance to the plaintext case. In future, we will consider a more realistic scenario to enable authorized content delivery via encrypted in-network caches from multiple content providers under their own different keys. Other threats like collusion attacks will also be investigated as future directions.

VIII.REFERENCES

[1] Cisco, "Virtual Networking Index (VNI)," http://www.cisco.com/web/ solutions/sp/vni/vni forecast highlights/index.html, 2015.

[2] B. Ahlgren, C. Dannewitz, C. Imbrenda, D. Kutscher, and B. Ohlman, "A survey of information-centric networking," IEEE Communications Magazine, vol. 50, no. 7, pp. 26–36, 2012.

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

[4] W. So, A. Narayanan, and D. Oran, "Named data networking on a router: fast and dos-resistant forwarding with hash tables," in Proc. Of ACM/IEEE ANCS, 2013.

[5] Cisco, "Cisco ASR 9000 Series Integrated Service Module," on line at: http://www.cisco.com/c/en/us/products/collateral/routers/asr-9000-seriesaggregation-services-routers/data sheet c78-663164.pdf, 2012.

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

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

[8] A. Chanda and C. Westphal, "Contentflow: Mapping content to flows in software defined networks," in Proc. of IEEE Globecom, 2013.
[9] Y. Sun, S. K. Fayaz, Y. Guo, V. Sekar, Y. Jin, M. A. Kaafar, and S. Uhlig,"Trace-driven analysis of icn caching algorithms on video-on-demandworkloads," in Proc. of ACM CoNEXT, 2014.
[10] N. A. Jagadeesan, R. Pal, K. Nadikuditi, Y. Huang, E. Shi, and M. Yu, "A secure computation framework for sdns," in Proc. of ACM HotSDN,2014.
[11] R. Wang, Y. Shoshitaishvili, C. Kruegel, and G. Vigna, "Steal this movie: Automatically bypassing drm protection in streaming media services." in Proc. of USENIX Security, 2013.
[12] S. Misra, R. Tourani, and N. E. Majd, "Secure content delivery in information-centric networks: design, implementation, and analyses," in Proc. of the 3rd ACM SIGCOMM workshop on Information-centric networking, 2013.
[13] J. Liang, J. Jiang, H. Duan, K. Li, T. Wan, and J. Wu, "When HTTPS meets CDN: A case of authentication in delegated service," in Proc. ofIEEE S&P, 2014.
[14] F. Angius, C. Westphal, M. Gerla, and G. Pau, "Drop dead data: Whatto expect securing data instead of channels," in Proc. of IEEE CCNC, 2015.
[15] D. Dorwin, A. Bateman, and M. Watson, "W3c editor's draft: Encrypted media extensions," on line at: https://w3c.github.io/encrypted-media/, 2015.
[16] J. Sherry, C. Lan, A. R. P. Popa, and S. Ratnasamy, "Blindbox: Deep packet inspection for encrypted traffic," in Proc. of ACM SIGCOMM, 2015.
[17] ISO/IEC 23009-1:2014, "Information technology – Dynamic adaptive streaming over HTTP (DASH) – Part 1: Media presentation description and segment formats," 2014.
[18] R. Curtmola, J. A. Garay, S. Kamara, and R. Ostrovsky, "Searchablesymmetric encryption: Improved definitions and efficient constructions," Journal of Computer Security, vol. 19, no. 5, pp. 895–934, 2011.
[19] S. Kamara, C. Papamanthou, and T. Roeder, "Dynamic searchable symmetric encryption," in Proc. of ACM CCS, 2012.
[20] B. Fan, D. G. Andersen, M. Kaminsky, and M. D. Mitzenmacher, "Cuckoo filter: Practically better than bloom," in Proc. of ACMCoNEXT, 2014.
[21] ISO/IEC 23008-1:2014, "Information technology – High efficiency coding and media delivery in heterogeneous environments – Part 1: MPEG media transport (MMT)," 2014.
[22] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved proxy re-encryption schemes with applications to secure distributed storage," ACM TISSEC, vol. 9, no. 1, pp. 1–30, 2006.

