© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 12 Issue: 03 | July - September 2021
Paper is available at http://www.jrps.in | Email : info@jrps.in

Video Content Encryption and Cloud Video Security: A Review

Mohit Malik, M. Tech.
Ms. Shalini Bhadola, Kirti Bhatia, Assistant professor
Department of CSE, Sat Kabir Institute Of Technology And
Management Maharishi Dayanand University

Abstract

Cloud Server attaches emphasis to its digital multimedia data gathering. Multimedia data become the primary source of information in a library and preferred collecting method. Digital materials are not secure by their nature on the network. Today in communications and telecommunications Current multimedia technologies will broadcast the material continuously. Hackers and eavesdroppers technically referred to as possible hazards by corrupting or stealing vital information carried on through Communication are extremely important to stop. Ensure security for various multimedia applications such as on-demand video service, video conferencing, video streaming and multimedia mails. A secure video transmission guarantees that consumers cannot get information from video from unauthorised eavesdroppers when it is transmitted to the receiver, meaning that users who pay for these services may only see videos and films.

Keywords: Communication, Multimedia, Cloud Server, Digital, Conferencing, etc.

Introduction

Current multimedia (digital communications) technologies will broadcast ongoing material. Hackers and eavesdroppers technically referred to as possible hazards by corrupting or stealing vital information carried on through Communication are extremely important to stop. Because of the need for streaming videos, streaming apps will be limitless.

Secured video transmission's main purpose is to provide: authentication, tracking of material, restricted access, copy control, secrecy. Security level varies with each video programme. The necessary security application may be categorised as: VoD and pay TV entertainment apps.

The video encryption methods used in recent years have mostly developed to optimise encryption time and cost, and selective video encryption increased more or less during the previous decade.

The addition of less data for selective encryption is not free. Some of the following issues are associated with current selective encryption methods. Careful balance and trade – a multimedia encryption for a particular application must be developed.

1. Inadequate safety. Partial information is encrypted via selective encryption. Must emphasis on selective encryption methods is not content secrecy but perceptive impairment. Usually, a piece of encryption using selective encryption still contains some structural content information. Although there is a perceptual degradation, many selective encryption programmes suffer from perceptual attacks, which allows simple signal processing technology to recover significantly enhanced coefficients and vectors, DC and low-frequency AC coefficients and meaningful DCT bit plans with error concealment and other image processing technologies to recover significantly. Different statistical features with frequency coefficient may also be used to launch cypher text only attacks against selective encryption systems. For example, a low pass image property may be utilised to significantly limit the search space to only launch an attack on a method that randomly permits the order of Zigzags of DCT coefficients in Tang. Moreover, many selective encryption systems Unable to resist the known plaintext or the plaintext attack selected. Encrypted data part in selective encoding and perceptive multimedia redundancy make plaintext assaults a serious danger.

2. Important compression efficiency overhead. Some of the previously mentioned selective encryption systems alter compressed or compressed data statics, which significantly reduces compression efficiency. For example, encryption of the chosen bit plan alters the original statistical characteristics of the impacted Bit plans and makes it harder for them to compress using a later compression method. Random zigzag scan permutation of DCT coefficients modifies the optimum architecture of the original JPEG and MPEG compression to reduce compression efficiency.

3. Sharing the Key While selective sharing of video encryption key is a major issue, such as symmetric key encryption, which leads to overhead communication that increases delaying multimedia content communications, and increases the vulnerability to asymmetric key encryption and then access to video, this results in hacking or access to secure video content.

Video content authentication issues

1. All other methods provide partial safety Some of them offer privacy Some of them provide authentication or some of them give access restriction. There is no composite solution that can guarantee that the bi-part or one-party conversation ends securely and authentically.

2. Most current video authentication models utilise visible or invisible watermarking methods, however the payload capacity and video quality after the watermarking process are extremely low with regards to image quality.

3. Hackers may simply obtain the current secret symbols of video authentication since it is embedded and no data fragmentation is performed.

Secure Video Streaming Cloud Issues

1. Video on Demand is a non-actual time streaming technology that has developed over the last years in cloud computing, but has made less effort to guarantee safe communication in the cloud.

2. Efforts were taken to ensure safety at one end or at the end of the storage, but not both in combination.

3. Most cloud providers providing Video on Demand do not offer SSL security when streaming StraaS (Storage as Service) video and security ads.

In addition to debates and references, more has to be done in secure cloud video communication, which may be developed and implemented to guarantee safe and quick video streaming. Works carried out separately by different researchers and technocrats are extremely powerful, but they are not compiled and are not a comprehensive answer.

Review of literature:

Rahat Afreen and S.C. Mehrotra **(2011)** This article discusses cryptography, which uses the public key, commonly known as PKC systems. In PKC systems, two keys which are completely distinct are used for encoding and decoding data. Safety and strength is determined by big key sizes, since one of two keys is disseminated in PKC systems and kept accessible to the whole public. Mathematical difficulties like prime factorization and discrete logarithm have already been used in PKC systems. The ECC has promised and shown safety with almost equal to above with relative tiny sizes of key.

Paul Kocher, Ruby Lee, Gary McGraw , Anand Raghunathan and Srivaths Ravi **(2004)** This article discusses the security element of embedded in depth. A case study has been conducted taking into consideration attempts to secure electronic systems, in increasing instances, where data from embedded systems have been hacked and destroyed, resulting to a significant loss in the past few years. Embedded global systems that are specially and especially used for data collection and then storage and access if needed to maintain their security sensitivity have a great deal of security and other difficulties in ensuring complete data security. In the area of cryptographic computers and network security, significant research is underway.

Junfeng Fan, Kazuo Sakiyama and Ingrid Verbauwhede **(2009)** The following article includes Elliptic Curve Cryptography (ECC) on a multi-core embedded system and detailed techniques for scheduling tasks at different levels. A technique for planning instructions using

the core to perform operations in parallel has been suggested for a single modular operation. Then, several fundamental modular processes are executed in parallel. A comparison study with two implementations was developed to plan connecting above two kinds of parallelism. Here, the field programmable gate array Elliptic curve cryptography has been utilised and implemented over a prime field.

***Thomas Eisenbarth, Sandeep Kumar, Christof Paar, Axel Poschmann and Bochum Leif Uhsadel* (2007)** In this article, a Lightweight-Cryptography Implementation Survey Report has been examined and an above map assessed. A completely different lightweight cryptography is to create a new hardware-optimized cypher from the base level and also to implement efficiently or adapt it to a small extent to a well-established cypher. In this way, it is an SPN based on a network with replacement permutations and a thirty two rounded cypher which is one block with sixty four bits of block size and a key size of eighty or one twenty eight bits.

***Wang Qingxian* (2006)** The basics, components and characteristics of cryptosystems of Elliptic Curve have been explored in depth here. It also provides information between elliptical curve encryption and embedded world applications. This is done with the results, virtues and demerits of performance, etc. They also emphasised the significance of information security and must safeguard it in all systems in the embedded environment. To this end, they conducted a comprehensive analysis of ways to attack such a system and how to counteract them from the surface.

***Lejla Batina, Alireza Hodjat, David Hwang, Kazuo Sakiyama and Ingrid Verbauwhed* (2006)** This article examines several designs that are suited to the use of cryptographic services to improve security and system protection, taking into account the lowest feasible costs. To establish a number of compatibility hardware combinations in elliptical and super elliptical curve cryptography. It is recorded and a thorough analysis is conducted to learn huge bit lengths and the impact of complicated arithmetic on an 8-bit built-in microcontroller. Here we can see that a few of the major variables affect performance.

***HoWon Kim1 , YongJe Choi1 and MooSeop Kim1*(2005)** In this article the authors reported the design and implementation result of a cryptoprocessor consisting of a 32-bit RISC processor and a 3-bit DES and SEED co-processor block. The private key crypto algorithms dedicated crypto processor block is accelerated and the crypto controller programmability enables the rapid execution of different crypto-algorithms (such as RSA, ECC etc.) and security application. Hynix's 0.5m CMOS technology is utilised as an ASIC chip for the implementation

of the cryptoprocessor.

***Marc Joye,ascal Paillier and Berry Schoenmakers*(2009)** This article covers the analysis of differential power (DPA). Differential Power Analysis (DPA) is the most effective and efficient analytical technique for cryptography, which seeks to recover critical sensitive secured data from the systems via the process of sampling and tracking power usage. The use of different strategies and approaches to mask, such as data whitening techniques, by hardware designers and software programmers may avoid leakages.

***Song Sun Zijun Yan Joseph Zambreno*(2008)** This article analyses different outcomes during the experimentation of embedded systems based on FPGA attacks with DPA (Differential Power Analysis). After conception and publication of the aforementioned, the global power analysis assaults were felt in public. Using techniques and methodologies to counteract and avoid power analysis assaults, the same was done extensively with software such as smartcards and digital signal processing and is also used for hardware such as field programmable grid array, etc.

***I. Branovic, R. Giorgi, E. Martinelli*(2003)** This article analyses the use of Elliptic Curve in cryptography and its characterisation of the workload in embedded environments. Elliptically Curved Cryptography (ECC) has developed into the most effective and user-friendly public key system in settings that have limited and restricted resources and are very tiny in terms of key sizes and computational efficiency, while retaining the same safety standards. It developed a set of benchmarks that could be used for a standard comparison and corresponding public-key techniques on the elliptical curve.

Cloud Server Digital Data Security Steps

Data security is an ongoing process of due care and due diligence to prevent unauthorised access, use, disclosure, destruction, alteration and interference to digital information systems. It is an unending data security procedure. The security and management of data is an important component of IT. Data security includes various computer systems elements, hardware and software, operating system, user components, network components and server components. Libraries and information centres act as intermediaries between the developer of information and the end user. Digital data transaction needs data protection, content security, permitted usage and user privacy. Access to pricing data is limited to IP-specific machines and password-protected.

Conclusion:

Security for various multimedia applications such as video on-demand, video, video and media streaming is essential. A secured video transmission guarantees that the user does not get the information from the video while it is transmitted to the recipient, i.e. that only users who have paid for these services may see the videos and films. When the video is redundant the attacker may recreate the original video file simply. Data like text and computer code is less redundant than movies in their structure. All these characteristics make it more difficult to provide security for an MPEG video. The security of the MPEG video transmission includes the encryption of portions of the MPEG bit stream or the whole bit stream.

Reference:

1. Han Qi, Abdullah Gani (2012). Research on Mobile Cloud Computing: Review, Trend and Perspectives. Second International Conference on Digital Information and Communication Technology and it's Applications (DICTAP), pp. 195-202.
2. Maneesha Sharma, Himani Bansal, Amit Kumar Sharma, International Journal of Soft Computing and Engineering 2(1) (2012) 421-424.
3. Nariman Mirzaei (2008). Cloud Computing. Available at: http://grids.ucs.indiana.edu/ptliupages/publications/ReportNarimanMirzaeiJan09.pdf
4. Peter Mell, Tim Grance (2011). The NIST Definition of Cloud Computing, the National Institute of Standards and Technology Report. 2011.
5. Sultan Ullah, Zheng Xuefeng (2013). Cloud Computing Research Challenges. IEEE 5th International Conference on Biomedical Engineering and Informatics, pp 1397-1401.
6. Tripathi A., Mishra A. (2011). Cloud Computing Security Considerations. Signal Processing, Communications and Computing (ICSPCC), IEEE International Conference.
7. Mohammad Reza Modarres Zadeh, International Letters of Social and Humanistic Sciences 3 (2013) 21-29.
8. Leah Garner-O'Neale, Jelisa Maughan, Babalola Ogunkola, International Letters of Social and Humanistic Sciences 2 (2014) 41-55.
9. Gaines, Helen Fouché (1939). Cryptanalysis, Dover, ISBN 0-486-20097-3. Considered one of the classic books on the subject, and includes many sample ciphertext for practice. It reflects public amateur practice as of the inter-War period. The book was compiled as one of the first projects of the American Cryptogram Association.

10. Konheim, Alan G. (1981). Cryptography: A Primer, John Wiley & Sons, ISBN 0-471-08132-9. Written by one of the IBM team who developed DES.
11. Patterson, Wayne (1987). Mathematical Cryptology for Computer Scientists and Mathematicians, Rowman & Littlefield, ISBN 0-8476-7438-X
12. Welsh, Dominic (1988). Codes and Cryptography, Oxford University Press, A brief textbook intended for undergraduates. Some coverage of fundamental information theory. Requires some mathematical maturity; is well written, and otherwise accessible.