International Journal for Research in Engineering Application & Management (IJREAM)
ISSN : 2454-9150 Vol-03, Issue-09, Dec 2017

A effective Encryption with Resource Optimization on Multimedia Files for Security

[1]Dheeraj Patil, [2]Prof. Manmohan Singh

[1]M.Tech, [2]Associate professor, Department of Cyber Security, RKDF School of Engineering, Indore, India.

Abstract -: **Multimedia data security is important for multimedia commerce. To maintain security and privacy, digital video needs to be stored and processed in an encrypted format. Previous cryptography studies have focused on text data. The encryption algorithms developed to secure text data may not be suitable for multimedia applications because of the large data size and real time constraint. So in this paper, we focus and investigated on the confidentiality of multimedia big data under resources constraints. Firstly, the growth trend of data volume compared with computational resources is discussed and an analysis model for multimedia data encryption optimization is proposed. Secondly, a general-purpose lightweight speed tunable video encryption scheme is introduced. Thirdly, a series of intelligent selective encryption control models are proposed. Fourthly, we as a contribution provide auditing to big files by using hashing algorithm. The experimental results have demonstrated the feasibility and efficiency of the proposed scheme.**

***Keywords* — *Internet of Things, multimedia sensing multimedia big data, video encryption, file auditing, MES*.**

I. INTRODUCTION

Information technology has been accompanied by information security problems since its birth. This situation is more severe in network times and the IoT- Internet of Things which based on the network communication technology inherits its security problems unsurprisingly. So in IoT the security issues of the big data become an innermost concern which may obstruct the development of IoT technology and also it has fascinated extensive attentions [1]. With regards to this reason the European Union established a framework of privacy and data protection impact assessment of IoT applications [4]. IETF also proposed a draft on security considerations in the IP-based IoT [5]. Multimedia big data generated by IoT system have some special characteristics like high volume, real-time, dynamicity, heterogeneity etc. As well as different characteristics like individual privacy should also be considered in the big data. Therefore, excepting the traditional security problems in distributed system, the particular characteristics of the multimedia big data have brought in some new security problems like individual privacy protection, processing of multimedia big data, and etc.

Especially, for large-scale multimedia collaborative work, video conference, intelligent video surveillance system and other multi-stream multimedia sensing system are important categories of IoT applications. The security of these hundreds of streams with high data volume becomes a new dispute. The nodes in those systems which process large amounts of media data might become the bottlenecks. Moreover, as to mobile, unplugged sensing devices, their limited computation and energy resources further restrict the protection of data security, because the computational complexities of encryption and decryption operation are very high [1]. So, due to the special characteristics of unplugged devices in IoT, data processing with limited resources has attracted researcher's attention [1][5]. In the period in-between, the impact of limited resources on IoT security has also been considered by various researches. That means selection of a suitable algorithm should depend on the particular application requirements rather than existing experimental research on data confidentiality under limited resources is somewhat quite rare. Also, auditing

DOI : 10.18231/2454-9150.2017.0065

module keep a watch on attack which tries to check the originality of file on cloud by using hashing procedure.

II. Related work

Information security has traditionally been ensured with different encryption techniques. Generally, encryption techniques such as the DES-Data Encryption Standard, AES-Advanced Encryption Standard, RSA-Rivest-Shamir-Adelman algorithm, 3DES-Triple DES, IDEA- International Data Encryption Algorithm and SEA-Scalable encryption algorithm, all of which work on bit stream of data input without regards to their nature of application. In other terms, the encryption proceeds without distinguishing the input data as either: audio, video, text, or graphics. The below table 1 shows the basic operation of above listed different algorithms as below [2],

Table 1: Different categories of algorithms

Encryption algorithm	Basic Operation	Advantages	Disadvantages
DES	XOR Substitution Permutation	Suitable for high speed and low cost hardware/software	Small 56-bit key size makes it undesirable
3-DES	Comprises 3 DES keys	Efficient & susceptible to chosen plain text	More memory & time required
AES	Sub bytes shift rows mix column & add round key	Very good performance in hardware & software implementations Low memory requirement	
IDEA	XOR Addition & multiplication	Security level is high as compared to DES	
RSA	Primality test modules Euler's totient function Co-prime & multiplicative inverse	It is public key system	Secured but speed is lower when compared with symmetric key systems
SEA	X-OR S-box word rotation bit rotation modular addition	Extremely simple	Used only in Embedded applications

If Multimedia data is not a real time data, it can be consider as a regular binary stream and then above different listed conventional techniques can be apply. But when varieties of constraints are present, then it is so difficult to carry out security for multimedia data.

III. Analysis

Computation and power resources in some IoT nodes are very scarce; these challenges become more serious when that complex data security process on multimedia data is restricted by the aforementioned limited resources. However, system not provides confidentiality to multimedia big data by considering resources constraints. The various researches proposed number of different techniques with its advantages and disadvantages are given as,

A. Partial encryption of compressed images and video

In 2000, Cheng and Li in his paper [9] described, initially offered partial encryption schemes for still images and further extensive to the video. This partial encryption schemes works with quad tree compression algorithms and wavelet compression algorithm based on zero trees for the video stream I-frame, motion compensation and residual error coding. Also, this scheme works for the video stream based on Set Partitioning in Hierarchical Trees image compression algorithm. Therefore, proposed methods are not suitable for JPEG images and hence these are not applicable for MPEG video compression standard. Proposed partial encryption encrypts the I-frames, motion vectors and residual error code of video stream.

B. A format compliant configurable encryption framework for access control of video

In year 2002, Wen et al.explain [10], the generalized ideas of selective encryption into format-compliant method called format Compliant Configurable encryption. In this scheme data is grouped in to information carrying and also if no any information carrying parts, then only information carrying fields are encrypted. These information fields can be of fixed length code (FLC) codeword's or variable length code (VLC) codeword's. Lastly, format compliance bits for encryption chosen and after encrypting with DES placed back to its original bit position in video stream.

C. Efficient frequency domain selective scrambling of digital video

In 2002, Zeng and Lei in his paper [11], proposed the frequency domain scrambling algorithm. This scheme of scrambling is based on some or all of the different three operations, first Selective bit scrambling, second block shuffling and third block rotation. As most of the video compression uses Wavelet Transform or Discrete Cosine Transform, hence this proposed encryption is designed for these distinct transforms.

D. Partial video encryption based on alternating transform

In 2009, Siu-Kei et. al. in his paper[12] proposed encryption technique during transform encoding phase. Also, they have proposed MTT based technique in which a transform is selected from various unitary transforms based on the key and the order in which the transform is applied is kept secret. This proposed scheme does not offer higher security as it is used only for the encryption of residual frames without encrypting I-frames and motion vectors but it has a low cost and in turn it results to low speed.

E. Fast and Secure Real-Time Video Encryption

In year 2008, author Narsimha Raju et. al. [13] proposed technique based on frequently occurring patterns in the DCT coefficients of the video and they state that computational complexity of the encryption proportional to the influence of the DCT coefficient on the visual data. Lastly they reported that the average encryption time taken by the algorithm is 8.32 ms per frame.

IV. Proposed System

In proposed system, we approached an optimization model for data encryption under resources constraint is proposed. Secondly, a general-purpose light-weight speed adjustable video encryption scheme is proposed, which reduce the computation overload on weak nodes and achieve a balance between performance and security. Thirdly, a series of selective encryption control models are proposed, in which the improved model is built based on SAFE encryption scheme. Further, we had added an auditing system which will add security to our data by providing auditing technique to our cloud data which will notify user about the data alteration or data hacked.

A. Multimedia File Upload

Multimedia File Upload model will let users to upload big volume of video file.

B. SOAP-Simple Object Access Protocol

SOAP originally defined as “Simple Object Access Protocol” is a protocol specification for exchanging structured information in the implementation of web services in computer networks.

C. Frames Segmentation

H.264 video process constitutes different types of frames like (I-P-B) and can be used for encryption to get the required efficiency and illustrate the theoretical formula for each quality of frames.

D. Optimizing Problem

Model M is the set of target multimedia data and MES is a set of corresponding multimedia encryption scheme. The optimization principle of this model is selecting appropriate encryption schemes for media data to maximize the security of utility value of multimedia information which would be protected (equals to minimize the utility value which could be got by attackers).

E. Selective Encryption Control Model

To build a general selective encryption control model, simplified multi-stream multimedia system is considered firstly. In this system, there are jt clients and the total number of media streams is not in time t. There are also some sink nodes and central nodes that process mass data.

F. Auditing Algorithm

Security monitoring on the cloud is important, because computers sharing data are most readily available to an attacker. Without mechanisms in place to detect attacks as they occur, a system not realizes its security. Therefore it is vitally important that computers residing in the cloud are carefully monitored for a wide range of audit events. The auditing in a system consists of three steps. The first step is the attack has

DOI : 10.18231/2454-9150.2017.0065

attempted on any node in system, secondly the attack is detected by the system using hashing algorithm after detection of attack the notifications are send to data owner. Due to this security is improved.

V. Conclusion

This paper has presented a literature review and analysis of the different systems. It is clear that, existing security schemes there are some drawbacks. At system level in multi- streams our proposed models can optimize the resources distribution and presented schemes are effective enough to support real-time applications.

References

[1] L. Atzori and A. Iera, "The internet of things: A survey. Computer Networks", 54(15), pp. 2787-2805, 2010.

[2] H. Ning and H. Liu, "Cyber-Physical-Social Based Security Architecture for Future Internet of Things," Advanced in Internet of Things, 2(1), pp.1-7, 2012.

[3] Q. Jing, A.V. Vasilakos, J. Wan, J. Lu, and D. Qiu, "Security of the Internet of Things: perspectives and challenges," Wireless Networks, 20(8):pp.2481-2501, 2014.

[4] European Union. Privacy and Data Protection Impact Assessment Framework for RFIDApplications,2011. http://cordis.europa.eu/fp7/ict/enet/documents/rfid-pia-frameworkfinal.pdf.

[5] O. Garcia-Morchon. S. Kumar, R. Struik, S. Keoh, R. Hummen, Security Considerations in the IP-based Internet of Things. IETF Internet Draft. http://tools.ietf.org/html/draft-garcia-coresecurity- 04, 2012.

[6] T. Heer, O. Garcia-Morchon, R. Hummen, S.L. Keoh, S.S. Kumar and K. Wehrle. "Security Challenges in the IP-based Internet of Things," Wireless Personal Communications, 61(3), pp. 527-542, 2011.

[7] S. G. Lian, "Multimedia content encryption: techniques and applications," CRC Press, Boca Raton, FL, USA, 2008.

[8] F. Liu, and Koenig, "A survey of video encryption algorithms," computers & security, 29(1), 3-15, 2010.

[9] H. Cheng, X. Li. Partial encryption of compressed images and video. IEEE Transaction on Signal Processing,48(8):2439-2451; 2000.

[10] Wen J. Severa M, Zeng W, Luttrell MH,Jin W. A formatcompliant configurable encryption framework for access control of video. IEEE Transaction on Circuits and Systems for Video Technology (12)(6):545-57; June 2002.

[11] W. Zeng ,S.Lei. efficient frequency domain selective scrambling of digital video. IEEE transaction on Multimedia(5)(1):118-219;March 2002.

[12] Siu-Kei, Au Yeung, Shuyuan Zhu, Bing Zeng. Partial video encryption based on alternating transform. IEEE Signal Processing Letters(6)(10):893-896; October 2009.

[13] C. Narsimha Raju, Ganugula, Umadevi, Kannan Srinathan, C.V. Jawaha, "Fast and Secure Real-Time Video Encryption".in: Sixth Indian Conference on Computer Vision, Graphics & Image Processing, pp. 257-264, 2008.

DOI : 10.18231/2454-9150.2017.0065