International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 05 | May-2018 www.irjet.net p-ISSN: 2395-0072

Selective Encryption Control Model for Multimedia Big Data with Data Auditing Technique

Prajakta Bhamare[1], Rupali Chaudhari[2], Pratima Hurpade[3]

[1,2,3] *Student, Dept. of Computer Engineering, R.H.Sapat College of Engineering Management Studies and Research, Nasik , Maharashtra ,India*

Abstract - *Multimedia data security is important for multimedia commerce .In the present method the data is hidden behind the images, the intruders can easily acquire this information because it is not encrypted Digital video sometimes needs to be stored and processed in an encrypted format to maintain security and privacy. Previous cryptography studies have focused on text data. The encryption algorithms developed to secure text data may not be suitable to multimedia applications. we have developed a technique to hide data in Encrypted images. We have explored the limits of Stenography theory and practice and have arrived to this unique method of data hiding. The confidentiality of multimedia big data under resources constraints is investigated in this paper. 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 had applied an auditing technique to provide auditing to big files using hashing algorithm. Experimental results have demonstrated the feasibility and efficiency of the proposed scheme.*

***Key Words*: internet of things, multimedia sensing, multimedia big data, video encryption, file auditing, cloud computing.**

1. INTRODUCTION

CLOUD computing has become an important technology trend, which can provide highly efficient computation and large-scale storage solution for video data. Given that cloud services may attract more attacks and are vulnerable to untrustworthy system administrators, it is desired that the video content is accessible in encrypted form. The capability of performing data hiding directly in encrypted H.264/AVC video streams would avoid the leakage of video content, which can help address the security and privacy concerns with cloud computing. Multimedia big data generated by IoT system have some special characteristics, such like high volume, real-time, dynamicity, heterogeneity. In addition, other characteristics like individual privacy should also be considered in the big data age. 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, as for large-scale multimedia collaborative work, video conference, intelligent video surveillance system and other multi-stream multimedia sensing system, which are important categories of IoT applications, security of the hundreds of streams with high data volume becomes a new challenge. 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]

The goal of advanced *encryption* is covert communication. This approach of information hiding has recently became important. This project has following objectives: 1. To produce security tool based on *encryption* techniques. 2. To explore techniques of hiding data using encryption module of this project 3. To extract techniques of getting secret data using decryption module [18].

In recent years, video encryption schemes for massive multimedia data have been researched. Those schemes always focus on the real-time characteristic, while the cost of energy and other resources is generally disregarded. The selection of an appropriate algorithm should depend on the particular application requirements. But existing experimental research on data confidentiality under limited resources is relatively quite rare. Auditing module keep a watch on attack. It tries to check the originality of file on cloud by using hashing technique.

2. RELATED WORK

Multimedia collaborative work, video conference, intelligent video surveillance system and other multi-stream multimedia sensing system, which are important categories of IoT applications, security of the hundreds of streams with high data volume becomes a new challenge. 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. Video encryption often requires that the scheme be time efficient to meet the requirement of real time and format compliance. It is not practical to encrypt the whole compressed video bitstream like what the traditional ciphers do because of the following

two constraints, i.e., format compliance and computational cost. Alternatively, only a fraction of video data is encrypted to improve the efficiency while still achieving adequate security. The key issue is then how to select the sensitive data to encrypt. It is reasonable to encrypt both spatial information (IPM and residual data) and motion information (MVD) during H.264/AVC encoding.

3. LITERATURE SURVEY

As for multimedia collaborative work, video conference, intelligent video surveillance system and other multi-stream multimedia sensing system, which are important categories of IoT applications, security of the hundreds of streams with high data volume becomes a new challenge. 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. Because of the special characteristics of unplugged devices in IoT, data processing with limited resources has attracted researchers' attention, and there are some researches on it [1][5]. In the meantime, the impact of limited resources on IoT security has also been considered by scholars.

Sr. No.	Author	Demerits
1.	J. Gray and D. Patterson Explain Moore's law.[10]	Ability of Encryption are correlated Growth of CPU speed.
2.	S.G. Lian,"Multimedia content encryptions".[8]	Video encryption schemes for multimedia data focus on the real-time characteristics and cost of energy, resources are dsregarded.
3.	C.Xiao, S. Ma, K. Xu and L. Wang.[9]	There is no scheme that could t for all applications.
4.	L. Atzori and A. lera[2]	Growth of data volume and the rapid adoption technology includes security problems.

Table -1: Literature Survey table

4. PROPOSED SYSTEM

In this proposed system we had approached an optimization model for data encryption under resources constraints is proposed. Secondly, a general-purpose lightweight speed adjustable video encryption scheme is proposed, which can 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.

4.1Multimedia File Upload:

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

4.2SOAP Protocol:

"Simple Object Access Protocol" [6] is a protocol specification for exchanging structured data in the implementation of web services in computer networks. This SOAP protocol is used for interfacing with Cloud Service Provider (CSP).

4.3 FRAMES SEGMENTATION

H.264 video process consists of several different types of frames, such as (I-P-B), and can be used for Encryption to get the required efficiency below illustrate the theoretical formula for each quality of frames. If image is been uploaded there is no need of segmentation.

(I-intra frame) Is an autonomous framework which can encrypt and decrypt independently without need for another picture as a source of information retrieval, the first image of the video is for this type of frame, and the (I-frame) is the starting point for the video display as well as his importance in information retrieval synchronization if any damage in transport stream bit (bit stream), the flaw in this window that consumes the largest possible number of bits for encryption because it takes the window image full but on the other hand, the error rate is low.

(P-Inter Frame) Predictive Inter Frame: is derived from the current frame to the video sequence frame by reducing the time between frames increase unlike previous quality work only within the space of pixels, the principle of its work essentially compare the block of the current window with the block of the previous frame and the centre of block is search for match, this called (matching block), all theories have one and is the best possible match and this is called motion estimation (ME), after finding the best match, we put the block of the original block and the remaining known as compensation (motion compensation),B-frames (Bi-predictive inter frame), this type of frame be intermediate between (I, and B frames) used at high levels for perfect efficiency but complex where the highest of qualities as follows based on the comparison between more than one source for block.

4.4Optimizing 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).

4.5 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 it 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. Some Parameters of the system are defined as follows.

Parameters of nodes in system

Let d, c, b, v, e, x, and x, be n_t dimension vectors.

Data streams can be quantified as vector d= ($d1 \ldots dn_t$), which denotes the n_t different data streams in time t.

Stream copies can be quantified as vector c = ($c1 \ldots cn_t$), and ci is the number of copies of data streams di, namely there are ci clients display di.

Algorithm of embedding text inside image

Input: Cover Image, Text Data, Password;

1. Convert Image into bitmap;
2. Convert each character into ASCII code;
3. Encrypt text data using CryptoClass;
4. Put a marker in cover image which consist of information length;
5. Convert BMP into selected image format;

Output: Embedded image

Safe Algorithm:

Procedure Packet-Oriented SAFE Scheme

Procedure SAFE

1.Divide plaintext into blocks with length of BlcLength

Repeat

2.Use FE to encrypt the first block in the buffer.

3.Fori=1 to l do

let next l blocks ciphertext

cipherBlcj=blcj-1 Blcj.

until get last block.

4.For the last block ,

encrypt it using FE.

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, an system my not realize 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 attempted on any node in system , secondly the attack is detected by the system by hashing algorithm after detection of attack the notifications are send to data owner. Due to this security is improved.

1. Start
2. Read user data owner id (udoid)
3. If (doid ≠ udoid)
4. Stop
5. Else Read file name from TPA xml
6. Retrieve No. of blokes for Auditing
7. Select the block number that user want to verify.
8. Get the auxiliary information for block from TPA xml
9. Based on Auxiliary information generate new root for Auditing
10. If (new root ≠ root) file modified
11. Else File not modified
12. Stop.

5. EXPERIMENTAL RESULTS

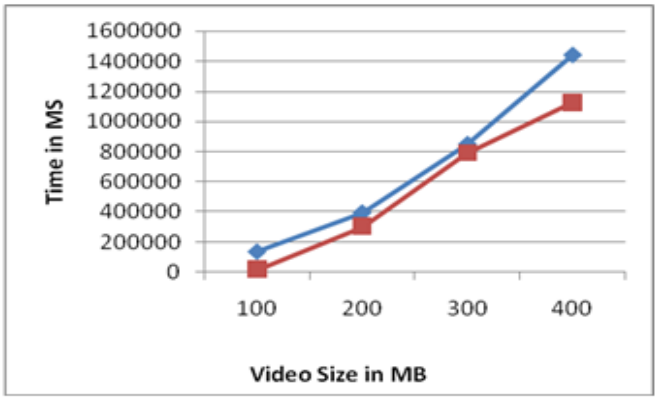

Chart-1 Encryption Time graph

	Safe 256 bits(Existing)	Safe 128 bits(Proposed)
100	136631.46	16334.78
200	396040.43	304090.2
300	850916.5	790864.1
400	1442535.04	1125125.25

The above table shows that for 100Mb file the encryption time required using Safe of 128 bits is 16334.78ms while the same size of file required to encrypt in Safe 256 bits is 136631.46ms. Similarly for 200mb file size the encryption time required using Safe of 128 bits is 304090.2ms while the same size of file required to encrypt in Safe 256 bits is 396040.43ms. For 300mb file size the encryption time required using Safe of 128 bits is 850916.5ms while the same size of file required to encrypt in Safe 256 bits is 790864.1ms. For 400 kb file size the encryption time required using Safe of 128 bits is 1125125.25ms while the same size of file required to encrypt in Safe 256 bits is 1442535.04ms.

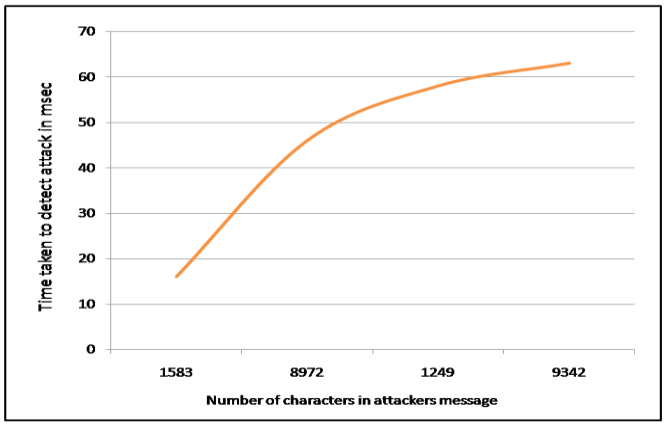

Chart -2: Attack Detection time graph

Time required for attack detection depends on the size of message to replace. As the data size i.e number of bytes increases the time required to detect also increases. The time required is calculated depending delay time to make attack and detection.

Sr. No.	Size(bytes) of data Updated	Time to detect
1.	1583	16 ms
2.	8972	46 ms
3.	1249	58 ms
4.	9342	63 ms

Table -2: Graph Table

3. CONCLUSION

The security problem of multimedia big data in multimedia sensing and other IoT systems is a new challenge since the computation and power resources are scarce. In this paper, firstly, by analyzing the resources constraints in multimedia sensing system, it is found that the problem of resources constraints will be aggravated. Then an optimization model for data encryption under resources constraints is proposed. Secondly, a general-purpose lightweight speed adjustable video encryption scheme is proposed, which can 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. We have also proposed an Signature based auditing technique for data verification on cloud side.

REFERENCES

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

[2] [2] H. Ning and H. Liu, “Cyber-Physical-Social Based Security Architecture for Future Internet of Things,” Advanced in Internet of

[3] Things, 2012, 2(1), pp.1-7 .

[4] [3] Q. Jing, A.V. Vasilakos, J. Wan, J. Lu, and D. Qiu, "Security of the Internet of Things: perspectives and challenges," Wireless Networks,

[5] 2014, 20(8):pp.2481-2501.

[6] [4] European Union. Privacy and Data Protection Impact Assessment Framework for RFID Applications, 2011. pdf.

[7] [5] O. Garcia-Morchon. S. Kumar, R. Struik, S. Keoh, R. Hummen, Security Considerations in the IP-based Internet of Things. IETF

[8] [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,”

[9] Wireless Personal Communications, 2011. 61(3), pp. 527-542.

[10] [7] S.G. Lian, “Multimedia content encryption: techniques and applications,” CRC Press, Boca Raton, FL, USA, 2008.

[11] [8] F. Liu, and Koenig, “A survey of video encryption algorithms,” computers & security, 2010, 29(1), 3-15.

[12] [9] C. Xiao, S. Ma, K. Xu and L. Wang, “A Dynamic Optimal Selective Control Mechanism for Multi-Datastream Security in Video

[13] Conference System,” IEEE ICME 2007, 2007. pp 871~874.

[14] [10] J. Gray and D. Patterson, “A conversation with Jim Gray,” ACM Queue, 2003, 1(4), pp. 53-56.

[15] [11] L. Qiao and K. Nahrstedt, “A new algorithm for MPEG video encryption,” In Proceeding of the First International Conference on

[16] Imaging Science, Systems and Technology (CISST"97). Las Vegas:Nevada, July 1997, pp. 21-29.

Data Hiding in Encrypted Images. Ankita Sawant, Vishakha Darji, Anisha Shetty.