A Selective Encryption and fraud detection on Multimedia Files for data security with Resource Optimization Technique

[1]Dheeraj Hari Patil, [2]Dr.Manmohan Singh
[1]PG Student, [2]Associate Professor,
[1]Department of Cyber Security,
[1]RKDF School of Engineering, Indore, India

Abstract*—Recently in every field there is a need of effective security of data which is also required in multimedia commerce. So, to maintain security and confidentiality digital video stored and keep processed in the encrypted form. As cryptography is a field which focused on text and numerous algorithms developed not suitable for applications of multimedia due to large data size and real time constraint. So we check confidentiality of multimedia big data under resources constraints. In first phase comparing growth trends of data volume with computational resources, and proposed encryption resource optimization technique. Then, a general-purpose lightweight speed tunable video encryption scheme is introduced. Thirdly, a series of intelligent selective encryption control models are proposed. Lastly, using hashing algorithm, we provide auditing to large files. The experimental results show and demonstrate the feasibility and efficiency of the proposed technique.

***Index Terms*—— Internet of things IoT, Multimedia Sensing, Multimedia big data, Video encryption.**

I. Introduction

The Information technology IT has been accompanied by information security problems from the time of its birth. This situation is more rigorous in network times and the IoT- Internet of Things which based on the network communication technology inherits its security problems unsurprisingly. So in the field of Internet of Things (IoT) the security issues of the big data become an innermost concern which may hamper the development of IoT technology and also it has awestruck widespread 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 represent and 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. Also, it constitutes 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 etc.

The important and distinct categories of IoT application includes large-scale multimedia collaborative work, video conference, intelligent video surveillance system and other multi-stream multimedia sensing system etc. That means, the security of these hundreds of streams with high data volume becomes a new argument. The nodes in those systems which process large amounts of media data might become the bottlenecks. In addition to mobile, unplugged sensing devices which has limited computation and energy resources restricts the protection of data security as encryption and decryption operations have the computational complexities are very high [1]. Due to this special characteristic of unplugged devices in IoT, data processing with limited resources has attracted and focuses researcher's attention [1][5]. Also, in between the periods, the IoT security with impact of limited resources has been considered by various researches. This shows that selection of a suitable algorithm should depends on the particular application requirements rather than that of existing experimental research on data confidentiality under limited resources. To check the originality of a file on a cloud, keep continuous watch on auditing module through a use of hashing procedure.

II. 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.

2.1Multimedia File Upload:

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

2.2SOAP Protocol:

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

2.3 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.

2.4 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).

2.5 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 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.

2.6 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 BlcLenght
       Repeat
    2.Use FE to encrypt the first block in the buffer.
    3.Fori=1 to l do
         let next l blocks chiphertext
         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 $\neq$ 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.

III. EXPERIMENTAL RESULTS

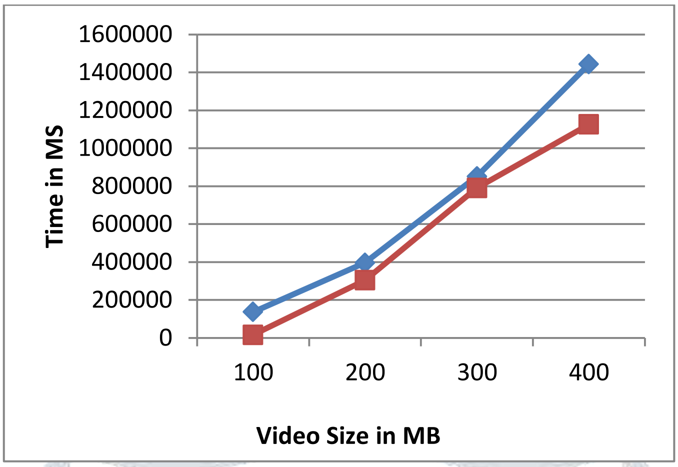

Chart-1 Encryption Time graph

Table 1

	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.

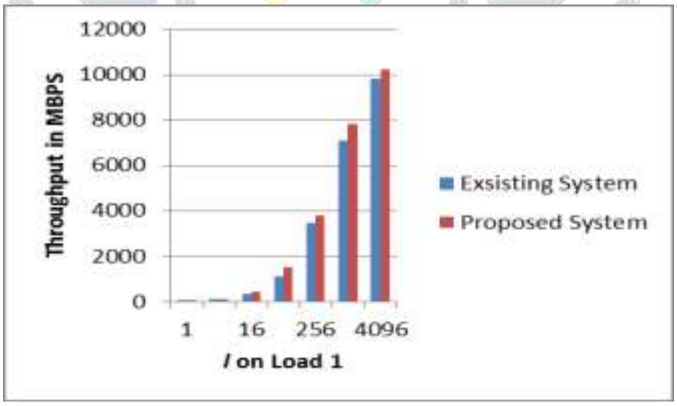

Chart-2 Throughput graph on load 1

Table 2

	Existing System	Proposed System
1	37.92	42.8
4	94.29	96.3
16	314.2	410.2
64	1114.1	1525.3
256	3489.1	3765.3
1024	7113.2	7822.3
4096	9808.3	10231.6

We had analyzed the throughputs of existing and proposed system with different values of parameter l results shown in Table 2 is the throughputs of system when the test computer has difficult loads. The result is measured in MBps. Load 1 gives result of both existing and proposed system which shows that our proposed system results is quite better than existing result.

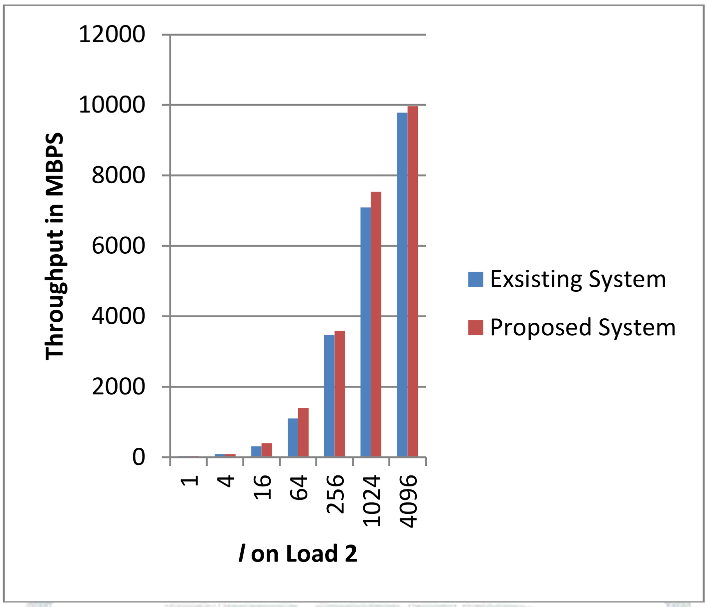

Chart-3 Throughput graph on load 2

Table 3

	Existing System	Proposed System
1	37.74	41.9
4	93.85	94.8
16	312.3	402.6
64	1106.9	1401.8
256	3475	3595.6
1024	7096	7536.2
4096	9782	9964

We had analyzed the throughputs of existing and proposed system with different values of parameter l results shown in Table 3 are the throughputs of system when the test computer has difficult loads. The result is measured in MBps. Load 1 gives result of both existing and proposed system which shows that our proposed system results is quite better than existing result.The results shows the superiority of proposed algorithm over the other algorithms in terms of the throughput of encryption and decryption (Video) process. Because more throughput and more speed.

Security Level Graph

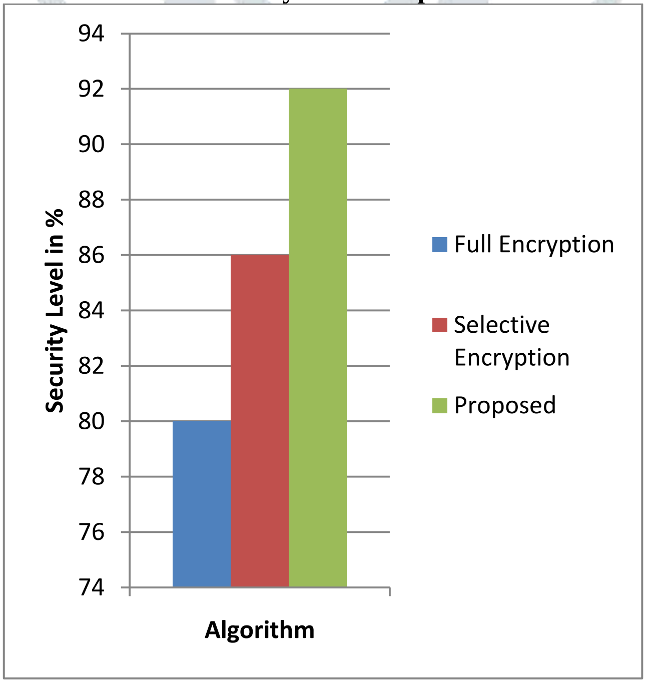

Chart-4 Security Level Graph

Table 4

Full Encryption	Selective Encryption	Proposed
80	86	92

The security of a cryptosystem should rest on the structure of the algorithm and this security is enhanced if the algorithm is held secret. As per above table we have compared our system with full encryption and selective encryption. We had seen that our system security level is high comparatively to previous system. This security is been checked on the basis of key and rounds which will led to minimize of attacks done.

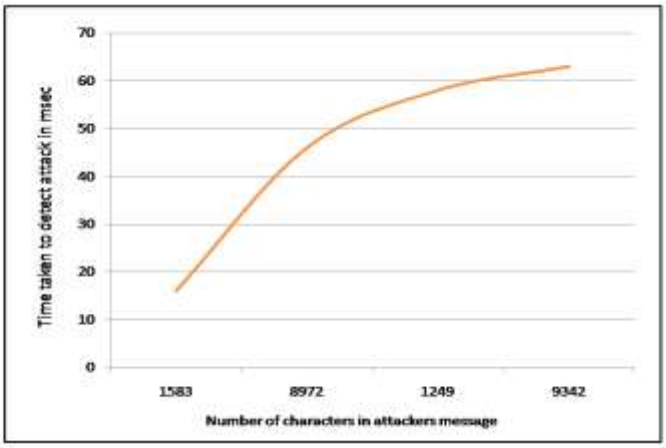

Chart -5: Attack Detection time graph

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.

Table -5: Graph Table

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

CONCLUSION

In multimedia sensing and IoT systems, the security in a multimedia big data is challenging one in terms of computation and power resources. So there is a need of to focus on confidentiality of multimedia big data under resources constraints. In first phase comparing expansion trends of data volume with computational resources, and proposed encryption resource optimization technique. Then, a general-purpose lightweight speed tunable video encryption scheme is introduced. Thirdly, a series of intelligent selective encryption control models are proposed. Lastly, using hashing algorithm, we provide auditing to large files. The experimental results show that the superiority of proposed algorithm over the other existing algorithms in terms of the throughput of encryption and decryption (Video) process as more throughput and also then more speed.

REFERENCES

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

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

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

[4] European Union. Privacy and Data Protection Impact Assessment Framework for RFID Applications, 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, 2012. http://tools.ietf.org/html/draft-garcia-coresecurity- 04.

[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, 2011. 61(3), pp. 527-542.

[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, 2010, 29(1), 3-15.

[9] C. Xiao, S. Ma, K. Xu and L. Wang, “A Dynamic Optimal Selective Control Mechanism for Multi-Datastream Security in Video Conference System,” IEEE ICME 2007, 2007. pp 871~ 874.

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

[11] L. Qiao and K. Nahrstedt, “A new algorithm for MPEG video encryption,” In Proceeding of the First International Conference on Imaging Science, Systems and Technology (CISST"97). Las Vegas:Nevada, July 1997, pp. 21-29.