Selective Encryption Control Model For Multimedia Big Data Security And File Auditing In Cloud Computing

Mr. Arshad N. Inamdar[1], Prof. M. B. Vaidya [2]
[1, 2] Dept of Computer
[1, 2] AVCOE,Sangamner

***Abstract**- Multimedia data security is important for multimedia commerce. 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 because of the large data size and real time constraint. The confidentiality of multimedia big data under resources constraints is studied 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, lightweight speed adjustable video encryption scheme is offered. Thirdly, a sequence 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 determined the feasibility and efficiency of the proposed scheme.*

Keywords- Cloud Computing, File Auditing, Internet of Things, Multimedia Sensing, Multimedia Big Data ,Video Encryption

I. INTRODUCTION

Cloud computing has become an important technology trend, which capable to provide highly effectual 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 like that the video content is accessible in encrypted form. Multimedia big data produced by Internet of Things system have certain properties, such as high volume, realtime, dynamicity, heterogeneity. And some other properties such as individual privacy should also be considered in the age of big data. Therefore, excluding the traditional security issues in distributed system, the aforementioned characteristics of the multimedia big data have brought in some new security problems like .Mainly, for large-scale multimedia collaborative work, video conference, intelligent video surveillance system and other multi-stream multimedia sensing system, this are important categories of IoT applications, security of the multi streams with high data volume becomes a new challenge. The nodes in those systems, which process large volume of multimedia data, might become the bottlenecks. furthermore mobile, unplugged sensing devices, with their limited computation and energy resources restrict the of data security, because the computational complexities of encryption and decryption operation are very high.

In recent years, video encryption schemes for big multimedia data have been researched. Those schemes always focus on the real-time properties, while the cost of energy and other resources is generally neglected. The selection of an convenient algorithm should depend on the precise application requirements. But actual 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.

II. RELATED WORK

How to obtain data confidentiality under tight resources constraints has become an important topic nowadays. In IETF’s draft of “Security Considerations in the IP-based IoT”, the “tight resources constraints” is consider to be the first challenge of IoT security. And some other researches pointed out that complex security process should not be used, and energy-efficiency schemes should be considered to achieve a balance between performance and security. Those researches also indicate that the current study on data confidentiality under tight resources constraints is relatively unsubstantial. Video encryption usually requires that the scheme is time effective to meet the requirement of real time and format compliance. It is not precise to encrypt the whole video bit stream 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 obtaining adequate security. The key issue is then how to select the sensitive data to encrypt. It is feasible to encrypt both spatial information (IPM and residual data) and motion information (MVD) during H.264/AVC encoding.

III. LITERATURE SURVEY

L. Atzori and A. Iera define recent improvements in sensor technology and network technology, specifically the wireless network technology, the IoT applications are extensively deployed [3]. Meantime, growing data volume and the rapid a

Identify the constructs of a Journal – Essentially a journal consists of five major sections. The number of pages may vary adoption technology inherits its security problems naturally. So the security issues of the big data in IoT become a fundamental concern which may hamper the development of IoT technology, and it has attracted comprehensive attentions.

T. Heer, O. Garcia present large-scale multimedia new challenges [4]. The nodes in those systems, which process large amounts of media data, might become the bottlenecks. Moreover, with limited computation and energy resources of mobile, unplugged sensing devices restrict data security .How to achieve data confidentiality under tight resources constraints has become an important topic nowadays. In IETF's draft of "Security Considerations in the IP-based IoT", the "tight resources constraints" is believed to be the first challenge of IoT security

L. Qiao and K. Nahrstedt [5] present multimedia encoding, the Huffman coding processes eliminate the redundant information from the original media data, and statistical properties of compressed multimedia stream is different from that of text data dramatically. Statistical analysis shows that coded multimedia data have high randomness at the byte level.

J. Li, X. Huang, J. Li, X present processing ability of encryption is highly correlated with the growth of the CPU speed. According to Moore's Law, the performance of computer would double every 18 months, or grows about 60 percent a year. Secondly, the disk densities increase 100 percent per year, which is faster than the increasing of CPU according to the Moore's Law. Moreover, a lot of scholars point out that the image process ability and bandwidth of core network grows even faster than disk capacity. In addition, the computation and encryption capabilities of battery-powered equipments are also constrained by battery capacity, which grows even slower and makes the resource constrained problem trickier.

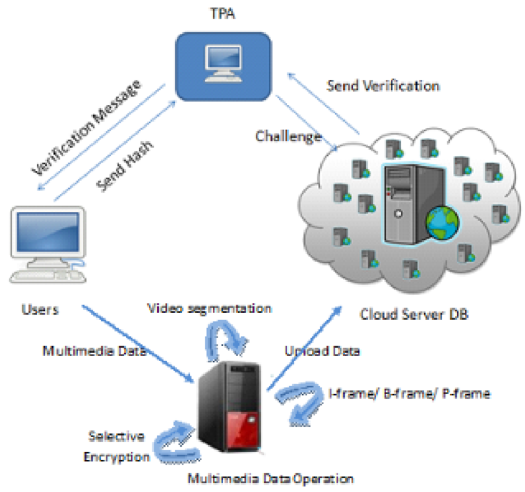
The authors of [7] define the network resource allocation problem as a cross-layer decision of transmission strategies across the APP, MAC and HY layers of a traditional network protocol stack to maximize multimedia quality with rate and delay constraints. And S.G. Lian, present modeled the communication network as a generalized utility maximization problem to provide a systematic optimization method by analysis of layered decomposition, where each layer corresponds to a decomposed sub problem and the interfaces among layers are quantified as functions of the optimization variables coordinating the sub problems. Those efforts are, however, mainly focused on the architectural decisions in networking, not tuning the system parameters for energy-quality-security gain.

The F. Liu, and Koenig, presented a quality-driven security design and resource allocation framework for wireless sensor networks with multimedia selective encryption and stream authentication schemes proposed at the application layer and network resource allocation schemes at low layers. In particular, an unequal (partial) error protection-based network resource allocation scheme is proposed by jointly designing selective multimedia encryption and multimedia stream authentication with communication resource allocation. Their cross layer resource management framework for secure multimedia streaming solves a global optimization problem requiring full awareness of the system dynamics while our compositional approach leads to acceptable solution quality at low complexity. Also, the composition can be fully distributed and capable of utilizing different even conflicting local objectives through the generic interface of constraint language.

IV. METHODOLOGY

Cloud computing has become popular because cloud hosted services are delivered to users in pay per- use, multi-tenancy, scalability, self-operability, ondemand and cost effective manner. All the services offered by servers to users are provided by the Cloud Service Provider (CSP) which is working same as the Internet Service Provider(ISP) in the internet computing.

The proposed cloud computing architecture for service providing consist of user or client, a third party auditor, selective encoding scheme and cloud server In the cloud computing architecture, user is the one who uses the services of cloud. It may be a mobile device or stationary device which request for services to the cloud, service provider on demand services to users and then the basis of user’s requests to third party auditor provides solution for data integrity of data due to internal and external threats. offered by the cloud server. In the cloud computing data is stored in data centers with selective encryption scheme with SAFE procedure and 3DES encryption algorithm from where data is accessed when or wherever it is required. With the data centers virtual servers are connected in which one or more virtual machines (VM) are situated for computation.

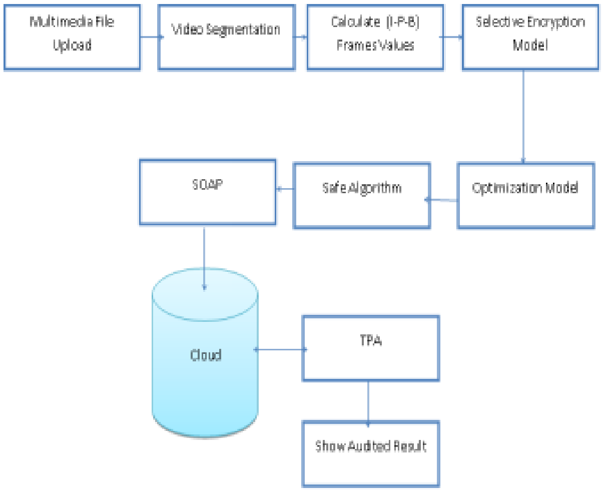


A. Multimedia File Upload:

Multimedia File Upload model will let users to upload big volume of video file which want to be uploaded on cloud server .

B. SOAP Protocol:

This SOAP protocol is used for interfacing with Cloud Service Provider (CSP). 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. cloud computing is about virtualized infrastructure, network, storage, compute, platforms, applications and SOAP is an API standard ,SOAP API to control a virtualized element, e.g. the application, which would mean that Infrastructure-as-a-service or IaaS has a SOAP interface .It relies on Comma separated values (CSV) files for its message format and usually relies on other application layer protocols.



C. VEDIO SEGMENTATION

The basic idea behind the MPEG- video compression is to remove spatial redundancy within a video frame and temporal redundancy between video frames. DCT-based compression is used to reduce spatial redundancy. Motion-compensation is used to exploit temporal redundancy. The MPEG compression scheme converts the video bit stream in terms of I (intracompressed), P (forward predicted), and B-frame (bi-directional predicted).such as (I-P-B), and can be used for Encryption to get the required efficiency, and exhibit the theoretical formula for each quality of frames.

(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: which is obtain 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.

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).

When M is a single stream, MES means a specific multimedia encryption algorithm. similarly, when Mincludes streams of a system, MES means a whole scheme include the selection of encryption algorithms and selection of streams to be encrypted. It should determine the optimum encryption algorithm for each stream in the system, and let the used encryption resources to be concentrated on the streams with higher security weightiness

E. Selective Encryption Control Model:

To construct a general selective encryption control model to encrypt multimedia data , simplified multi-stream multimedia system is considered . In this system, there are jt clients, and the total number of media streams is not in time t. Some Parameters of the system are defined as follows.

- Parameters of nodes in system

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

Data streams can be quantified as vector d=(d1…dnt),which denotes the nt different data streams in time t.

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

Stream bandwidths can be quantified as vector b =(b1…bnt). The bi denotes the bandwidth of di, and is assumed to be fixed during a session.

- Data security and decision variables

Let E be the set of candidate encryption algorithms, and Ek € E, is an algorithm in E.

Encryption schemes can be quantified as vector e =(e1…ent), while ei € E, is the selected encryption scheme
applied on data di.

Considering some encryption schemes can adjust the rate of encrypted data, and get different security levels, we defined the following parameters:

Encryption rates can be quantified as vector x =
(x1…xnt), and xi € [0,1] is the encryption rate of di.

Let SCEk(xi) € [0,1] be the function of security score ,denote the security score of data di which is encrypted by algorithm Ek with an encryption rate of xi. In additional, SC'Ek(xi), the first order derivative of function SC is positive real number.

Then Security score vector can be defined as s = (s1…snt), where si = SCei(xi), denote the security score of di.

- The weight of multimedia streams

Security weightiness vector can be defined as v = (v1…vnt), where vi denotes the security weightiness of di, and it is a positive parameter which can be predetermined or calculated according to the number of listener of data di.

- Resources constraints:

If throughput of traditional encryption on the central nodes is C is threshold value . Due to the real-time constraint, the encryption input should be less than C (even could not equal to). Otherwise, the encryption delay will increase unlimitedly according to queuing theory.

According to the ODEC model proposed appropriate encryption schemes for streams should be selected under resources constraints to maximize the security of utility value of data which have been protected. Therefore, the following expression should be satisfied.

$$\sum xi \quad * bi \leq C$$

A better scheme is to select appropriate algorithms with different security levels and different complexities or with tunable security level(e.g. SAFE). Then the streams should been divided into several groups with different levels of value-weight ratios. At last different algorithms would be used to encrypt different groups. However, this scheme is too complex to be calculated automatically.

A compromised scheme is building a layered model with few algorithms and groups. In this subsection two layered scheme is proposed., in which three candidate algorithms could be used. The first one is full encryption En; the second one is ESAFE; the and third one is unencrypted or some very low encryption rate algorithm (EVLERA), like simple permutation in packet header, whose encryption rate can be ignored.

Let CSAFE and CEn be the throughput of En, and ESAFE in the central unit. When $\sum Wi > CSAFE$ streams with higher value-weight ratio are selected and encrypted by SAFE, and let the other streams encrypted by VLERA. Correspondingly, when $\sum Wi \leq CSAFE$ full encryption and SAFE are used, all the data should protected by ESAFE firstly. Then the rest resources should be allocated to selected important data by replace ESAFE with traditional encryption algorithm En.

Safe Procedure:

Huffman coding and other coding processes remove the redundant information from the original media data for Multimedia data encoding, statistical characteristic of compressed multimedia stream is different from that of text data. Statistical analysis shows that coded multimedia data have high level randomness at the byte level Based on this statistical analysis of media data, a traditional full encryption FE is used to encrypt a block of data, and a prior block of plaintext is used as a stream cipher key to protect the following l blocks. By altering the parameter l, the speed of the encryption scheme can be controlled.

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. For i=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.
```

Moreover, data in practical system is packed by given the RTP protocol, so it needs to be encrypted by RTP packet.

The statistical characteristic of encoded multimedia stream makes analytical attacks difficult to be effective. Thus, if attackers cannot decipher the traditional full encryption scheme FE used in the improved scheme.

they cannot get any information of video. Our scheme takes small resources and could acquire a higher security assurance.

F. The Third Party Auditor :

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.

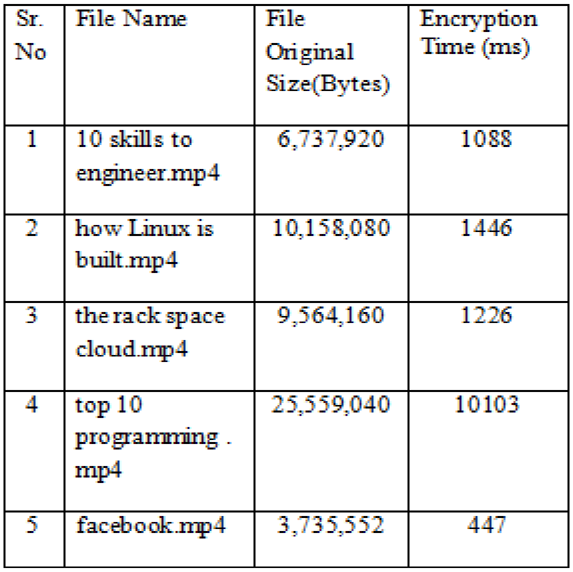
Auditing Algorithm:

```
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.
```

V. EXPERIMENTAL RESULTS

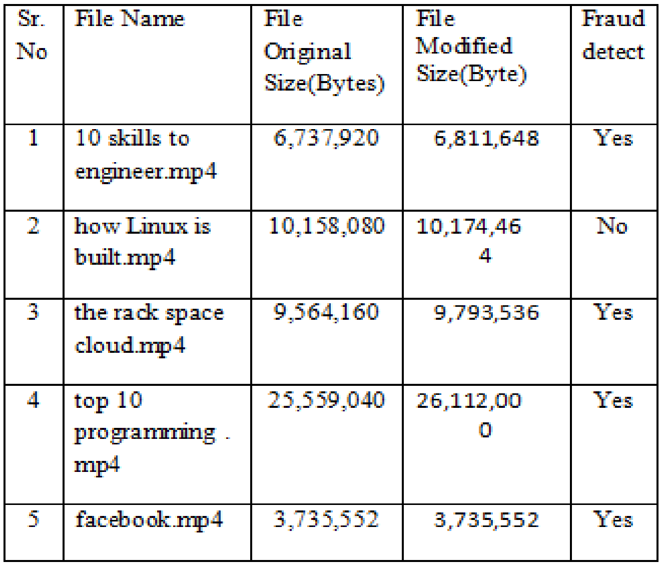
Our proposed system solves the problem of security of data while uploading implementing a secure and efficient access control mechanism across cloud platform with N users. For performance measure we compare the computational over head that is incorporated in implementing of intelligent selective encryption control models and auditing technique Mechanism. Computational overhead is involved in process of selective encryption control model with SAFE algorithm which is measured in terms of time cost required to generate N tags for Data D uploaded by N users. As data length increases the number of blocks increases which incurs more tags to be created thus increasing the time required for generating tags.

The proposed system is implemented in Java. And front end,JFrame has used. Coding of application is done with JDK1.7.Here MS-ACESS database is used to auditing the data and this can store on One Drive Cloud service provider. NetBeans IDE 7.2.1 is used as IDE with INTEL 2.8 GHz i3 processor and 4 GB RAM.



Sr. No	File Name	File Original Size(Bytes)	Encryption Time (ms)
1	10 skills to engineer.mp4	6,737,920	1088
2	how Linux is built.mp4	10,158,080	1446
3	the rack space cloud.mp4	9,564,160	1226
4	top 10 programming . mp4	25,559,040	10103
5	facebook.mp4	3,735,552	447

The above table shows the safe algorithms performance for user Multimedia data conversion as well encryption Time. Time required for attack detection depends on the size of message to replace. As the data size i.e number of bytes are change . we take a sample of File and Alter or Modify them as following table. Which Show Original Size And Size after Data Alteration with respect to this our Auditing Scheme Capable to detect Altered Data In Cloud file.



Sr. No	File Name	File Original Size(Bytes)	File Modified Size(Byte)	Fraud detect
1	10 skills to engineer.mp4	6,737,920	6,811,648	Yes
2	how Linux is built.mp4	10,158,080	10,174,46 4	No
3	the rack space cloud.mp4	9,564,160	9,793,536	Yes
4	top 10 programming . mp4	25,559,040	26,112,00 0	Yes
5	facebook.mp4	3,735,552	3,735,552	Yes

VI. CONCLUSIONS

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.

VII. ACKNOWLEDGEMENT

I express my sincere thanks to my project guide Prof. M. B. Vaidya who always being with presence & constant, constructive criticism to made this paper. I would also like to thank all the staff of Computer Department for their valuable guidance, suggestion and support through the paper work, who has given co-operation for the project with personal attention. Above all I express our deepest gratitude to all of them for their kind-hearted support which helped us a lot during paper work. At the last I thankful to my friends, colleagues for the inspirational help provided to me through a paper work..

REFERENCES

[1] Chen Xiao and Lifeng Wang “A Multi-level Selective Encryption Control Model for Multimedi Big data Security in Sencing System with Resourse Constaint”.2016 IEEE Conference on Cyber Security and Cloud Computing, pp148-153.

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

[3] 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 .

[4] 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.

[5] 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.

[6] 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- .

[7] 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.

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

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

[10] 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.

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

[12] 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.

[13] S. Martello and P. Toth, "Algorithms for Knapsack Problems," Annals of Discrete Mathematics, NorthHolland, 1987.