# Survey on Security and Privacy Mechanisms of Multimedia Big Data

**M. Priyanka[1] A. Bhagyalakshmi[2]**
[1,2]Department of Computer Science & Engineering
[1,2]Velammal Engineering College, India

*Abstract*— In the recent years, the very hot topic in the research environment is Big Data. The huge amount of data processing and storage also increases the chances of breaching the privacy of an individual's and the security challenges in the data storage. As multiple system are involved, the risk of violation of security and privacy is also increased. The goal of this paper is to provide a theoretical overview of security and privacy violations and its prevention mechanisms. The major part of a Big Data is the multimedia context. The complete security to the data and privacy of a user using the data is still an open question in the research industry. This paper analyses and compares the different security and privacy mechanism for storing and processing the data.

***Keywords:*** BigData, Security, Encryption, Privacy

## I. INTRODUCTION

Nowadays, multimedia is considered as a biggest big data as it reduces the traffic in the internet and mobile phones. Multimedia big data generated by several systems have some special characteristics, like high volume, real time, dynamicity, heterogeneity. The main characteristics of multimedia big data are human centricity, multimodality and un-precedented volume. Multimedia Data such as text, video, audio, animation sequences, graphical objects etc., are the unique type of data in the big data era. Meanwhile, big data could be in any form, structured, semi-structured or unstructured[1]. So the performance of data storage and processing task becomes more challenging. Therefore, we need to store the analyses data and to store in the real time situation.

Multimedia data consists of more data types. For example, Ten people in the social forum would like to like or share the video instead of the information in the text. As multimedia data attracts everyone in the world, the protection of those data is still facing a critical problem. It has higher level of complexity than text bases, for example, the composition of different sets of video data such as camera video, interactive video, social video etc. The multimedia data in the big data environment must undergoes the different life cycles such as Acquisition, Compression, Storage, Processing, Security, Computing and Understanding. Acquiring multimedia data from different heterogeneous resources including portable mobile devices Such as smart phone, digital camera and digital devices, the IOT, multimedia sensors, Social media.

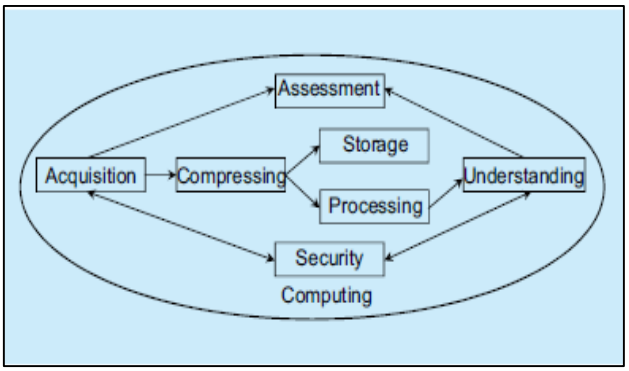


Fig. 1: Comprises of the security formats.

This paper covers the security and privacy mechanisms that are carried out for multimedia big data. The encryption mechanism and selective privacy mechanisms, features and its limitations are discussed in detail. The security and privacy are two different terms but both are mostly needed to protect the big data environment. This various aspects of security included are: Management in Security and Privacy of multimedia data in the multimedia big data. Cryptography, Authentication ,Authorization and usage control of multimedia big data are discussed[1].

## II. PROBLEM OVERVIEW

Multimedia data including text, image, audio, and video which creates a large amount of Internet and mobile communication traffic. consider a Facebook generates about 500 Tbytes of social data each day, Walmart processes millions of customers' transaction information per hour, and airplanes each generate several hundred Tbytes of flight data perFlight. These forms produces a numerous amount of data which are stored using a warehouse. The security to these data is a crucial part in processing and storage. Since data is very large, the security mechanism which is involved will take a large amount of time to process. So, the articles which are discussed in this paper provide a security and privacy to the data under temporal and spatial constraints.

In addition the technical challenges, big data provides a way for big data applications. There are many obstacles in the development of big data applications. Due to its unprecedented volume and is stored in a distributional manner, security is a long term problem that still remains open. For multimedia big data, we should consider that different users or analyzers should have different access rights, which is provided by different data owners.

Meanwhile, we should also restrict the sources without access to the entire data. The new method should avoid the violation of privacy concerns. Due to its large scale and high diversity, a multimedia big data safety mechanism should be designed, which includes effective cryptography approaches, access control, safety management, and safety communication. In this paper, the various encryption mechanisms, Protocols and Security Models are discussed in

 

order to overcome the security and privacy issues in the multimedia big data providing effective processing and storage.

## III. CONTRIBUTIONS

In the article [1], the author has proposed a different medium for encrypting a multimedia big data while transmission. He actually compares the existing encryption mechanisms and overcomes the issues in those algorithm. The limitations of existing algorithm starts from the hash algorithm in which, it cannot deal with the huge multimedia data from the IoT model since it uses the combination of encryption and hash algorithm. Using Elliptic curve cryptography is basically complex in nature. He has proposed a system which uses the Feistel Encryption Scheme, Advanced Encryption Standard and Genetic Algorithms. It produces high throughput using a GPU processing, completes in a lowest running time and produces high avalanche effect. It deals with the limitations and constraints in the encryption of transmitted data in the IoT.

In the article [2], the author has proposed a new method to encrypt the images by adding little features to the traditional watermarking approach. The image pixels are transformed into the unsequence or unordered matrix forms which acts as a encryption to an image. A combination of both image encryption and reversible watermarking technique is used. It uses the Digital Cosine Transform(DCT) Equation which is applied on the watermarking image to produce the image in more encrypted form. It can break the image into different frequency bands such high, low and middle. Due to this the choice of band in which the watermark is embedded becomes easier. This technique is mainly used to encrypt the images which are stored in a big data environments.

In the paper [3], the author has proposed a security framework for the videos which are stored in the cloud environment. He has referenced a video of a surveillance system which is basically a live video streaming, having a unprecedented and various forms of data. So the proposed framework supports the set of camera sensors which are divided into groups. Groups are then connected by Mobile Edge Computing server that is coordinating with the base stations where the group of cameras are connected to. These set of groups are connected to the cloud through the internet.

`The algorithms which are used to provide the security to a data are AES which is a symmetric data encryption algorithm for the end to end video streaming. To distribute the AES keys, RSA technique is used. To indicate there is no tampering in between the information transformation Hash Based Message Authentication is used. The protocol called "SRTP" i.e. Secure Real Time Protocol acts as a security framework that provides a mutual authentication, session key management and confidentiality and integrity of a data.

In the article [4], The author has done a survey on multimedia big data where he focuses mainly on how the multimedia data is computed and stored in the cloud or any distributed environment and how the data is acquired from the different heterogeneous sources. Different computation techniques, storage mechanisms and the assessment of data are addressed in this paper. Multimedia assessment is done by evaluating the QoS operations. The security method followed by the big data applications are mentioned and the characteristics of a security methods are provided. The basic understanding of a multimedia big data, its challenges and security models are evaluated in this paper.

In the article [5], the author primarily focuses on privacy leakage issues in multimedia system and how to maximize the weight of a privacy under different security levels in predefine space and temporal constraints. A Selective Preserving method is proposed to allocate the encryption mechanisms based on the privacy weight and each data package execution time. And the encryption method is chosen according to the privacy level. The author has clarified the data into different groups depending on Privacy levels. For example, the high level of privacy could be given to the medical records, license plate numbers, facial information collected in monitoring or reporting videos.

Initially, the selective mechanism will categorize the data packages into multiple groups according to the privacy weight levels. Then it decides whether a package has to be encrypted or not. In order to reduce heavy loads and huge latency, the input data is split into two components and then they transmitted to the different cloud storage servers. This reduces the easy retrieval data from the cloud operators. In this case, if the data has to be retrieved from cloud servers, the encrypted data is taken from the different cloud servers and then encryption is done.

In this article [6], the main challenges in roadside accident vehicular cloud network video reporting is discussed. Privacy of a data, Security, Data management and computing efficiency of a data storage are considered as a big challenges in reporting video to the cloud server. The registered vehicles in the VCN are allowed to record a live video in case of any roadside accidents and it sends the video directly to the cloud using 5G services.

| Encryption Schemes | Features | Limitations |
|---|---|---|
| A Selective Privacy Preserving Approach | – It considers both resource and time delay constraints in multimedia systems<br>– It uses data-split based encryption technique to avoid malicious cloud attacks | – Increase of multimedia data size, increases the operation time for data encryption and retrieval process |
| Attribute Based Encryption | – Access control is based on user's attribute<br>– More secure and flexible as granular access control is possible | – Updating cipher text receiver is not possible<br>– Data to be processed must be downloaded and encrypted |

 

| | | |
|---|---|---|
| Identity Based Encryption | – Access control is based on the identity of a user<br>– Complete access over all resources | – Time consuming in large environment<br>– Data to be processed must be downloaded and encrypted |
| Dynamic Data Encryption Strategy(D2ES) | – classifying data packages according to privacy level | – it gets hard to recover your own data due to overprotective data access mechanisms |

Table 1: Comparison of Security and Privacy Mechanisms

The destination is the official authorities via the cloud storage. The key issues in the processes are usage of conventional public key, the expensive operations and usage of an Attribute Based Encryption in which the participating vehicle sends the video, where it should know the receiver's public key to achieve the access control.

The lightweight and secure protocols are enhanced for cloud assisted reporting services in 5G enabled Vehicular Networks. The proposed system works on the three way handshake approach which is used to verify the data that has been received successfully and it also checks and secure the data between two computer in the communication.

In the paper [7], the author specifies the key issue ae execution time of encrypting data during the data processing and transmissions. The privacy issue is considered and proposed a novel data encryption scheme called Dynamic Data Encryption Strategy D2ES. Under the time constraints, the data is encrypted selectively using a selective encryption strategy. It follow the two major techniques, the data packages are classified based on the privacy level and determines whether the data package can be encrypted or not based on the time constraints. This method is used in a distributed cloud computing storages. It is designed to dynamically select the data packages that are encrypted under certain condition, considering both the time constraints and facilities capacities.

Selective Encryption method for big data stream which is furnished with key renewability and makes tradeoff among security performance and resource utilization. The salient features of selective encryption method is described in [9] as, it has efficient key broadcasting without retransmission, ability to recover lost keys with a proper detection, seamless key refreshment without interrupting the data streams, maintain the data confidentiality based on the data sensitivity level.

In many cloud application made the critical issues in data security and privacy and, [10] proposes an intelligent cryptography approach, using which the cloud service operators cannot directly reach partial data. This approach divides the file and separately stores the data in the distributed cloud servers. It is entitled Security-Aware Efficient Distributed Storage(SA-EDS) model, which includes Alternative Data Distribution Algorithm.

In this approach, it mainly splits the sensitive data and store it in a separate cloud servers and merges operations have been done during data retrieval.

## IV. Conclusion

The amount of data increasing day by day and it is impossible to imagine the next generation without the execution of data driven algorithms. In this paper, we have conducted a survey on the security and privacy mechanisms while dealing with the multimedia big data. And we have discussed the some advantages and disadvantages of encryption techniques which are used to protect the data storage and data transmission. A lot of works have been made to protect data and the privacy of users from data generation to data processing, but still there exist several open issues and challenges.

## References

[1] Zaijian Wang1,*, Shiwen Mao2, Lingyun Yang1, Pingping Tang1, "A Survey of Multimedia Big Data", 4th June 2017Auburn, AL 36849-5201 USA.

[2] ShadiAljawarneh. Muneer BAniYAssein .We'am Adel Talfha, "A Resource Efficient Encryption Algorithm for Multimedia Big Data", DOI 10.007/s 11042-016-4333-y published on December 2016.

[3] AkshayPushpad,Anjali Ashish Potnis, "Improved Image Security Scheme using Combination of Image Encryption and Reversible Watermarking" 2017 4th International Conference on SPIN.

[4] Abid Mehmood, IynkaranNatgunanathan, Yong Xiang, Guang Hua, Song Guo "Protection of Big Data Privacy" IEEE, 9th May 2016.

[5] Mr.Arshad Inamdar, Prof.Vaidya M.B., "Selective Encryption Control Model for Multimedia Big Data with Resource Constraints",Vol-3, Issue-2 2017.

[6] Huining Li and Kun Wang, Xiulong Liu, Yanfei Sun, Song Guo, " A Selective Privacy Preserving Approach for Multimedia Big Data", 1070-986X/17/$33.00 ©2017 IEEE.

[7] Zahrah A. Almusaylim1, Noor Zaman2 and Low Tang Jung3, " Proposing A Data Privacy Aware Protocol for Roadside Accident Video Reporting Service Using 5G in Vehicular Cloud Networks Environment", 2018 4th International Conference on ICCOINS.

[8] Keke Gai1, Meikang Qiu2∗, Hui Zhao3, Jian Xiong4, "Privacy-Aware Adaptive Data Encryption Strategy of Big Data in Cloud Computing", 978-1-5090-0946-6/16 $31.00 © 2016 IEEE.

[9] Deepak Puthal, Xindong Wu, Surya Nepal,Rajiv Ranjan, Jinjun Chen, "SEN: A selective Encryption Method to Ensure Confidentiality for Big Sensing Data Streams", DOI 10.1109/TBDATA.2017,IEEE.

[10] Yibin Li, Keke Gai, LongfeiQiu, MeikangQiu, Hui Zhao, "Intelligent cryptography approach for secured distributed data storage in cloud computing", Information Sciences 387(2017) 103-115.

 