RESEARCH ARTICLE OPEN ACCESS

Analysis of Homomorphic Technique and Secure Hash Technique for Multimedia Content System

Jyoti .V. Ighare
ME (CSE) Student CSE Department, P.E.S college of Engineering Aurangabad India, Maharashtra

I. INTRODUCTION

To modernize the content management system, security of multimedia documents and applications are an active research area. While one motivation for this is to reduce operational costs of the organization by eliminating the data centers managed by the centers. It is defined in our paper to store and dispense data quickly to the user for long term data as digitized measurements of a multimedia vitals over the course of his/her requirements that is longer than what can be obtained within the organization in paper format.

The system can be used to protect various multimedia content types, including regular 2-D videos, new 3-D videos, images, audio clips, songs, and music clips. The system can run on private clouds. The design is cost effective since it uses the computing resources on demand. The design can be scaled up and down to support varying amounts of multimedia content being protected.

To turn this vision into reality, the privacy and security of the data is at the topmost priority. In phase-I acquisition, data are acquired and given to the system as input. In phase-II the storage, where the data is stored permanently for future use, is deployed. In third phase computation, where the data is processed, is taken care. While existing FHE-based encryption techniques can ensure data privacy in phases-I and phase-II, achieving computation requires operating on encrypted data.

Here a feasibility study was conduct for achieving phase-III by using the emerging Fully Homomorphic Encryption (FHE) techniques on a restricted set of multimedia documents. It was focused on the case, where there has no resources allocated to the storage or computation, which strictly act as the graphical user interface (GUI) devices. Proposed system is where input data is Homomorphic Encrypted and stored. Without loss of generality, it is specifically focused on multimedia documents security for the used applications and the resulting secured data storage and retrieval. The goal of the system is to push the entire workload in FHE form on storage. To best knowledge, this is the first kind of techniques that focuses on the application of Fully Homomorphic Encryption to multimedia documents.

This deployment model was used to show the flexibility of our system, which enables it to efficiently utilize varying computing resources and minimize the cost, since cloud providers offer unlike pricing models for computing and network resources. Through extensive experiments with real deployment, we show the high accuracy (in terms of precision and recall) as well as the scalability and elasticity of the proposed system.

The rest of this paper is organized as follows. We summarize the related works in Section II. In Section III, we present the design goals and a high-level description of the proposed system. In Section IV, we present the analysis of the proposed method. We conclude in Section V.

II. LITERATURE REVIEW

Cloud computing is a new computing model that will interconnect the large-scale computing resources to effectively integrate, and to computing resources as a service to users. Users can use the broad band network at any time on demand access to virtual computers and storage systems, without the need to consider the complexities of the implementation and management, greatly reducing the difficulty and hardware to achieve the user's investment.

Cloud computing effectively the actual separation of physical and virtual services, a variety of business services reduced costs, improved utilization of network resources. With cloud computing applications and research at home and abroad continue to advance the development of cloud computing faces many critical issues, and bear the brunt of security issues and, with the growing popularity of cloud computing, security issues, showing the importance of a gradual upward trend, has restricted its important factor in development.

Recently, Amazon, Google and other cloud computing sponsors a variety of security incidents continue to burst exacerbated people's fears. For example, in March 2009, Google place a large list of user files leak, in February 2009 and July, Amazon's "Simple Storage Service i.e. simple storage service, called S3)" depends on two break lead to a single storage network Service's website was forced to a standstill, etc. Thus, to make businesses and organizations with large-scale application of cloud computing platform, safely delivered to their own data management in the cloud service provider, we must fully analyze and address the cloud computing security issues facing.

Ovunc Kocabas et. al. [1] proposed system where phase I (Acquisition) of the long-term health monitoring is achieved via the purpose of remote sensors that are capable of regular FHE encryption and transmission to the cloud via existing wireless access points. They formulate Full Homomorphic Encryption (FHE) as the core of this idea. They identified the challenges in making this possible for a specific application based on remote-ECG monitoring. They determined what is possible within the following few years while FHE acceleration is being widely researched. Jiadi Yu et. al. [2] proposed the concepts of similarity relevance and scheme robustness. We, thus, perform the first attempt to develop the privacy issue in searchable encryption, and we show server-side ranking based on order-preserving encryption (OPE) inevitably violates data privacy. Mohd Rizuan Baharon et. al. [3] in their work proposed a new FHE scheme based on a finite field that supports *n*-multilinear maps. The scheme is constructed based on an open problem raised by Boneh et al. in their scheme that supports a bilinear map. Scott et. al. [4] took advantage of both homomorphic encryption and searchable encryption. On one hand, the homomorphic property is exploited in order to preserve users' privacy, as the cloud (or the sink in adhoc / sensor networks) handles only encrypted data. The cloud only provides operation as well as storage services and it has no knowledge about what kind of information is being processed. Therefore, users' privacy is preserved this way. On the other hand, due to the large amount of data, efficient retrieval of users' data is supported through the use of searchable encryption. Moreover, the support for searchable encryption cannot compromise users' privacy. Qingjie Meng et. al. [5] discussed in their study Cloud computing leads the development of industry informatization and society informatization, along with the popularity of Internet of things and mobile internet, the permeation of cloud computing in various industries was becoming increasingly apparent. But cloud computing security issue has become a bottleneck restricting its application, mainly related to information security and privacy protection issues, which involves encryption, information isolation, authentication, key management and access control and other issues, it is the current cloud computing security research hotspot also. Y Govinda Ramaiah, et. al. [7, 8] gives Fully Homomorphic Encryption (FHE), which allows processing the data in encrypted form. Whereas FHE is yet to be practical, several theoretical results have been proposed for various cloud security problems based on it. Also, research is actively going on in developing the cryptographic trust mechanisms such as verifying the computation performed over the cloud resident data called. Ankita Lathey et. al. [6] proposed a novel and efficient SSS based method to perform the arithmetic division operation for non-terminating quotients (involved in LPF for image enhancement by smoothing and removing noise) over cloud in ED. This allows an authorized user to reconstruct the improved quality images from the *CDC*s. They developed scheme that uses a (*T*, *N*)-SSS scheme to divide the original (noisy) images (called 'secret') into *N* modified images (called 'shares'). The *N* shares are stored at *N* different *CDC*s. In order to view the original image, an authorized user first obtains the share images from any (T ≤ N) CDCs and then reconstructs an improved quality LPF image. NIU Yukun et. al. [9] introduced a new data checking way which is based on additive homomorphic encryption and the characteristic of SM data. Obviously, user's consumption data is the difference of SM reading value in different time, that is to say, SM reading in the current time is the sum of consumption data and SM reading in the last time. Using additive homomorphic encryption, they made the equation still valid. In this way, we can find whether the data is tampered because the equation will not be valid if it is tempered by adversary. An-Ping Xiong et. al. [10] proposes CP-ABE (Cipher-text-Policy Attribute-Based Encryption) that owners which encryptors can define their own data access policies by themselves, that more suitable for the implementation of access control to shared data in the cloud storage environment. At present, a large number of research on the CP-ABE access control, and these scheme give more consideration to the flexibility of the attribute-based access control, or focus on fine-grained access control of encrypted data, and they less consider the result of cipher-text redundancy, or the keys update frequently.

The prominent technology is emerged by the multimedia computing to generate, edit, process, and search media contents, such as images, video, audio, graphics. The internet and mobile wireless networks over for the multimedia requisition and services, cloud computing for this strong requirement is available because serving millions of internet or mobile users is required expressive amount of computation at the same time [11]. Great challenges is imposes in a cloud of the multimedia processing. The multimedia computing of the cloud has several fundamental investigation is highlighted as follows [12].

III. DETAILS OF WORK

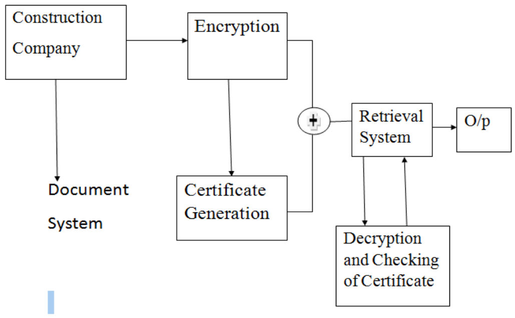


Figure 1: Block diagram for proposed system

The block diagram shows multimedia content protection system in Fig. 1. The block diagram has multiple blocks as construction company that creates data, encryption module where FHE encryption is done on the multimedia document, Certificate generation module generate a signature components that as to be matched, retrieval system decrypts the data and outputs it for the use.

The figure shows a general case where one or more cloud providers can be used by the system. This is because some cloud providers are more useful and/or provide more cost saving for different computing and communication tasks. For example, a cloud provider offers lower cost for inbound bandwidth and storage can be used for downlink and temporarily storing videos from online sites, while another cloud provider offers better compute nodes at lower costs can be used to maintain the circulate index and to perform the copy detection process. For storing the images and other data such as audio cloud is used for it. In this cloud storage the major use is that only publically can used the data but private user can used the authenticate data. Image is stored on cloud in this framework in the encrypted form and then transform. This framework is responsible for providing the certification authority for the public key to the data holder. This design supports creating composite signatures that include of one or more of the following elements:

In this two types of techniques is implemented first is homomorphic technique second is secure hash technique. In homomorphic technique it is form of encryption that allows computations to be carried out on ciphertext, thus generating an encrypted result which when decrypted, matches the result of operations performed on the plaintext.

In secure hash technique is a family of cryptographic hash functions published by the national institute of standard and technology (NIST). SHA-256 and SHA-512 are novel hash functions computed with 32-bit and 64-bit words, respectively. They use different shift amounts and additive constants, but their structures are otherwise virtually identical, differing only in the number of rounds.

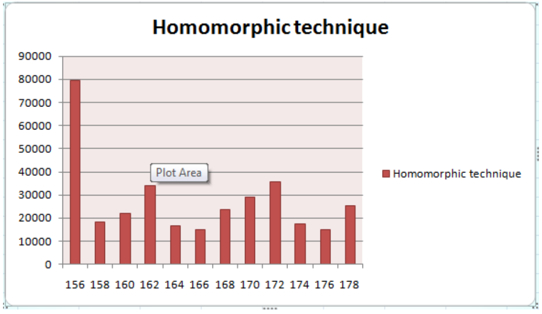
The scope of the proposed technique in this multimedia content protection system illegally made copies of the multimedia objects over the internet that illegally copies are find out. It is large scale and complex with multiple involved parties. Due to this we select some approaches and goals of this project. Accuracy, computational, efficiency, scalability, and cost efficiency all this are goals

IV. ANALYSIS

The processing speed and time complexity of the system was considered. Ticks were measured at various operations and statistical data table is generated. Table 1 show the request and response date time. Here file ID and request date time associated with the file is in column 1 & 2. In column 3 the time required to upload that particular file in the terms of Ticks is measured. Here tick is measure unit of time. Similarly in column 4 total response time of the same file and the time taken to recall the file are measured in millisecond.

Table 1: Recall Information of Homomorphic Technique

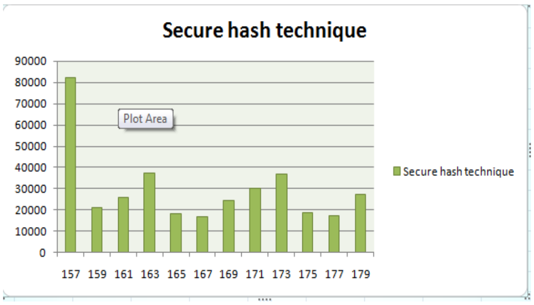
Session Id	Request Date Time	Response Date Time	Total Response Time
156	12:17:46.077	12:19:05.737	79661
158	01:04:44.570	01:05:02.977	18405
160	04:39:09.260	04:39:31.313	22053
162	06:15:39.377	06:16:13.313	33938
164	06:16:25.540	06:16:41.937	16396
166	06:16:51.150	06:17:05.960	14811
168	06:17:12.180	06:17:35.660	23480
170	06:18:38.937	06:19:08.080	29146
172	06:20:11.380	06:20:47.067	35687
174	06:21:33.577	06:21:51.150	17572
176	06:22:50.507	06:23:05.560	15052
178	06:23:57.757	06:24:22.940	25183



Graph1: Recall Information of Homomorphic technique

Table 2: Recall Information of Secure Hash Technique

Session Id	Request Date Time	Response Date Time	Total Response Time
157	12:17:46.077	12:19:08.197	82121
159	01:04:44.570	01:05:05.677	21108
161	04:39:09.260	04:39:35.200	25939
163	06:15:39.377	06:16:16.583	37205
165	06:16:25.540	06:16:43.637	18097
167	06:16:51.150	06:17:08.097	16947
169	06:17:12.180	06:17:36.523	24344
171	06:18:38.937	06:19:08.867	29929
173	06:20:11.380	06:20:48.333	36953
175	06:21:33.577	06:21:52.140	18562
177	06:22:50.507	06:23:07.827	17321
179	06:23:57.757	06:24:25.090	27332



Graph 2: Recall Information of Secure Hash Technique Graph

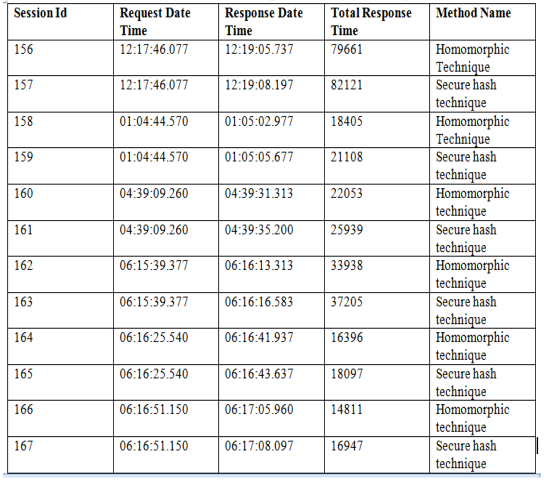
In this the total response time is calculated by difference between request time and response time is saved in ticks. The ticks are divided by 1000 so get the result in millisecond.

Ticks/1000=millisecond

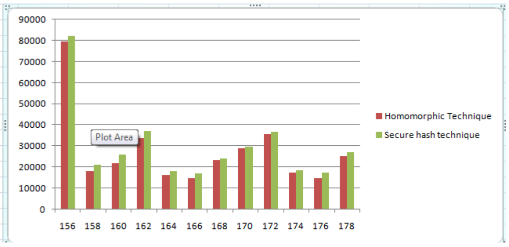
This system captures the depth signal of the 3-D video, without explicitly computing the exact depth map, which is computationally expensive. Our experiments showed that the proposed 3-D signature creates high accuracy in terms of both precision and recall and it is robust to many video transformations including new ones that are specific to 3-D videos such as synthesizing new views. Our experiments showed that it can elastically utilize varying amount of computing resources and it produces high accuracy. The experiments also showed that it outperforms the closest system in the literature in terms of accuracy and computational efficiency.

In this Homomorphic encryption technique with SHA hash technique. The secure hash algorithm is a family of cryptographic hash functions published by the national institute of standard and technology (NIST) as a U.S federal information processing standard (FIPS).

Table 3: Comparison with Secure Hash Technique with Homomorphic Technique



Session Id	Request Date Time	Response Date Time	Total Response Time	Method Name
156	12:17:46.077	12:19:05.737	79661	Homomorphic Technique
157	12:17:46.077	12:19:08.197	82121	Secure hash technique
158	01:04:44.570	01:05:02.977	18405	Homomorphic Technique
159	01:04:44.570	01:05:05.677	21108	Secure hash technique
160	04:39:09.260	04:39:31.313	22053	Homomorphic technique
161	04:39:09.260	04:39:35.200	25939	Secure hash technique
162	06:15:39.377	06:16:13.313	33938	Homomorphic technique
163	06:15:39.377	06:16:16.583	37205	Secure hash technique
164	06:16:25.540	06:16:41.937	16396	Homomorphic technique
165	06:16:25.540	06:16:43.637	18097	Secure hash technique
166	06:16:51.150	06:17:05.960	14811	Homomorphic technique
167	06:16:51.150	06:17:08.097	16947	Secure hash technique



Graph 3: Comparison total response time in milli second

In this homomorphic technique compare with secure hash technique file id there request date time and response date time and how much take time to uploading the file there total response time shown in the table. For 3-D videos homomorphic technique takes time 79661 millisecond whereas secure hash technique take time 82121 millisecond. In the graph sum of performance analysis total response time of both techniques shown in the graph. In this comparison secure hash technique take more time then homomorphic technique to uploading the files so that homomorphic technique is better than secure hash technique.

V. CONCLUSION AND FUTURE WORK

We presented in this paper a new design for multimedia content protection systems. The system supports different multimedia content types and it can be deployed on private and/or public clouds. We proposed two key components of the system. The first one is of creating a signature of 3-D videos and second key component in our system is the distributed index, which is used to match multimedia objects characterized by high dimensions.

Furthermore, the crawler component needs to be customized to find online sites that offer pirated video streams and obtain segments of these streams for checking against reference streams, for which the signatures would also require to be generated online. Another future direction for the work in this paper is to design signatures for recent and complex formats of 3-D videos such as multi-view plus depth. A multi-view plus depth video has multiple texture and depth components, which allow users to view a scene from different angles. Signatures for these videos would need to capture this complexity, while being efficient to compute, compare, and store.

REFERENCES

[1]. Ovunc Kocabas, Tolga Soyata, Jean-Philippe Couderc, Mehmet Aktas, Jean Xia, Michael Huang (2013) Assessment of Cloud-based Health Monitoring using Homomorphic Encryption, 978-1-4799-2987-0/13 2013 IEEE, pp. 443-446

[2]. Jiadi Yu, Peng Lu, Yanmin Zhu, Guangtao Xue, Minglu Li (2013), Toward Secure Multi key word Top-k Retrieval over Encrypted Cloud Data, IEEE transactions on dependable and secure computing, Vol. 10, no. 4, july/august 2013, 1545-5971/13, pp. 239-250

[3]. Mohd Rizuan Baharon, Qi Shi, David Llewellyn-Jones, Madjid Merabti (2013) Secure Rendering Process in Cloud Computing, 2013 Eleventh Annual Conference on Privacy, Security and Trust (PST), 978-1-4673-5839-2/13 2013 IEEE , pp82-87

[4]. Scott C.-H. Huang_y, Qiao-Wei Liny, Chih-Kai Changy (2013) Secure Homomorphic and Searchable Encryption in Ad Hoc Networks, 0190-3918/13 2013 IEEE DOI 10.1109/ICPP.2013.135 pp. 937-942

[5]. Qingjie MENG, Changqing (2013) GONG Research of cloud computing security in digital library, 2013 6th International Conference on Information Management, Innovation Management and Industrial Engineering, 978-1-4799-0245-3/13 2013 IEEE, pp. 41-44

[6]. Ankita Lathey, Pradeep K. Atrey, Nishant Joshi (2013), Homomorphic Low Pass Filtering on Encrypted Multimedia over Cloud, 2013 IEEE Seventh International Conference on Semantic Computing, 978-0-7695-5119-7/19 5119 IEEE DOI 10.1109/ICSC.2013.60 pp. 310-313

[7]. Y Govinda Ramaiah, G Vijaya Kumari (2013) Efficient Public key Homomorphic Encryption Over Integer Plaintexts 978-1-4673-2588-2/12 2012 IEEE pp. 123-128

[8]. Y Govinda Ramaiah, G Vijaya Kumari (2013) Complete Privacy Preserving Auditing for Data Integrity in Cloud Computing 2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications 978-0-7695-5022-0/13 2013 IEEE DOI 10.1109/TrustCom.2013.191 pp. 1559-1566

[9]. NIU Yukun, TAN Xiaobin, CHEN Shi, WANG Haifeng, YU Kai, BU Zhiyong (2013) A Security Privacy Protection Scheme for Data Collection of Smart Meters Based on Homomorphic Encryption, 978-1-4673-2232-4/13 2013 IEEE EuroCon 2013 14 July 2013 Zagreb, Croatia pp. 1401-1405

[10]. An-Ping Xiong, Qi-Xian Gan, Xin-Xin He, Quan Zhao (2013) A Searchable Encryption Of Cp-Abe Scheme In Cloud Storage, 978-1-4799-2446-2/13 2013 IEEE pp. 345-349

[11]. J.Nich and S.J.Yang, “Measuring the Multimedia Performance of Server Based Computing”

[12]. Wenwu Zhu, Chong Luo, Jianfeng Wang, and Shipeng Li, “Multimedia Cloud Computing”, 19 April 2011.