International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 – 5161

Available at http://inpressco.com/category/ijcet

Research Article

Time based integrity checking and data sharing over Cloud

Miss.Poonam M. Kamble and Prof. Mrs. J. M. Kanase

Department of Computer Engineering PES Modern college of Engineering Pune, India

Received 10 Nov 2020, Accepted 10 Dec 2020, Available online 01 Feb 2021, **Special Issue-8 (Feb 2021)**

Abstract

Cloud computing is one of evolving technology nowadays, giving versatile services. However, secure information sharing is vulnerable to cloud computing. With cloud storage services, customers can remotely keep their information to the cloud and recognize the data sharing with others. Access management is a troublesome task to share sensitive information on cloud servers. Remote data integrity auditing is proposed to guarantee the integrity of the information stored in the cloud. The cloud data might contain some sensitive information it should no longer be exposed to others when the cloud report is shared. Encrypting the entire shared file can recognize the sensitive data hiding, however, it will make this shared report not able to be utilized by others. At pick time the server not able to serve all the request at the time. In order to address this problem, we propose a remote data integrity auditing scheme and secure Data sharing with time constraints mechanism in Cloud Computing. This paper comprises the study of various encryption schemes which can be put to use for securing the patient's sensitive health information on cloud along with the implementation and performance analysis of a healthcare application which encrypts the health records of patients before outsourcing it for storage over cloud and ensures effective access control, secrecy and integrity of health information.

Keywords: *Cloud storage, Third-Party Auditor (TPA), time server, data integrity auditing, sensitive information hiding.*

Introduction

The data shared in cloud servers, usually carries customer's sensitive/private data and needs to be nicely protected. Also it is crucial to verify the integrity of information. It is a big challenge to defend the privacy of shared records in cloud, especially in cross cloud and big data environment. Where huge data consists of excessive volume, high range and excessive veracity records units with high pace processing requirement. Big data gives the superb opportunities and transformable capability for diverse areas inclusive of ecommerce, health care industry manufacturing, social network and academic services. In order to satisfy this mission, it is essential to layout an answer to provide user-described authorization length and also provide excellent grained get right of entry to control at some point of this duration. It is also important to provide the integrity through comparing both the signatures to confirm whether the data stored on cloud is tampered or not. It verifies the integrity of records on call for of the customers. Mobile healthcare is an innovative combination of mobile devices and mobile communication technologies, for it can provide necessary health information, routine care improvements, potential infectious disease prevention, health interventions, etc. It is getting more and more widely to apply the emerging cloud computing technology into the fields of mobile healthcare. By using mobile healthcare system, the electronic health record (EHR) can be transmitted over the network to the cloud service provider (CSP) for remote storage. Moreover, the healthcare providers can read it from an end device or access it remotely using a mobile device to provide real-time medical treatment.However, data security issues are the major obstacles to the application of MHSN. MHSN extends the traditional centralized healthcare system, in which the patients stay at home or in hospital environment and the professional physicians in the healthcare center take responsibility of generating medical treatment. Compared to traditional hospital-centric healthcare which not only lacks efficiency when dealing with identifying some serious diseases in early stages but also suffers from limited healthcare information, MHSN enables continuous health monitoring and timely diagnosis to the patients in the smart city. It relies on wearable devices and medical sensors to measure the patients' health conditions and sends health data to the processing unit for doctors' further diagnosis and analysis and provides easy access to a patient's historical comprehensive health information.With cloud storage services, users can remotely save their data to the cloud. Remote data integrity auditing is

proposed to guarantee the integrity of the data stored in the cloud. In a few common the sensitive data should not be uncovered to others when the cloud file is shared. Encrypting the complete shared file can realize the sensitive information hiding, however will make this shared file not able to be used by others. How to realize information sharing with sensitive information hiding in remote data integrity auditing. In order to address this problem, we endorse a remote a integrity auditing scheme that realizes information sharing with sensitive information hiding in this paper.

Literature Survey

In This paper, The identity of the signer on every block in shared knowledge is unbroken personal from public verifies, efficiency verify shared knowledge integrity while not retrieving the whole file. Additionally is ready to perform multiple auditing tasks at the same time rather than corroborative them one by one. In this scheme Ring signatures is utilized to construct homomorphic authenticators so that a public verifier is able to audit shared data integrity without retrieving the entire data, yet it cannot distinguish who is the signer on each block. But this scheme unable to handle 1. Traceability-which means the ability of the group manager to reveal the identity of the signer based on verification metadata in some special situations. 2. How to prove data freshness [1]It uses a novel methodology for making certain privacy and data freshness of shared knowledge in cloud exploitation Holomorphic authenticable ring signature (HARS) theme to preserve the user privacy and Overlay tree rule is employed for making certain that users the information with needed level of freshness. Also Third Party Auditor (TPA) audits the information keep within the cloud. He should be able to verify the trustiness of the CSP while not disclosing the identity of the users within the group. The disadvantage is malicious activities made by means of the user cannot be detected. The hassle with this system is to extend the traceability, which means only the authentic user, can monitor the identity of the signer in order to preserve the malicious pastime made via the user within the group.[2]Introduced an efficient and privacy-preserving cosine similarity (PCSC) computing protocol in reaction to the efficiency and privacy requirements of data mining in the Big data era. The proposed PCSC protocol isn't only privacy maintaining however also efficient. It is particularly appropriate for big data analytics. The gain is the computation overhead of the proposed PCSC protocol also will increase when n is large. The downside is needs to provide specific privateness for some specific big data analytics. Introducing protocol like privateness computing to provide whole and unique protection in Big Data era.[3] Propose a singular access manage model combining Roleprimarily based Access Control (RBAC) version, symmetric encryption, and cipher text attribute-based totally encryption (CP-ABE) to aid fine-grained access control for big facts outsourced in cloud storage systems. We also reveal the efficiency and overall performance of our proposed scheme through the implementation.[4] On this paradigm, key updates are frequently accurately outsourced to a few authorized party, and as a result the important thing-update burden at the patron are going to be kept minimal. The third party auditor (TPA) in many present public auditing designs, permit it play the function of legal celebration in our case, and make it in Rate of each the storage auditing and therefore the relaxed key updates for Key-exposure resistance. In this technique, TPA simplest ought to maintain an Encrypted model of the client's secret key at the same time as doing of these burdensome obligations on behalf of the client. The consumer simplest must download the encrypted mystery key from the TPA while uploading new files to cloud. Except, this layout additionally equips the consumer with functionality to further verify the validity of the encrypted mystery keys supplied by using the TPA. one hassle with this system is that the TPA have to perform the outsourcing computations for key updates under the situation that the TPA doesn't understand the important secret key of the patron.[5]

In this paper, the author describes many new challenges for data security and access control when users outsource sensitive data for sharing on cloud servers. To access the data stored in cloud, existing work usually apply cryptographic methods such as attribute-based encryption. However, in doing so, these solutions inevitably leak the attribute and identity information of the users. For the purpose of secure access control in cloud computing while keeping the user's privacy, we propose the notion of identity-based group signature and apply it to realize the anonymous authentication to the cloud servers. Furthermore, both the user grant and revocation are supported by using the group techniques. [6]In this paper the author first implement forward secure identity based ring structure by the use of HMAC algorithms. The model also comes in with the trendiest notion of forward security. The proposed model can be implemented by both, either with or without random oracles depending on the need of the system design. Also, the key can be entered manual by the receiver or queried from the system as automated. We have tried to cover and show different comparisons of different ways a system can be designed and implemented. There is always a room for improvement, so we believe more secure implementation with similar features can be done, also by giving more ease to the end user. We consider the same as open problem and motivation for future work. [7] In this paper, the author proposes a Highly Available, Scalable and Secure distributed data storage system for high performance and secure data management. Distributed and parallel data storage or file systems such as Object-based Storage Devices and flexible key distribution schemes Data at rest (static) and in transit (dynamic) are protected with different

encryption strategies for privacy and integrity. Secret sharing and replication support both security and availability. Encryption and key management are not necessary in data at rest protection. The future work includes a detailed simulation and further performance analysis. [8] In this the author proposed a security scheme for users. This scheme provides storing and sharing their intricate data in the Cloud environment. This scheme provides vital encryption and decryption technique for achieving security on cloud application. The revocation procedure is an explicit performance destroyer within the access control method in cryptography. In this scheme, the unique data is firstly separated into numerous parts. Then these parts are sent to the cloud server. Whenever a user revocation happens, the data owner desires merely to retrieve one part and re-encrypt it. This scheme is based on cryptographic storage application. Furthermore techniques are implemented to improve the security of the data. [9]In this paper, author presented a middleware solution approach to support data and network security over eHealthcare system sing medical sensor networks. It has been shown that a masquerade attack can be launched to the system and patients 'data are in danger. We proposed this middleware to counter this kind of attack where a user and all devices into the healthcare network are mutual authenticated. Finally a performance analysis has been done with regard to masquerade attack and the result reveals the efficient of the proposed solution.[10]

Proposed Methodology

In our proposed scheme, the PKG generates the personal key for consumer in line with his identification ID. The consumer can test the correctness of the obtained private key. When there may be a desire for the user to upload data to the cloud, so that it will preserve the private sensitive facts of the original report from the sanitizer, this person needs to use a blinding element to blind the information blocks corresponding to the private sensitive information of the original report. When necessary, the user can recover the original file from the blinded one by means of the usage of this blinding component. And then this consumer employs the designed signature set of rules to generate signatures for the blinded data. These signatures will be used to verify the integrity of this blinded data. In addition, the person generates a record tag, that is used to ensure the correctness of the record identifier call and some verification values. The consumer also computes a transformation fee that is used to transform signatures for sanitizer. Finally, the consumer sends the blinded report, its corresponding signatures, and the report tag together with the transformation cost to the sanitizer. When the above messages from consumer are valid, the sanitizer firstly sanitizes the blinded data blocks right into a uniform layout and additionally sanitizes the data blocks corresponding to the organization's sensitive records to protect the privateness of organization,after which transforms their corresponding signatures into valid ones for sanitized record using transformation value. Finally, the sanitizer uploads the sanitized record and the corresponding signatures to the cloud.When the information integrity auditing challenge is performed, the cloud generates an auditing evidence according to the undertaking from the TPA. The TPA can affirm the integrity of the sanitized file stored the cloud by means of checking whether or not this auditing proof is accurate or not.In this scheme, Time Server plays important role in time based integrity checking, bandwidth utilization, and the server will be up time for all the user as we have share time to access the server for different user at different time it will help to use the server full capacity and also reduce the cost of server as user get access to server at different time. In this system we have used time server technique to give and dedicated time slot to an user to avoid the server down time and utilize the server with fill efficiency and performance by this we avoid the problem of down time.

A. Architecture

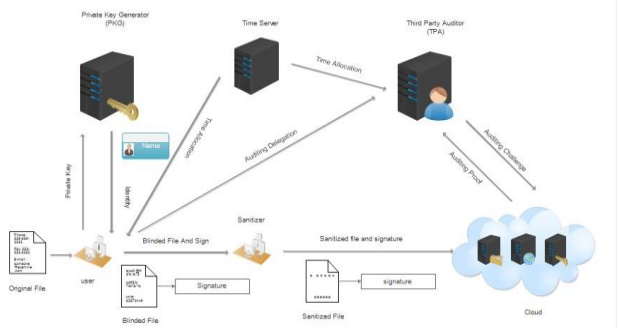

Fig. 1. System Architecture

In this paper, we mentioned the different modules of the proposed system:

Cloud Servers: It contains nearly unlimited storage area which is capable of store and manage all the data or less within the system. Other entities with constrained storage space can save their data. The cloud provides enormous data storage space to the user. Through the cloud storage service, users can upload their data to the cloud and percentage their records with others.

Users: : The person is a member of an organization, which has a massive range of files to be stored within the cloud.

PKG: It is an imperative entity, which is answerable for generating, distributing and managing all public parameter and the private keys for the user according to his identity ID.

Sanitizer: The sanitizer is in the rate of sanitizing the data blocks corresponding to the sensitive records (personal sensitive data and the organization's sensitive data) in the document, reworking these data blocks' signatures into legitimate ones for the sanitized

document, and uploading the sanitized report and its corresponding signatures to the cloud.
TPA: TPA has understanding and abilities that cloud users do not have and is depended on to check the integrity of the cloud information on behalf of the cloud person upon request. Each entity has their very own responsibilities and blessings respectively. The TPAs process is to carry out the data integrity checking on behalf the cloud user.Time Server: It is a time reference server without any interaction with other entities involved in the system. It is accountable for a unique release time specification. The user first of all blinds the data blocks similar to the non-public sensitive data of the document and generates the corresponding signatures. These signatures are used to guarantee the authenticity of the document and confirm the integrity of the report. Then the consumer sends this blinded file and its corresponding signatures to the sanitizer. After receiving the message from the user, the sanitizer sanitizes those blinded data blocks and the data blocks corresponding to the organization's sensitive information and then transforms the signatures of sanitized data blocks into legitimate ones for the sanitized record. Finally, the sanitizer sends this sanitized record and its corresponding signatures to the cloud. These signatures are used to verify the integrity of the sanitized report inside the phase of integrity auditing. The TPA verify the integrity of the sanitized data stored inside the cloud based on timestamp, he sends an auditing task to the cloud. And then, the cloud responds to the TPA with auditing evidence of facts possession. Finally, the TPA verifies the integrity of the sanitized report by checking whether or not this auditing proof is accurate or not.

B. Algorithms

Advanced Encryption Standard:
The more popular and widely adopted symmetric encryption algorithm likely to be encountered nowadays is the Advanced Encryption Standard (AES). It is found at least six time faster than triple DES.
A replacement for DES was needed as its key size was too small. With increasing computing power, it was considered vulnerable against exhaustive key search attack. Triple DES was designed to overcome this drawback but it was found slow.
The features of AES are as follows

- Symmetric key symmetric block cipher
- 128-bit data, 128/192/256-bit keys
- Stronger and faster than Triple-DES
- Provide full specification and design details
- Software implementable in C and Java

Operation of AES:
AES is an iterative rather than Feistel cipher. It is based on substitution–permutation network. It comprises of a series of linked operations, some of which involve replacing inputs by specific outputs (substitutions) and others involve shuffling bits around (permutations).
Interestingly, AES performs all its computations on bytes rather than bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing as a matrix. Unlike DES, the number of rounds in AES is variable and depends on the length of the key. AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Each of these rounds uses a different 128-bit round key, which is calculated from the original AES key.
1) Input:
2) 128 bit /192 bit/256 bit input(0,1) 3)secret key(128 bit)+plain text(128 bit).
4) Process:
5)10/12/14-rounds for-128 bit /192 bit/256 bit input
6)Xor state block (i/p)
7)Final round:10,12,14
8)Each round consists:sub byte, shift byte, mix columns, add round key.
9)Output:
10)cipher text(128 bit)
MD5

In cryptography, MD5 (Message-Digest calculation 5) is a generally utilized cryptographic hash work with a 128-piece hash esteem. As an Internet standard (RFC 1321), MD5 has been utilized in a wide assortment of security applications, and is likewise regularly used to check the trustworthiness of records. A MD5 hash is ordinarily communicated as a 32 digit hexadecimal number. MD5 is a fortified adaptation of MD4. Like MD4, the MD5 hash was concocted by Professor Ronald Rivest of MIT. Additionally, MD5 was clearly utilized as the model for SHA-1, since they share numerous normal highlights. MD5 and SHA-1 are the two most broadly utilized hash calculations today.
The Following five steps are performed to compute the message. Step 1: Append Padding Bits. Step 2: Append Length
Step 3: Initialize MD Buffer
Step 4: Process Message in 16 –Word Blocks.
Step 5: Output
C. Mathematical Model
1. Mathematical equation:
The algorithm implemented in this project is describe as: Initialization: password,key,time,salt:string time ←– *get time* _
$input \longleftarrow (password)$
$key \longleftarrow salt + time$
Encryption:
Ciphertext ←– *AESEncrypt*(*password,key*) *output*(*ciphertext*) Decryption:
key ←– *salt – time*
forasmuchtolerancegiventime
$if key = get\_time$
$key \longleftarrow salt + time$
plaintext ←– *AESDecrypt*(*ciphertext,key*) *endif endfor output*(*plaintext*)

Result and Discussion

For input data size of 1, 91,383 and 2, 32,398 required 165 second and 209 seconds respectively for Two Fish algorithm. Which shows more efficiency than DES, 3DES, AES, BF.

Table 1: Comparison of symmetric algorithms

Algo - rithm	Key size	Block size	Round	Structure	Flexible	Features
DES	64 bits	64 bits	16	Feistel	No	Not structure Enough
3DES	112 or 118 bits	64 bits	48	Feistel	Yes	Adequate security
AES	128256 bits	128 bits	20	Feistel	Yes	Excellent security
BLOW FISH	32448 bits	64 bits	16	Feistel	Yes	Good Security

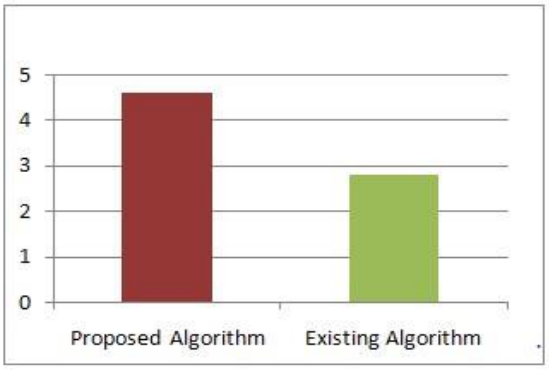

Fig. 2. Graph 1

Conclusion

In this system, we investigated a new primitive acknowledged as time-based integrity checking and information sharing for secure cloud storage. In this paper, we proposed an identity-based data integrity auditing scheme for secure cloud storage, which supports data sharing with sensitive information hiding. In our scheme, the file stored in the cloud can be shared and used by others on the condition that the sensitive information of the file is protected. Besides, the remote data integrity auditing is still able to be efficiently executed. The security proof and the experimental analysis demonstrate that the proposed scheme achieves desirable security and efficiency.

References

[1]. Boyang Wang, Baochun Li,Hui Li, "Privacy-Preserving Public Auditing for Shared Data in the Cloud" IEEE transactions on cloud computing, vol. 2, no. 1, january-march 2014.

[2]. Tina Esther Trueman ,P.Narayan asamy "Ensuring privacy and data freshness for public auditing of Shared data in cloud," 2012:

[3]. Rongxing Lu, Hui Zhu, Ximeng Liu, Joseph K. Liu, Jun Shao , "Toward Efficient and Privacy-Preserving Computing in Big Data Era " July/August 2014

[4].] S. Fugkeaw , H. Sato, Chiang Mai , "Privacy-preserving access control model for big data Cloud", International Computer Science and Engineering Conference (ICSEC), 2015, pp. 1-6.

[5]. J. Yu, K. Ren, and C. Wang, "Enabling cloud storage auditing with verifiable outsourcing of key updates," IEEE Trans. Inf. Forensics Security, vol. 11, no. 6, pp. 1362–1375, Jun. 2016.

[6]. Zhusong Liu, "A Secure Anonymous Identity-based Access Control over Cloud Data", 2013 Fourth International Conference on Emerging Intelligent Data and Web Technologies.

[7]. Vivek Pandey, Umesh Kulkarni, "Effective Data Sharing with Forward Security Identity based Ring Signature using different algorithms", 2017 International Conference on Intelligent Computing and Control (I2C2).

[8]. Zhiqian Xu, Hai Jiang, "HASS: Highly Available, Scalable and Secure Distributed Data Storage Systems", 2009 International Conference on Computational Science and Engineering.

[9]. Kamara, S., Lauter, K. Sion, R., Curtmola, R., Dietrich, "Cryptographic Cloud Storage", 2010 Workshops of LNCS Springer, Heidelberg, vol. 6054, pp. 136-149, 2010.

[10]. Ndibanje Bruce, Mangal Sain, Hoon Jae Lee, "A Support Middleware Solution for e-Healthcare System Security", IEEE 16th International Conference on Advanced Communication Technology.

[11]. W. Shen, J. Yu, H. Xia, H. Zhang, X. Lu, and R. Hao, "Light-weight and privacy-preserving secure cloud auditing scheme for group users via the third party medium," J. Netw. Comput. Appl., vol. 82, pp. 56–64, Mar. 2017

[12]. Y. Yu et al., "Identity-based remote data integrity checking with perfect data privacy preserving for cloud storage," IEEE Trans. Inf. Forensics Security, vol. 12, no. 4, pp. 767–778, Apr. 2017.

[13]. J. Shen, J. Shen, X. Chen, X. Huang, and W. Susilo, "An efficient public auditing protocol with novel dynamic structure for cloud data," IEEE Trans. Inf. Forensics Security, vol. 12, no. 10, pp. 2402–2415, Oct. 2017.

[14]. G. Yang, J. Yu, W. Shen, Q. Su, Z. Fu, and R. Hao, "Enabling public auditing for shared data in cloud storage supporting identity privacy and traceability," J. Syst. Softw., vol. 113, pp. 130–139, Mar. 2016.

[15]. Anjana Devi, Ramya B. S., "Two fish Algorithm Implementation for lab to provide data security with predictive analysis", IRJET ,Volume: 04 Issue: 05 — May -2017

[16]. Jia Yu, Kui Ren, Cong Wang, IEEE "Enabling Cloud Storage Auditing With Verifiable Outsourcing of Key Updates", IEEE ,VOL. 11, NO. 6, JUNE 2016

[17]. H. Wang, D. He, and S. Tang, "Identity-based proxy-oriented data uploading and remote data integrity checking in public cloud," IEEE Trans. Inf. Forensics Security, vol. 11, no. 6, pp. 1165–1176, Jun. 2016.

[18]. Yong Yu, Man Ho Au, Giuseppe Ateniese, Xinyi Huang, Willy Susilo, Yuanshun Dai, and Geyong Min, "Identity-based Remote Data Integrity

[19]. Checking with Perfect Data Privacy Preserving for Cloud Storage",IEEE , pp. 1556-6013 (c) 2016

[20]. Aldar C-F. Chan,Ian F. BlakeScalable, "Server-Passive, User-Anonymous Timed Release Cryptography",IEEE 1063-6927/05©2005

[21]. Kenneth G. Paterson and Elizabeth A. Quaglia, "Time-Speci c Encryption" ICT-2007-216676 ECRYPT II.