IJCSEInternational Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-5, Issue-12 E-ISSN: 2347-2693

Privacy Protection on Cloud Computing with Auditing Scheme

Nimmymol Manuel[1*], Simy Mary Kurian[2], Neena Joseph[3], Neema George[4]

[1,2,3,4]Department of Computer Science & Engineering,Mangalam College of Engineering, Kerala, India

[*]*Corresponding Author: nimmymol.manuel@mangalam.in, Tel.: +91 9496380516*

Available online at: www.ijcseonline.org

Received: 23/Nov/2017, Revised: 08/Dec/2017, Accepted: 15/Dec/2017, Published: 31/Dec/2017

Abstract— Distributed computing gives an assortment of administrations to our current specialized regions. It is helpful for the two customers and organizations to utilize applications without access their own records. Security is an unavoidable component of our cloud administration. So we ought to make sure that our specialist organization can give the security to our information. Yet, various prominent hacking cases will prompt various sorts of safety issues on cloud. It for the most part happens in multi clients distributed computing regions Cloud security is significant in each field of clients. Everybody needs to give their data completely safe. For this reason, here we can utilize property-based encryption that is a kind of open key encryption. Characteristic based encryption permits information proprietors and clients to encode and decode in light of the individual ascribes. So we propose a audit scheme which gives a sort of security insurance on clients and keep from unapproved access from programmers.,

Keywords— Encryption, CP-ABE, Collusion Attack

I. INTRODUCTION

Distributed computing is a technique for conveying different administrations where assets are recovered from the Internet through online applications. Instead of keeping records on a hard drive or neighborhood stockpiling gadget, cloud-based capacity makes it conceivable to save them to a distant data set. Distributed computing is usually utilized in the present IT world in light of its high openness and accessibility.

Significant dangers to cloud security incorporate information break, information misfortune, account hacking, unreliable application programming Interfaces (APIs),poor decision of distributed storage gives and shared innovation that can think twice about security. There are a few kinds of encryption strategies are utilized on distributed computing for giving security on clients information and qualities. Out of these the most presumably utilized strategy is property based encryption. Clinical proposition is a fundamental part in current medical care the executives. Wellbeing data at different levels could be produced from Medical theory. Exact and solid data is required for arranging medical care exercises and wellbeing planning and this could be acquired uniquely from these records. It works on the capacity, recovery, and sharing of the clinical data more productive. We center around numerous information proprietor situation.

The significance of information honesty has been featured by the accompanying examination works under various framework and security models. The major issue related to security problem is collude attack.

So here present an auditing scheme for security assurance on the information's put away on the cloud server. It really takes a look at the trustworthiness of put away information without help from anyone else. Through point by point security investigation, the proprietor's archive is demonstrated to be safer.

The rest of this paper is coordinated as follows. In section2, the related works are talked about. Section3, the proposed strategies are introduced. In section4, Experiment result followed by Conclusion.

From the user's perspective, the ability to utilize and access the resources on demand and the availability of the cloud are strong incentives for the usage of cloud. But there exist many security problems. The importance of data integrity has been highlighted by the following research works under different system and security models.

The major issue related to security problem is collude attack. So here introduce an auditing scheme for privacy protection on the data's stored on the cloud server. It checks the integrity of stored data by themselves. Through detailed security analysis, the owner's document is shown to be more secure. The remainder of this paper is organized as follows. Insection2, the related works are discussed. Section3, the proposed techniques are presented. In section4, Experiment result followed by Conclusion

II. RELATED WORK

There exists an issue over scrambled cloud information when customized multi-watchword positioned search is utilized to check regardless of whether questioned catchphrases where present.

The framework is a combination of both proxy signature, enhanced TGDH and proxy re-encryption both together into a single protocol. By applying the proxy signature technique, the group leader can definitely grant the privilege of managing the group to one or more chosen group members. [1]

Data access control involving characteristic based encryption in broad daylight distributed storage is the one more related work which incorporate Attribute Based Encryption (ABE), is a cryptographic framework which gives information owner direction command over their information openly distributed storage. In the standard ABE scheme comprises of single position to keep up quality set which can bring a singular point change on both security and execution. 2] Presently we utilize edge multi-authority Cipher content Policy Attribute-Based Encryption (CP-ABE) get to control plot, called by the name TMACS. TMACS is Threshold Multi-Authority Access Control System. The fundamental benefit of Cipher text strategy characteristic based encryption calculation is it gives fine grained and secure data access control for cloud storage distributed storage (public) with cloud servers. Yet, it has a few defects in its structure for example the single characteristic authority should execute the tedious client approval, confirmation and mystery key appropriation, and thus it brings about a solitary point execution overhead.[3] When this strategy is utilized continuously clients need to hang tight in the sitting tight line for a lot of opportunity to acquire individual mystery key, consequently it costs the effectiveness of the framework. This framework can't defeat the disservices of single point upward productivity. [4] Only one position to keep up with the entire property set in the prior ABE conspire, yet it can bring a solitary point bottleneck on both security and performance.[5]

A few numerous specialists are thusly proposed which various specialists are independently keeping up with disjoint trait subset. However, this problem remains unsolved that were shown by earlier ABE scheme.[6] A threshold multi-authority CP-ABE access control scheme for public cloud storage is known as TMACS, in which multiple authorities jointly manage a uniform attribute set. Security and performance analysis of the above system's results show that TMACS is not only verifiable secure when less than the authorities are compromised, but also robust when no less than the authorities are alive in the system.[3] Furthermore, the traditional multi-authority scheme with TMACS combined efficiently, we construct a hybrid one, which achieving security and system-level robustness.

The System and Threat Model

The System and Threat Model We consider a cloud data storage service involving three different entities, as illustrated in Fig. 1: the cloud user (U), who has large amount of data files to be stored in the cloud; the cloud server (CS), which is managed by the cloud service provider (CSP) to provide data storage service and has significant storage space and computation resources (we will not differentiate CS and CSP hereafter); the third party auditor (TPA), who has expertise and capabilities that cloud users do not have and is trusted to assess the cloud storage service reliability on behalf of the user upon request.

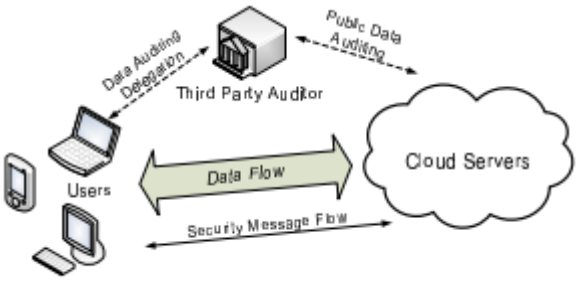
Users rely on the CS for cloud data storage and maintenance. They may also dynamically interact with the CS to access and update their stored data for various application purposes. To save the computation resource as well as the online burden, cloud users may resort to TPA for ensuring the storage integrity of their outsourced data, while hoping to keep their data private from TPA.

We consider the existence of a semi-trusted CS as [16] does. Namely, in most of time it behaves properly and does not deviate from the prescribed protocol execution. However, for their own benefits the CS might neglect to keep or deliberately delete rarely accessed data files which belong to ordinary cloud users. Moreover, the CS may decide to hide the data corruptions caused by server hacks or Byzantine failures to maintain reputation. We assume the TPA, who is in the business of auditing, is reliable and independent, and thus has no incentive to collude with either the CS or the users during the auditing process. However, it harms the user if the TPA could learn the outsourced data after the audit.

To authorize the CS to respond to the audit delegated to TPA's, the user can sign a certificate granting audit rights to the TPA's public key, and all audits from the TPA are authenticated against such a certificate. These authentication handshakes are omitted in the following presentation.

Design Goals

To enable privacy-preserving public auditing for cloud data storage under the aforementioned model, our protocol design should achieve the following security and performance guarantees.



1) Public auditability: to allow TPA to verify the correctness of the cloud data on demand without retrieving a copy of the whole data or introducing additional online burden to the cloud users.

2) Storage correctness: to ensure that there exists no cheating cloud server that can pass the TPA's audit without indeed storing users' data intact.

3) Privacy-preserving: to ensure that the TPA cannot derive users' data content from the information collected during the auditing process.
4) Batch auditing: to enable TPA with secure and efficient auditing capability to cope with multiple auditing delegations from possibly large number of different users simultaneously.
5) Lightweight: to allow TPA to perform auditing with minimum communication and computation overhead.

III. METHODOLOGY

For decreasing the circulation intricacy, the framework is isolated into numerous security credits. Here the security is given to the exploration papers of specialists having a place with five distinct nations. The security is given in the trait level. Subsequently each specialist has full command over their protection. So key administration intricacy can be diminished. To carry out and plan a module in light of trait encryption, security is more given. While utilizing this property put together encryption with respect to cloud, it upgrades the scrambled information. Here endorsement authority can oversee quality power and an inspecting plan is additionally accommodated security purposes. The fundamental issue is connected with multiuser.

The framework is acombination of both proxy signature, enhanced TGDH and proxy re-encryption both together into a single protocol. Byapplying the proxy signature technique, the group leader candefinitely grant the privilege of managing the group to one ormore chosen group members. [1] By the implementation of proxy re-encryption, the operations which are mostlycomputationall y intensive can be delegated to Cloud Serverswithout providing any of the private information. Extensivesecurity and performance analysis shows that our proposedscheme is highly efficient and satisfies the securityrequirements of the public cloud based on secure group sharing. [1]

But it has some flaws in its framework i.e. the singleattribute authority must execute the time consuming uservalidation, verification and secret key distribution, and henceit results in a single point performance overhead.[3] Whenthis technique is used in real time users have to wait in thewaiting queue for a significant amount of time to obtainrespective secret key, therefore it costs the efficiency of thesystem. This system cannot overcome the disadvantages ofsingle point overhead efficiency. [4] Only one authority tomaintain the whole attribute set in the earlier ABE scheme, but it can bring a single-point bottleneck on both securityand performance.[5]

Cloud is intrigue assault. This assault can be available to a degree by utilizing this inspecting plan. This examining plan is a sort of open key encryption .It is utilized to really look at the respectability of the clients .So it keeps up with the records and information with practically no adjustments. The records are apparent to just approved clients and they can't change or download it.

For reducing the distribution complexity, the system isdivided into multiple security attributes. Here the security is provided to the research papers of doctors belonging to fivedifferent countries. The security is provided in the attributelevel. Hence each doctor has full control over their privacy.So key management complexity can be reduced. Toimplement and design a module based on attributeencryption, security is more provided. While using thisattribute based encryption on cloud, it enhances theencrypted data. Here certificate authority can manageattribute authority and an auditing scheme is also providedfor security purposes. The main problem is related tomultiuser.Cloud is collusion attack. This attack can be present to anextent by using this auditing scheme. This auditing scheme isa type of public key encryption .It is used to check theintegrity of the users .So it maintains the documents and datawithout any modifications. The documents are visible to onlyauthorized users and they cannot modify or download it.

DATA INTEGRITY PROTECTION METHODS

Accordingly data integrity attacks in cloud includes Data Modification Attack, Tagforgery and Data Leakage Attack, Replay and Timeliness Attack, Roll-Back Attack and Collusion Attack and Byzantine Attack.

Data integrity achieved by utilizing precomputed token. The original file is represented by m column vectors in Galois Field. This file would be encrypted by multiplying with a certain matrix to achieve additional k parity check vectors. Thus, the encrypted file contains m+k columns in total. Further computation would be done over the last k parity check columns to protect the confidentiality. At the end the encrypted m columns and the modified last k parity check columns are sent to store in cloud. The encryption has additive homomorphic encryption attributes, which enables efficient updates of the file.

On each encrypted vector, if t times of verification is need-ed. Each time, a token is computed using partial blocks of data in the vector, thus (m+k)t tokens are precomputed in total. In order to verify the integrity of the file, the index would be sent to cloud storage, and same computation procedure on that partial data is done to generate the signature, which would be sent back and compare with the original token. Thus, if file corruption occurs, the corrupted location would be known.

This is mathematical approach of integrity checking is in data level. However, there are certain problems with this method:
a). All precomputed tokens need to be stored in local environment. Although the paper mentions that it could be stored in remote cloud, the untrusted cloud providers would be able to modify it.
b) Since the tokens are not generated on all parts of the file, it could only provide probabilistic integrity assurance.

A Trusted Cloud Computing Platform (TCCP) based on trusted computing is proposed to protect confidentiality

and integrity. The trusted platform module is implemented in each node. However, since users don't have control over the physical machines, remote attestation is needed to ensure that measurement indeed comes from the VM which users are running applications on. In each virtual machine, trusted platform module (TPM) is embedded and a trusted virtual machine monitor (TVVM) is installed during the booting. Besides, an external trusted coordinator (TC) is used to do the attestation. The virtual nodes need to register with TC.

Intel already has Intel Trusted Execution Technology (TXT) based on the TPM. It is compatible with OpenStack which is a open-source software platform for cloud computing. In it, and OpenAttestaion server is responsible for communicating with the trusted computing pool of hardware and software.

However, with trusted cloud computing, application level attack would not be determined. For example, if data stored in database are compromised. It would not be detected. In order to use TCCP, additional application level security needs to be implemented

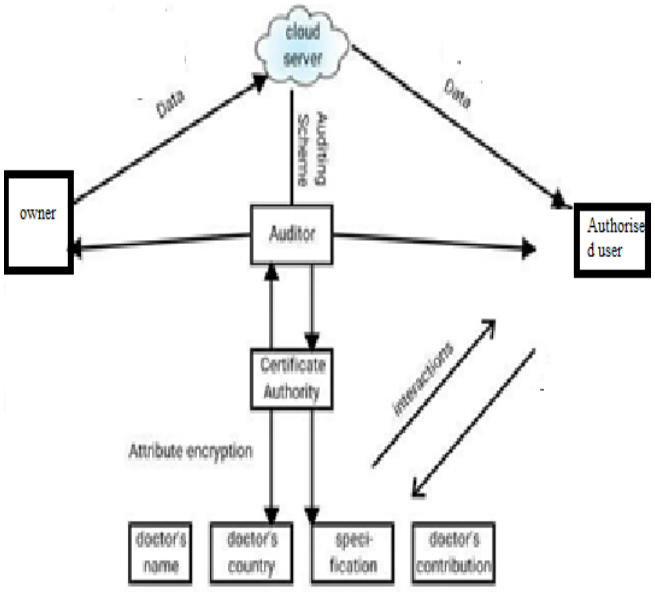


Figure 1. Proposed Architecture

IV. EXPERIMENTAL ANALYSIS

From the investigation of every innovation the security is improved all along. Inside the underneath shown diagram, the X - axis suggest that the social affair of records and the Y-axis addressed that the level of precision of information. Accordingly the disadvantage is, as the security issues decline the exhibition is additionally decline. When contrasted with different innovations the evaluating plan gives greater security. The component of this examining is to execute this with less time utilization. Arrangement assault is a drawback that is seen in multiuser cloud administration. Also, it could actually forestall this at a cutoff through this new examining plan. By utilizing the intermediary signature approach, the gathering chief can effectively outfit the honor of association the executives to something like at least one chose bunch members. Assuming this server got any harm during the hour of working that will influence the character of the client.

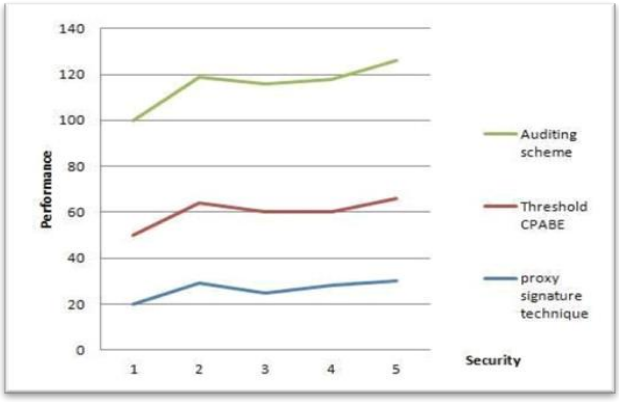


Figure 2: Experimental Result

The innovation access tree structure, the size of the code text in this innovation is steady. In the event that the size of the plain text is huge, the result of the comparing size won't get. Assuming utilize the Obfuscation innovation, the information given by us is switched over completely to another structure and it will conceal the presence of data. So the outcome is anything but a careful information. The deficiency of data is the serious issue of this plan. By the utilization of edge multi authority CP-ABE conspire we can oversee more than one authority with same trait set. Different specialists share Master keys and it will create Legal client's mystery keys. When contrasted with different advancements this innovation is safer and vigorous.

Revocable multi specialists CP-ABE plans are utilized to give information access security guarantee. Instead of that security can accomplish both forward and in reverse.

Security Evaluation

For different cloud providers, its ranking and cost are different. Also for different methods, the overall performance including time complexity T, cost C, security S and privacy P level are different. In order to evaluate a method with the overall performance, a weighted linear ranking is proposed as follows:

$$Pr= a1\times T+a2\times C +a3\times S +a4\times P$$

where ai is adjustable weight. The time complexity needs to be evaluated per algorithm base. The cost could be measured through the billing system of cloud providers. For data security and privacy in cloud, it is kind of overlapping. Because if encryption is used, as long as the data is confidential, the sensitive information will not be disclosed. In addition, the data mining attacks would be mitigated. Thus, here only data security is considered.

Data security includes data availability, integrity and confidentiality. Data availability would be compromised in

two main categories in cloud. First is the cloud architecture reliability, i.e. the regular maintenance and failure of machine instances. The other comes from attacks talked above.

For data confidentiality, there are three layers of confidentiality in the proposed architecture. In order to recover data, one needs to bypass the authentication of a cloud platform. Inside the cloud platform, hierarchical access to data is required. The encrypted information disclosed is partial. Thus, the non-confidentiality Level Probability of Accessing one of the cloud service * Hierarchically Access Probability that the original information contained in the virtual machine.

V. CONCLUSION

An inspecting plan, which depends on trait based encryption that gives additional security to the report put away in our cloud server. After some examination, we characterize the clients as per their specialization in their investigations and furthermore in which country they are from. Here greater security protection is forestalled for the records. The security depends on the property level we built another cipher text policy attribute based encryption (CP-ABE) with proficient encryption and decoding to stay away from the agreement assault for some degree. The technique and the examination result shows that our new plans put away in the cloud and it permits just approved clients to get to the records.

Future work

The proposed architecture could provide various security methods according to the data type and usage to reduce the complexity by calling a common API. However, there are some problems with this design to be solved:

a). The call to the common API would be intensive, thus caching and scalable procedures are needed.

b). Although most storage and computation are done in remote cloud, the preprocessing and certain data related information need to be stored and maintained locally.

c). Since algorithms over encrypted data are applied, customer-oriented algorithms need to be developed. Users need have a good knowledge of encrypted data.

d). A fully functional benchmark for the system need to be designed, implemented and evaluated with quantitative and qualitative performance metrics

REFERENCES

[1] K. Yang and X. Jia, "*Expressive, efficient and revocable data access control for multi-authority cloud storage*," IEEE Transactions on Parallel and Distributed Systems, Vol.**25**, Issue.no.**7**,pp. **1733-1744 2013**.

[2] K. Xue and P. Hong, "*A dynamic secure group sharing framework in public cloud computing*," IEEE Transactions on Cloud Computing, Vol. **2**, Issue **4**, pp. **459–470, 2014**.

[3]]. J. Han, W. Susilo, Y. Mu, J. Zhou, and M. H. A. Au, "*Improving privacy and security in decentralized cipher text policy attribute-based encryption,*" IEEE Transactions on Information Forensics and Security, Vol. **10**, Issue. **3**, pp. **665–678, 2015**

[4] K. Yang, X. Jia, and K. Ren, "*Secure and verifiable policy update outsourcing for big data access control in the cloud*," IEEE Transactions on Parallel &Distributed Systems, Vol. **26**, Issue **12**, pp. **3461–3470, 2015.**

[5] W. Li, K. Xue, Y. Xue, and J. Hong, "*TMACS:A robust and verifiable threshold multi-authority access control system in public cloud storage,*" IEEE Transactions on Parallel & Distributed Systems, Vol. **27**, Issue. **5**, pp**. 1484– 1496, 2016**

[6] Kai Fan1*, Qiong Tian1, Junxiong Wang1, Hui Li1, Yintang Yang2, "*Privacy Protection Based Access Control Scheme in Cloud-Based Services*" Vol.14,Issue.1,pp.61-71

Authors Profile

Ms.Nimmymol Manuel is working as Assistant Professor in the Department of Computer Science & Engineering of Mangalam College of Engineering ,Kerala ,India since 2008.Shecompleted her B.Tech in Computer Science & Engineering in 2006 from Mahatma Gandhi University with First Class and M.Tech in Computer Science & Engineering from M.S University Tirunelveli in 2012. Her research interest include Wireless Sensor Netwok, Artificial Intelligence, Computer Architecture and IoT. She has taught both undergraduate and post graduate topics and guided several projects. She is a member of Computer Society of India.

Ms.Simy Mary Kurian Assistant Professor , Department of Computer Science and Engineering, Mangalam College of Engineering, Kerala, India since 2011.She has completed B.Tech in Computer Science and Engineering from Mahatma Gandhi University and M.Tech in Software Engineering from Karunya Institute of Technology and Science. Her research interest include Image Processing, Data Science, Artificial Intelligence and Bio-inspired Computing .She has associated with many number of undergraduate and research projects.

Ms.*Neena Joseph* has completed her master's degree in Computer Science & Engineering from Manonmaniam *Sundaranar University* and bachelor's degree in Computer Science & Engineering from Mahatma Gandhi University. She has qualified UGC NET in Computer Science and Applications and has more than 10 years of under graduate teaching experience and 8 years of post-graduate teaching experience. She has to her credit several research papers, published in reputed National and International journals. She has presented many research papers in various conference of International repute. Her areas of interest include Theoretical Computer Science, Natural Language Processing and Compiler Optimization.

Ms.Neema George Assistant Professor , Department of Computer Science and Engineering, Mangalam College of Engineering, Kerala, India since 2008. Her research interest include Image Processing, Machine Learning, Artificial Intelligence Cloud Computing.

