Multipurpose Auditing Unit with Auditing and Security Measures in Cloud Computing

Miss Divya M. Kantode
SGBAU, Amravati
Maharashtra, India.

Dr. V. M. Thakare
SGBAU, Amravati
Maharashtra, India

ABSTRACT

Cloud data and its auditing, security and integrity are the issues which affects the cloud services. Users concerns about their privacy and to maintain it users need service that provides any how that maintains the security and integrity of data on cloud. Proposed methodology states the multipurpose auditing unit which aims for public auditing of the cloud data and also improves the data integrity and security. Proposed methodology can helps to provide hassle free use of cloud services and proposes to improve storage space also, which will increase user's trust on cloud service providers. Proposed method tries to gives overall secure methodologies which will connects users and service providers with easier and secure cloud services.

***Keywords*: -** *Cloud data, Integrity, Security, Public Auditing, and Cloud User.*

I) I) INTRODUCTION

Challenges in front of the intelligent connected object consists of: secure and reliable association of autonomous devices; secure and protected communication in uncontrolled environment; trust on services, people or devices; authentication of users and connecting them to their devices, data and services without compromising their privacy, data protection, security. Today's need is environment to look for general and standardized security decisions that suit the high demand of dynamic internet-based applications and smart objects[1].

One of the main services provided by cloud system is storage, which allows users to store their enormous amount of data to the remote clouds without bothering the complex management of storage hardware. But data security issues such as privacy and integrity brought by third parties cloud systems have been the major concerns for users utilizing such services. Since the data is stored and managed in the cloud, the data security highly depends on the IT management of the cloud services providers [2].

Cloud platform provides powerful storage services to individuals and organizations. It brings great benefits of allowing on-the-move access to the outsourced files, simultaneously relieves file-owners from complicated local storage management and maintenance. Some security concerns may impede users to use cloud storage. Identity-based data outsourcing (IBDO) system achieves a strong auditing mechanism. IBDO scheme achieves strong security in the sense that: (1) it can detect any unauthorized modifications on the outsourced files and (2) it can detect any misuse/abuse of the delegations/authorizations. These security properties are formally proved against active colluding attackers [3].

Cloud storage became one of the critical services, because users can easily modify and share data with others in cloud. However, the integrity of shared cloud data is vulnerable to inevitable hardware faults, software failures or human errors. In the worst cases, a cloud owner may even conceal data error accidents in order to preserve its reputation or avoid profit losses. NPP: A New Privacy-Aware Public Auditing ensures the integrity of data stored in cloud servers, a number of mechanisms based on various techniques. In particular, in order to reduce the burden on users, a trusted third-party auditor is engaged to conduct the verification, which is called public auditing [4].

Cloud computing is a new computation model; this kind of computing paradigm enables us to obtain and release computing resources rapidly. So it can access resource-rich, various, and convenient computing resources on demand. The computing paradigm also brings some challenges to the security and privacy of data when a user outsources sensitive data to cloud servers. Outsourced-ABE (OABE)organically integrate with PEKS and present a novel cryptographic paradigm called outsourced attribute-based encryption scheme which reduces the computation cost for users who want to access encrypted data stored in cloud by outsourcing the heavy computation to cloud service provider[5].

The proposed methodology provides a multipurpose auditing unit on a cloud system which helps to improve communication and security between sender and receiver. Proposed methodology states the additional security measures which will restrict the cyber-attack on cloud services. Users data uploaded on cloud should be easily available for sharing but integrity must be maintained. To maintain security multipurpose auditing unit is useful. Proposed methodology uses past recommendations and history analysis to deliver better services. Also aims to improve cloud storage space for more effective use of cloud services.

II) II) BACKGROUND

New challenges in front of the intelligent connected object consists of: secure and reliable association of autonomous devices; secure and protected communication in uncontrolled environment; trust on services, people or devices; authentication of users and connecting them to their devices, data and services without compromising their privacy, data protection, security. There are some solutions on the market that can be applied as RFID, NFC, SSO, and OAuth which will solve the trust related issues [1].

Outsourcing big data to clouds provides many benefits, e.g., low costs, good reliability and availability, but the data security issues such as privacy and integrity brought by third parties cloud systems have been the major concerns for users utilizing such services. Since the data is stored and managed in the cloud, the data security highly depends on the IT management of the cloud services providers which ensures cryptographic primitives such as a new type-based proxy re-encryption to design a secure and efficient data distribution system in MCC [2].

Cloud platform provides powerful storage services to individuals and organizations. It brings great benefits of allowing on-the-move access to the outsourced files, simultaneously relieves file-owners from complicated local storage management and maintenance. Some security concerns may impede users to use cloud storage. Identity-based data outsourcing (IBDO) system in a multi-user setting achieves a strong auditing mechanism. IBDO scheme achieves strong security [3].

Users can easily modify and share data with others in cloud. However, the integrity of shared cloud data is vulnerable to inevitable hardware faults, software failures or human errors. In the worst cases, a cloud owner may even conceal data error accidents in order to preserve its reputation or avoid profit losses a trusted third-party auditor is engaged to conduct the verification, which is called public auditing. Therefore, researchers proposed some new schemes to protect privacy, including data privacy, and identity privacy [4].

Cloud computing is a new computation model in which computing resources is regarded as service to provide computing operations. This kind of computing paradigm enables us to obtain and release computing resources rapidly. So it can access resource-rich, various, and convenient computing resources on demand. The computing paradigm also brings some challenges to the security and privacy of data when a user outsources sensitive data to cloud servers [5].

This paper introduces a multipurpose auditing methodology which aims to improve communication and security on cloud services this proposed theory. This paper organized as follows. **Section I** Introduction. **Section II** discusses Background. **Section III** discusses previous work. **Section IV** discusses existing scheme. **Section V** analysis and discusses scheme results. **Section VI** proposed method. **Section VII** includes outcome result possible. **Section VIII** concludes this review paper. **Section IX** discusses Future Scope.

III) III) PREVIOUS WORK DONE

N. Kakanakov et.al (2017) [1] proposed methodology which uses adaptive models for security and data protection in IoT could provide a base for systematic analyses and application of best practices and security techniques in variety of use cases. This could provide environment to look for general and standardized security decisions that suit the high demand of dynamic internet-based applications and smart objects.

Jiang Zhang et.al (2016) [2] proposed methodology with several cryptographic primitives such as a new type-based proxy re-encryption to design a secure and efficient data distribution system in MCC, which provides data privacy, data integrity, data authentication, and flexible data distribution with access control. Compared to traditional cloud-based data storage systems, proposed system is a lightweight and easily deployable solution for mobile users in MCC since no trusted third parties are involved and each mobile user only has to keep short secret keys consisting of three group elements for all cryptographic operations.

Yujue Wang et.al (2016) [3] proposed a method named identity-based data outsourcing (IBDO) system in a multi-user setting. IBDO scheme achieves a strong auditing mechanism. IBDO scheme achieves strong security in the sense that it can detect any unauthorized modifications on the outsourced files and can detect any misuse of the delegations/authorizations. These security properties are formally proved against active colluding attackers. To the best of knowledge, this is the first scheme that simultaneously achieves both goals. The IBDO proposal provides resilient security properties without incurring any significantly performance penalties.

Anmin Fu et.al (2016) [4] proposed a method which ensures integrity of data stored in cloud servers, a number of mechanisms based on various techniques. In particular, in order to reduce the burden on users, a trusted third-party auditor is engaged to conduct the verification, which is called public auditing. In particular, in order to reduce the burden on users, a trusted third-party auditor is engaged to conduct the verification, which is called public auditing. Therefore, researchers proposed some new schemes to protect privacy, including data privacy, and identity privacy. On one hand, the identity of each signer is anonymous; and on the other hand, the group manager can trace a signer’s real identity after a dispute. Unfortunately, in all existing public auditing schemes, the tracing process is accomplished by a single entity. As a result, that entity has the privilege of tracing, which may lead to abuse of single authority power. Therefore, an innocent user may be framed or a malicious user may be harboured.

Jiguo Li et.al (2017) [5] proposed a method, organically integrate outsourced-ABE (OABE) with PEKS and present a novel cryptographic paradigm called outsourced attribute-based encryption scheme with keyword search function (KSF-OABE). In this system, when the user wants to outsource his sensitive information to the public cloud, he encrypts the sensitive data under an attribute set and builds indexes of keywords. As a result, the users can decrypt the ciphertext only if their access policies satisfy the corresponding attributes. Outsourced ABE (OABE) with fine-grained access control system can largely reduce the computation cost for users who want to access encrypted data stored in cloud by outsourcing the heavy computation to cloud service provider.

IV) EXISTING METHODOLOGIES

A. Security and data protection in IoT with Cloud technologies.

Virtual devices provide many benefits in field of scalability and flexibility. Considering different security issues at a different step of transferring data from devices to the Cloud and vice-versa, following architecture shows the architecture for integration of IoT and Cloud.

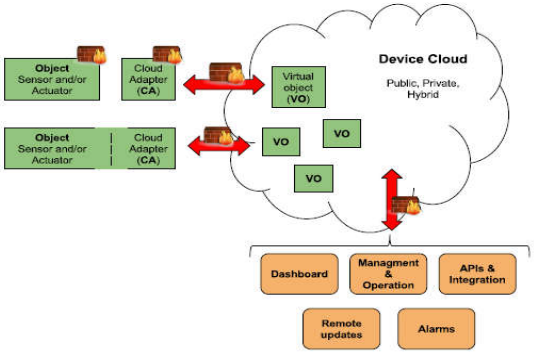

Fig.1. Device-Cloud architecture with virtual devices

The device-cloud architecture is complex which comprises of many interactions which leads to many points that should be secured. Devices should be securely paired to cloud adapter each physical device should be securely mapped to its virtualized entity; communication from device to gateway should be protected; communication from gateway to the cloud should be protected; data in the cloud should be kept in privacy; users should be authenticated in the cloud and their access rights
should be defined.

B. Data Distribution Systems in Mobile Cloud Computing.

Data distribution system consist of three main network entities namely, the cloud, the data owner and the data consumer. The data owner is a mobile user who stores his private data in the cloud and allows the data consumer to access his private data from the cloud. The cloud is an entity that provides storage services and is responsible to help the data owner to distribute the private data to the data consumer. The data consumer is an entity who first gets data access permission from the data owner.

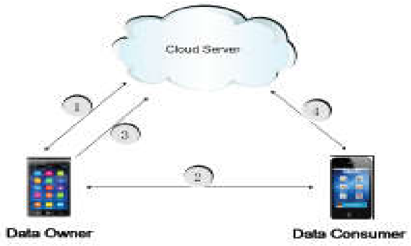

Fig 2. System Model of Data Distribution System

The proposed new type-based proxy re-encryption to design a secure and efficient data distribution system in MCC (Mobile cloud computing). A TB-PRE is single-hop unidirectional scheme consists of the following algorithms: Setup(1k), KeyGen(param, i), ReKeyGen(ski,pkj,t), Enc(pki,t,m), ReEnc(rki→j,t,Ci), Dec(ski,Ci). For efficiency, a secure symmetric encryption, e.g., AES is employed to encrypt the data under a uniformly and randomly chosen secret key for each data category, and the TB-PRE scheme is then used to encrypt the symmetric secret key. Namely, all the files in each category are encrypted under a unique symmetric secret key, and a TB-PRE ciphertext of the symmetric secret key is associated with the data category.

C. Identity-Based Data Outsourcing with Comprehensive Auditing in Clouds.

An IBDO system consists of five polynomial time computable algorithms/protocols, that is, Setup, Regst, Dlgtn, IBDOsc, and Audit. It is challenging to achieve both proxy data outsourcing and comprehensive auditing functionalities in IBDO. At a first glance, it seems that if the file-owner has delegated her outsourcing rights to some proxy, then the authorized proxy can simply employ the existing PDP/PoR schemes for processing and outsourcing files. In proposed IBDO system, to delegate outsourcing rights to a proxy, the file-owner signs a dedicated warrant for the proxy. The warrant may specify who can outsource which kind of files during what time on behalf of the owner, and so on. When a file is processed, it is partitioned into blocks, so as to generate metadata for each block individually. The warrant should be embedded into every metadata, to characterize that the metadata are generated by the authorized proxy. During the execution of integrity and origin auditing protocol, except the aggregate file blocks, the auditor also requests the aggregate metadata and the signed warrant. Both the aggregate metadata and signed warrant should be audited, in this way to conclude that the file is intact and is indeed outsourced by the one as specified in the warrant.

D. NPP: A New Privacy-Aware Public Auditing Scheme for Cloud Data Sharing.

System model contains four entities: cloud, TPA, trusted private key generator (PKG), and group users. The cloud has powerful storage space and computing capacity, and provides services (e.g., datastorage, datasharing, etc.) for group users. The TPA can verify the integrity of the shared data on behalf of the group users. The PKG generates the system public parameters and group key pair for group users. The group users include two types of users: GMs (Group Managers) and ordinary members. To achieve integrity checking of the shared data in the cloud, NPP is expected to the following design objectives: Public auditing, authorized auditing, Identity privacy, Nonframeability, Support data traceability and recoverability, Support group dynamics. The Group dynamics include two aspects. One is that GMs can easily join or leave the group; the other is that new users can be easily added into the group and misbehaved users can be efficiently excluded from the group. There are two kinds of threats related to share data integrity. One is that external attackers might corrupt the shared data in the cloud, so that group users can no longer access the correct data. The other is that the cloud may corrupt or delete the shared data due to the hardware/software faults or human errors.

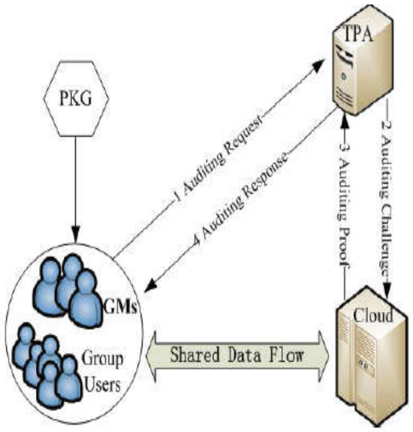

Fig 3. The system model of NPP.

E.Outsourced Attribute-Based Encryption with Keyword Search Function for Cloud Storage.

The system architecture for KSF-OABE scheme is shown as Fig. 4, which involves trusted authority centre which is responsible for the initialization of system parameters, and generation of attribute private keys. Key Generation Cloud Service Provider is a participant that supplies outsourcing computing service for TA by completing the costly key generation tasks allocated by TA.

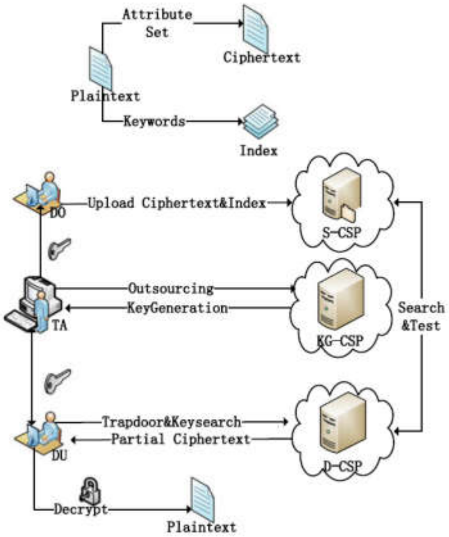

Fig4. Systems Architecture.

Storage-Cloud Service Provider is a participant that supplies outsourcing data storage service for users who want to share file in cloud. Data Owner intends to upload and share his data files on the cloud storage system in a secure way. The encrypted ciphertext will be shared with intended receivers whose access structure will be satisfied by attribute set embedded in ciphertext, responsibility of DO is to generate indexes for some keywords and upload encrypted data with the indexes.

V) V) ANALYSIS AND DISCUSSION

Security and the data protection in IoT architecture provide security at each level. Provides flexibility and scalability and will allow provision of security needs at design level. The integration of smart devices and data services to internet has led to new security requirements that use new adaptive decisions like secure association via data protection and depersonalization to reliable authentication and authorization [1].

Practical data distribution system in mobile cloud computing, which does not involve any trusted third party and provides several useful properties including data privacy, data integrity, data authentication, dynamic data modifications and deletions, as well as fine-grained access control. Efficient of secure type-based proxy re-encryption scheme, Merkle hash tree, as well as the BLS signature to ensure the security [2].

Scheme allows file-owner to delegate outsourcing capability to proxies. Only the authorized proxy can process and outsource the file on behalf of the file-owner. The identity-based feature and the comprehensive auditing feature make our scheme advantageous over existing PDP/PoR schemes. Security analyses and experimental results show that the proposed scheme is secure and has comparable performance as the SW scheme [3].

The public auditing scheme NPP has the lowest computation cost compared with Knox and PDM. Specifically, In terms of computation cost, NPP significantly out performs Knox and PDM. As for communication cost, although the cost of NPP is a bit more than that of Knox, the additional overhead 63KB is small and acceptable compared to the size of shared data with 2GB [4].

A CP-ABE scheme that provides outsourcing key-issuing, decryption and keyword search function. This scheme is efficient since only need to download the partial decryption ciphertext corresponding to a specific keyword. In this scheme, the time-consuming pairing operation can be outsourced to the cloud service provider, while the slight operations can be done by users. Thus, the computation cost at both users and trusted authority sides is minimized. Furthermore, the scheme supports the function of keywords search which can greatly improve communication efficiency and further protect the security and privacy of users [5].

Existing Methodologies	**Advantages**	**Disadvantages**
Security and data protection in IoT	Reliable and secure transportation of the data	Limited processing and storage resources
Data Distribution Systems in Mobile Cloud Computing	The data owner can perform data modification and deletion operations Without any loss.	The computation overhead of our data distribution system
Identity-Based Data Outsourcing with Comprehensive Auditing in Clouds	The authorized proxy can process and outsource the file on behalf of the file-owner	Cloud server which is not fully trustable.
NPP: A New Privacy-Aware Public Auditing Scheme for Cloud Data Sharing.	A public auditor to audit the shared data without retrieving all data from the cloud	When the current data has been corrupted, users cannot recover the old data
Outsourced Attribute-Based Encryption scheme	The computation cost at both users and trusted authority sides is minimized	It is a time consuming method.

TABLE**1**: Pro and Cons of existing methodologies.

VI) PROPOSED METHODOLOGY

Multipurpose auditing unit in cloud service:

Proposed method focuses on multipurpose auditing while providing the cloud service to user. Cloud system encounters various types' of attacks, sometimes service providers could not focus on overall security of system, and proposed method can improve sender-receiver connection as well as can improve security features. Also this method intended to maintain recommendations and history of data shared on cloud. Proposed methodology states the presence of auditing unit in between the cloud and data owner and data consumer. Any cloud operation such as uploading, accessing will be monitored by the auditing unit.

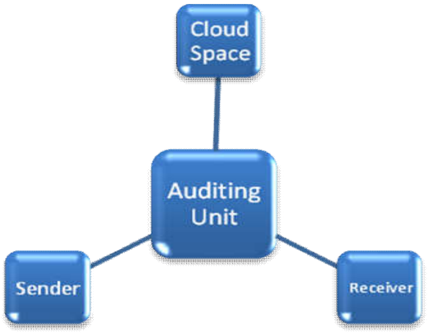

Fig. 1: Multipurpose auditing unit.

Data owner can directly upload data to cloud then the auditing unit will audit the sharing and after that if data consumer requests for access then auditing unit will follow the security measures as well as all previous recommendations to improve relationship and security. Proposed methodology aims in better and secure data sharing on cloud, modification and controlling can also be improved with effective use of auditing unit.

VII) OUTCOME AND POSSIBLE RESULT

This paper proposed multipurpose auditing methodology which not only aims for better sender receiver communication but also for improving security. Recommendations and history of communication can help to decide and manage the interaction more effectively. Provided quick access and restricting the access can be managed. Quick data sharing is possible if the receiver had communicated with sender. Various third party attacks can be restricted with layered security measures. Also limited storage capacity of cloud can also be improved with effective use of auditing unit. Overall improvement of efficiency in cloud service helps to build trust on cloud providers.

VIII) CONCLUSION

This paper focuses on multipurpose auditing unit which aims for better communication and security on cloud service. Many service providers' faces problem of trust on cloud service, secure and quick cloud useability can solve this problem. By providing more secured layered security measures and effective auditing proposed method aims to develop multipurpose cloud unit which helps to improve security and communication between sender and receiver.

IX) FUTURE SCOPE:

Future scope involves improving security measures and making communication secure and quicker. Storage space on cloud is also concerns of improvement. Provides flexibility and scalability and will allow provision of security needs at design level.

REFERENCES

[1] N. Kakanakov and M. Shopov, "Adaptive models for security and data protection in IoT with Cloud technologies", MIPRO, National Science Fund of Bulgaria, 2017.

[2] Jiang Zhang, Zhenfeng Zhang, and HuiGuo, "Towards Secure Data Distribution Systems in Mobile Cloud Computing", IEEE Transactions on Mobile Computing, 2016.

[3] Yujue Wang, Qianhong Wu, Bo Qin, Wenchang Shi Robert H. Deng, Jiankun Hu , "Identity-Based Data Outsourcing with Comprehensive Auditing in Clouds", IEEE TRANSACTIONS,2016.

[4]Anmin Fu, Shui Yu, Yuqing Zhang, Huaqun Wang, and Chanying Huang, "NPP: A New Privacy-Aware Public Auditing Scheme for Cloud Data Sharing with Group Users", IEEE Transactions on Big Data, 2016.

[5]Jiguo Li, Xiaonan Lin, Yichen Zhang, and Jinguang Han, "KSF-OABE: Outsourced Attribute-Based Encryption with Keyword Search Function for Cloud Storage", IEEE TRANSACTIONS ON SERVICES COMPUTING, 2017.