An Efficient Public Auditing Protocol and Privacy of data owners

Miss Divya M. Kantode Dr. Mrs R.D. Raut Dr. V. M. Thakare

Abstract--**Cloud data auditing about data packets consistency on cloud as well as DO and users identity discloser issues are the most focused concepts about cloud services. In this paper auditing protocol and privacy of the DO and users has been taken into consideration which resulted into a method which maintains the availability of data once it gets on cloud, also use of linked list effectively reduces the workload on servers also use of Merkle hash tree (MHT) helps to reduce verification computation complexity. Thus proposed method states the effective performance in maintaining the control on cloud data as well as prevents the identity of users which may prevent the system from cyber attacks.**

Keywords:- Cloud Services, Data Owner, Public Auditing Protocol, Cloud Services Providers, Security, Integrity.

I. INTRODUCTION

In the present digital era, cloud storage is widely used in many organizations; on demand service of cloud service provider satisfies the demand for cloud services. But the security concerns about data privacy and control must be maintained. Outsourcing and auditing the cloud data are the topics which are strongly under research [1]. Integrity of the data in the cloud cannot be effectively guaranteed due to the following reasons. First, due to users lose control of data under Cloud Computing, traditional cryptographic checking method cannot be directly used to protect data security. Therefore, the problem of verifying the integrity of the data in the cloud becomes even more challenging. Secondly, the cloud storage service, which often faces both software and hardware failure, may decide to hide the fact of data errors for the benefit of their own. Last but not the least; it can also saving money or storage space [2].

Apart from such cloud related problems IP trace-back is an effective solution to identify the sources of packets as well as the paths taken by the packets. For example, trace-back is useful in defending against Internet DoS attacks and integrity maintenance is achieved using effective IP trace-back [3]. As time goes by, the fast-growing data volumes make it hard for the sensors to store data due to their weak storage and computing resources. It becomes a problem that how to store these crowd-sensing data economically, as well as perform queries on it efficiently. Considering the flexible, on-demand and low-cost usage of cloud storage resources, the enterprises and individuals, i.e., data owners (DO), outsource their data to the cloud server.

Thus, the users can get the information of interest by asking the cloud service provider (CSP) for searching the outsourced data [4]. Many applications uses collected information from diverse devices via wireless networks have started to appear in our daily life, the concept of Internet of things has attracted a lot of attention as a key technology, in which the future society, numerous "things" with sensors are deployed and connected to networks, and data collected from these devices are used for a wide variety of innovative industrial applications [5]. The proposed methodology uses an auditing protocol which contributes in global and sampling verifications, sampling verification makes cloud data storage more secure. Proposed method improves the performance of the designed protocol, without introducing extra communication overhead. And a query answer authentication scheme based on the Merkle hash tree (MHT) helps to improve integrity of cloud services with maintaining autonomy of DO and users as per need. Method focuses on auditing cloud services and also protect the DO's identity. Internal nodes of MHT to sign, as well as the root node are taken into consideration thus verification computation complexity could be significantly reduced in the best case. Thus to improve cloud service experience of both CSP and users proposed method focuses on auditing data transfers and maintaining the DO's identity.

II. BACKGROUND

Numbers of organizations are accepting cloud computing but expecting reliable verification whether cloud service providers have stored their data securely. An efficient public auditing protocol with global and sampling block less verification as well as batch auditing, where data dynamics are substantially more efficiently supported than is the case with the state of the art with which computational and communication overheads can be reduced substantially [1]. The problem of ensuring the integrity of datastorage in cloud computing can be solved by reducing the burden of generating a constant amount of metadata

at the client side. By exploiting some good attributes of the bilinear group a simple and efficient audit service for public verification of untrusted and outsourced storage can be done, which can be important for achieving wide spread deployment of cloud computing. Extensive security and performance analysis shows efficiency and security [2]. IP trace-back plays an important role in cyber investigation processes, where the sources and the traversed paths of packets need to be identified. It has a wide range of applications, including network forensics, security auditing, network fault diagnosis, and performance testing. While this makes the trace-back service more accessible, regulating access to trace-back service in a cloud-based architecture becomes an important issue. Objective is to prevent illegitimate users from requesting trace-back information for malicious intention [3]. In cloud service over crowd-sensing data, the data owner (DO) publishes the sensing data through the cloud server, so that the user can obtain the information of interest on demand. But the cloud service providers (CSP) are often untrustworthy. The privacy and security concerns emerge over the authenticity of the query answer and the leakage of the DO identity. To solve these issues, a cooperative query answer authentication scheme, based on the ring signature, the Merkle hash tree (MHT) and the non- repudiable service protocol. Non-repudiation protocol during the transmission of query answer and verification object (VO) to protect trading behaviour between the CSP and users [4]. The concept of Internet of things (IoT) has attracted attention as a

key technology for realizing future industrial society. In the future society, numerous "things" with sensors are deployed and connected to networks, and data industrial applications. Focus on data collection for location-based authentication system as an application of industrial IoT. The authentication system uses ambient information, which is collected from the devices as unique information at a certain place and a certain time. However, since the ambient information changes continuously, it is required to collect it in real time from multipoint. The key point is to regulate the network performance for data collection by considering the application requirements. Since the location-based authentication system can be used in many situations and has large expensively [5].

This paper introduces an efficient public auditing protocol which helps to improve privacy of data owners this proposed theory is organizes 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** Conclude this review paper. **Section IX** discusses Future Scope

III. PREVIOUS WORK DONE

JianShen et.al (2016) [1] have proposed an efficient public auditing protocol which contributes in global and sampling verifications, guarantee of sampling verification makes Owners believe that the cloud has properly stored their data. Proposed method improves the performance of the designed protocol, without introducing extra communication overhead and cost effective in performing single auditing task and batch auditing tasks.

TAN Shuang et.al (2014) [2] have proposed efficient auditing scheme for checking the integrity of data stored in the cloud. Schemes try to reduce the cost of the initialization phase and improve the performance at initial level. The challenge-response protocol in proposed work further provides a high efficiency during initializing the checking protocol. Scheme tries to reduce the storage burden of the verifier by introducing the improved index- hash table. Extensive security and performance analysis shows that the proposed scheme is highly efficient and secure.

Long Chengy et.al (2016) [3] have proposed a methodology which handles access control problem in the cloud-based trace-back architecture. A framework for authentication in cloud-based IP trace back, named FACT is developed, which enhances traditional authentication protocols such as the password-based scheme in cloud-based trace-back. The proposed method not only ensures that the user (or entity) requesting for trace-back service is an actual recipient of the packets to be traced, but also adapts well to the limited marking space in IP header.

Liangmin Wang (2015) [4] have proposed a cooperative query answer authentication scheme, based on the ring signature, the Merkle hash tree (MHT) and the non- reputable service protocol. The proposed scheme could not only verify the query answer but also protect the DO's identity. First, it picks up the internal nodes of MHT to sign, as well as the root node. Thus, the verification computation complexity could be significantly reduced in the best case. Then it improves an existing ring signature to sign the selected nodes. The security and performance analysis prove the security and feasibility of the proposed scheme.

Yuichi Kawamoto et.al (2016) [5] have proposed scheme towards Secure Data Distribution Systems. Mobile Cloud Computing is a novel data collection method for authentication systems. This is an efficient data collection method considering the requirements from the authentication system. This method dynamically controls its parameters according to the surrounding environment and the requirements from the application side

The proposed methodology uses design an efficient public

auditing protocol. Proposed method contributes in global and sampling verifications; guarantee of sampling verification makes owners believe that the cloud has properly stored their data.

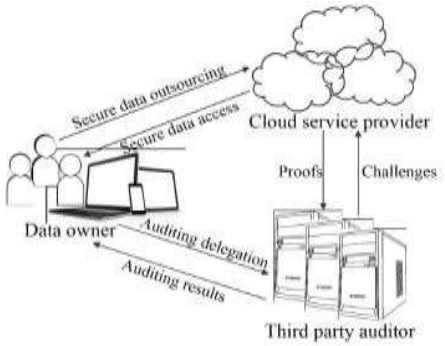

Fig. 1: The system model

Efficient data dynamics with a novel dynamic structure are provided in the protocol and various auditing properties are supported by the protocol. Proposed method improves the performance of the designed protocol, without introducing extra communication overhead

VI. EXISTING METHODOLOGY

4.1 An Efficient Public Auditing Protocol

Proposed method improves cloud services performance. Proposed protocol is less expensive both in performing single auditing task and batch auditing tasks. verifying the integrity of the data in the cloud becomes even more challenging. Secondly, the cloud storage service, which often faces both software and hardware failure, may decide to hide the fact of data errors for the benefit of their own. Last but not the least; it can also saving money or storage space. The proposed public checking scheme is a collection of four polynomial-time algorithms KeyGen, SigGen, GenProof, CheckProof, which works to implement a simple and efficient auditing scheme for checking the integrity of data stored in the cloud. Stateless verification, Unbounded use of queries, Public verification, Support dynamic operation are the different services are maintained while implementing the proposed auditing scheme.

4.2 Method for Checking the Integrity of Data in the Cloud

Service platform for the internet promises to provide wide range of services including security and integrity. One of the biggest concerns is that the integrity of the data in the cloud cannot be effectively guaranteed due to the following reasons. First, due to users lose control of data under Cloud Computing, traditional cryptographic checking method cannot be directly used to 0protect data security. Therefore, the problem of

4.3 Framework for Authentication in Cloud- based IP Traceback

IP trace-back is an effective solution to identify the sources of packets as well as the paths taken by the packets. It is mainly motivated by the need to trace back network intruders or

attackers with spoofed IP addresses, for attribution as well as attack defence and mitigation. For example, trace-back is useful in defending against Internet DoS attacks. It also assists in mitigating attack effects. DoS attacks can be mitigated if they are first detected, then traced back to their origins, and finally blocked at entry points. IP trace-back can be used for a wide range of while many different IP trace-back approaches have been proposed and importance of IP tracking is accepted worldwide.

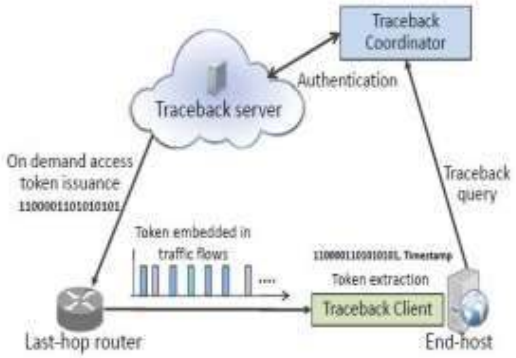

Fig. 2: Framework overview for temporal token-based authentication in cloud-based trace back

In this paper, first present a novel cloud-based trace-back architecture, which handles increasingly available cloud infrastructures for logging traffic digests, in order to implement forensic trace-back. Proposed cloud-based trace-back simplifies the trace-back processing and makes trace-back service more accessible.

4.4 Cooperative Query Answer Authentication Scheme

In this paper, the proposed methodology attends such a cloud service system based on crowd-sensing data comes into being. There are three entities in the system: DO, user, and CSP. The crowd-sensing data is provided by many data owners. More users and CSP would join in the system for utilizing these data. Due to the collaborative operation among DO, user and CSP, multiple security and privacy problems have to be taken into consideration. The security and privacy requirements include: In demand for privacy preservation, the DO tends to

outsource the data anonymously. Thus in some specific application scenarios, the DO is also called as the anonymous data provider. The CSP provides the paid service for users. Hence in pursuit of commercial profits, the CSP requires that users cannot deny having been served by the CSP if the CSP has sent the proper query answers to the users. Since the CSP is often untrustworthy, the users desire urgently for an efficient query answer authentication scheme.

4.5 Effectively Collecting Data of Location-for Location-Based Authentication in Internet of Things

Now a day's many kinds of applications using collected information from diverse devices via wireless networks have started to appear in our daily life, the concept of Internet of things has attracted a lot of attention as a key technology, in which the future society, numerous "things" with sensors are deployed and connected to networks.

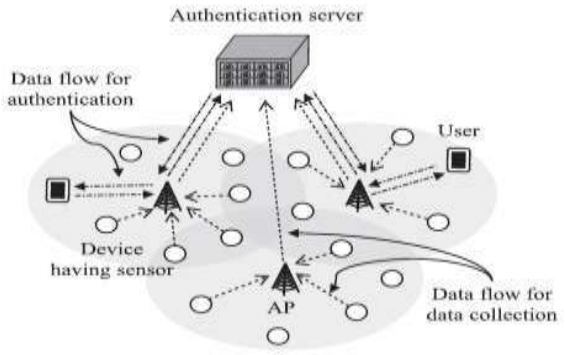

Fig. 3: Example of the system architecture.

The proposed method is an efficient data collection method considering the requirements from the authentication system. This method is focus on data collection for location-based authentication system as an application of industrial IoT. The authentication system uses ambient information, which is collected from the devices as unique information at a certain place and a certain time. The key point is to regulate the network performance for data collection by considering the application requirements. Since the location-based authentication system can be used in many situations and has large expensively, the proposed work is considered to significantly contribute to the future industrial IoT society.

IV. ANALYSIS AND DISCUSSION

Public auditing protocol with a novel dynamic structure composed of a doubly linked info table and a location array. Effective performance improvement when compared with the state of the art, **protocol** performs better both in terms of efficient dynamic support makes protocol perform better both in terms of efficient dynamic support and reduced overhead [1].
Efficient results on comparison of generating metadata under different file's size and different remote data integrity checking schemes. Maintain the auditing time under different remote data integrity checking schemes and different sectors in a block [2].
Metrics for comparison helps to analyse the performance of the method. Number of marked packets for token delivery: the number of packets marked by the last-hop router for delivering an access token to an end-host. Token delivery delay: the time elapsed from a preamble sent by the last-hop router to the last marked packet received by the end-host when delivering an access token [3].

A cooperative query answer authentication scheme which applies to cloud system not only verify the trustiness, completeness, authenticity of the query answers efficiently, but also satisfy DO's requirement for anonymity and guarantee non-repudiation service between CSP and user[4].

To improve the performance of the system, some parameters for the network control were adjusted dynamically according to requirements from the system and the surrounding network environment. Which improves accuracy of the location based authentication system [5].

Existing Methodologies	Advantages	Disadvantages
Efficient Public Auditing Protocol	Once data are outsourced to cloud, it will not remain unchanged during the whole period of the cloud.	Computational cost of the protocol is still relatively high.
Checking Integrity of Data in the Cloud	It Support efficient dynamic operations on data blocks, e.g. modification, insertion, deletion.	Problem of verifying integrity of the data in the cloud becomes even more challenging.
Authentication in Cloud	Little computational	Long detection cycle; high

Cooperative Query Answer Authentication Scheme	It provides higher efficiency and lowe r communication cost	If the signature is not trusted, then hash computation is wasted.
Collecting Data for the Location- for	Data collection method achieves to improve	Limitation network resources, it
the Location-Based Authentication in Internet of Things	accuracy of the location-based authentication system efficiently	collect data from numerous devices in real time.

TABLE 1: Pro and Cons of existing methodologies

VI. PROPOSED METHDOLOGY

Auditing Protocol can maintain identity of DO. The proposed method of maintaining privacy and auditing protocol can be categorised into two phases, first as auditing cloud and second about identity of DO. Auditing protocols can be divided into two phases: the setup and verification of contain which will be sending to cloud phase. Various existing protocols such asKeyGen, Filepro2C, and Filepro2T can be used for auditing the information. And in second phase proposed method maintains the identity of the DO. The Merkle hash tree and the cooperative query answer authentication scheme are used to maintain privacy about DO Furthermore, the proposed scheme employs the non-repudiation protocol uring the transmission of query answer and verification object (VO) to protect trading behaviour between the CSP and users which helps to reduce untrustworthy of CSP. Representation of proposed method is as follows:

Fig. 4: Auditing Protocol with maintaining identity

VII. OUTCOME AND POSSIBLE RESULT

This paper proposes collective functionality of public auditing protocol and an authentication scheme. Structure composed of a doubly linked info table and hash tree helps to improve efficiency of executing protocols. Dynamic support and reduction in managing overhead with managing DO's requirement for anonymity and guarantee non-repudiation service between CSP and user is proposed. Basic challenges such as batch auditing block less verification and lazy update can be managed effectively.

VIII. CONCLUSION

Future work involves minimisation in experimental comparison which improves analysis study.Maintaining cost efficiency and maintaining and improving the privacy of user can be treated as scope for future work.

REFERENCE

1] Jian Shen, Jun Shen, Xiaofeng Chen, Senior Member IEEE, Xinyi Huang, Willy Susilo, "An Efficient Public Auditing Protocol with Novel Dynamic Structure for Cloud Data", IEEE Transactions on Information Forensics and Security, 2016

[2] TAN Shuang, TAN Lin, LI Xiaoling, JIA Yan, "AEfficientMethod for Checking the Integrity of Data in the Cloud", China Communications, September 2014

[3] Long Chengy, Dinil Mon Divakarany, Aloysius Wooi Kiak Angz, Wee Yong Limy, Vrizlynn L. L. Thingy, "FACT: A Framework for Authentication in Cloud-based IP Traceback", IEEE Transactions on Information Forensics and Security, 2016

[4] Liangmin Wang, Member, IEEE Qingqing Xie, and Hong Zhong, "Cooperative Query Answer Authentication Scheme over Anonymous Sensing Data", IEEE ACCESS, VOL. 14, NO. 8, AUGUST2015.

[5] Yuichi Kawamoto, Yoshitaka Shimizu, Atsushi Takahara, "Effectively Collecting Data for the Location-Based Authentication in Internet of Things", IEEE SYSTEMS JOURNAL, 201