PRIVACY PRESERVING PROTOCOLS IN CLOUD COMPUTING: A SURVEY

Keirolona Safana Seles[1], Rex Fiona[2]
[1]Department of Computer Sciences Technology, Karunya University, Coimbatore, India, keirolona94@gmail.com
[2]Assistant Professor, Department of Computer Sciences Technology, Karunya University, Coimbatore, India, jrexfiona@gmail.com

Abstract
Cloud services are convenient for the users without any infrastructure limitations. When the data is been accessed by more than one users there comes the problem of privacy for the data. Users can outsource the data to cloud and they can use the computational power, storage, bandwidth and the software that are been shared. The user data should be in the form of encrypted type before it is been outsourced to cloud. This paper provides a survey of various protocols that address the privacy issue in cloud computing. The survey is classified into two main categories of the protocols, data sharing protocols and privacy preserving protocols.

Keywords
Authentication, Cloud Computing, Privacy Preserving, Shared Authority, User Privacy

I. INTRODUCTION

Cloud Computing is a environment that provides services for the users. The services are given by the third party and accessed over the internet. There is no cost for the purpose of installing hardware or a software. Cloud computing differs in three aspects and they are, it is on-demand, it is public/private and it is managed. The services are classified into three types namely Software as a Service(SaaS), Platform as a Service(PaaS) and Infrastructure as a Service(IaaS). These services are used for the purpose of deploying the clouds as public, private and hybrid clouds. Services delivered to the internal users are given from the business data center and it is called as the private cloud services. The model preserves the management, security control and also it provides versatility and greater convenience that are common to all local data centers. A third party provider is the one who delivers the cloud services in the internet and it is done in public cloud model. Public cloud services are on-demand. The users can pay only for the total CPU cycles, bandwidth and the storage they consume.

The third cloud model is a hybrid cloud model which is a combination of both public cloud services and private cloud services. Public cloud is used for bursting workloads when the company tries to execute mission critical workloads that scale as on-demand. The main aim of hybrid cloud is to create an automated, unified and scalable environment that has the advantage of public cloud infrastructure that provides control on mission critical-data. Cloud environment provides the sharing of data for the users that has been outsourced over the internet. In this way, the information is been shared between users and security issue arise. To overcome the security problem, protocol is been developed and that preserves the privacy of the data. The description of the paper is as follows. Section 2 describes about the privacy preservation; section 3 provides the study of privacy preserving protocols and section 4 concludes the paper.

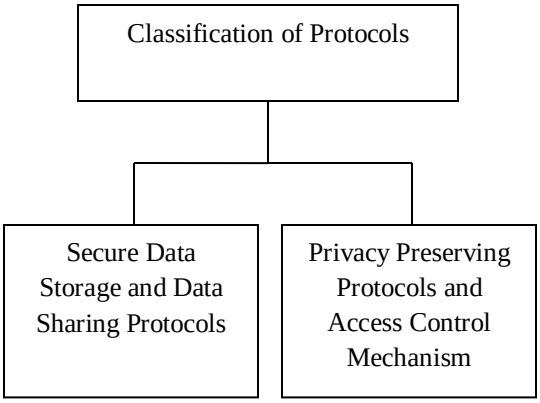
II. PRIVACY PRESERVING

The main aspect of privacy is to secure the data during the action of sharing the confidential information over the internet. In cloud computing, the data is been outsourced over the network for the purpose of sharing the information with all the users over the internet. There is no privacy for the data that is been shared. Therefore, privacy preserving becomes the important concept in cloud computing. The process of preserving the user's identity and data is very important in the cloud environment. Privacy preservation has been increased due to the growth and usage of cloud computing. But still, the process of privacy preserving needs attention to overcome the issue of privacy. By solving all the privacy criteria would bring success for the privacy issue in cloud computing. When a particular user is in the need for the other user's data that has been outsourced in the cloud server at this time, the access request reveals the privacy of the user without the data access permission for the requested data from the cloud. To increase the business benefits users try to access and also share the data among themselves that produces a security and privacy challenges in the cloud storage system.

III. PRIVACY PRESERVING METHODS

Privacy preserving issues have been solved by many methods and the study provides a brief overview about the approach. The privacy of the data should be preserved at all the time and it is very important task of preserving the data. Therefore the job takes place in two tracks, the data's privacy should be preserved and also preserving the privacy while the third party assures the data correctness. The goal is to address the sensitive access of the user that is related to the privacy at the time of sharing data in cloud environment. It is very important to design a humanistic scheme based on the security issue at the same time to achieve the access control to data and privacy preserving work.

Fig.1 Classification of Protocols



3.1 Secure Data Storage:

Secure data storage mentions about the computing processes and technologies manually and automated that are used to provide stored data integrity and security. Secure data storage applies to the information that are stored in the computer portable devices like hard drives and USB, also in online/cloud, network based storage area network (SAN) or network attached storage (NAS). Data storage is been secured by the following ways:

- Encryption of Data.
- Each storage device has the access control mechanism.
- Preserving the data from viruses, threats and worms.
- Physical storage device and security infrastructure.
- Layered storage security architecture is enforced and implemented.

3.2 Data Sharing Protocols:

Data sharing is a process in which the data outsourced can be used by the research scholars for other investigation. Duplication of data files is possible in cloud storage. Many security policies have been considered by many institutions, funding agencies and publication due to openness and transparency.

3.3 Privacy Preserving Protocols:

Privacy is a state in which the data is been isolated from the unauthorized users. A brief description about the protocols that are used to preserve the privacy of the data, that is been shared over the network. Privacy in cloud computing means the data should be preserved from all the interference. Degree if intimacy is been maintained between the privacy of the data. Protecting the information of the user in the cloud environment is privacy. The violation of privacy creates lot of troubles among the cloud users.

I. TYPES OF SECURE DATA STORAGE AND DATA SHARING PROTOCOLS

Secure data storage and data sharing protocols are divided into:

1.1 Data Sharing With Anonymous ID Assignment Using AIDA Algorithm

An anonymous ID assignment is based on data sharing algorithm (AIDA) for the purpose of distributed and multiparty oriented cloud computing systems. An integer data sharing algorithm is been implemented on top of the data mining operation of secure sum data and the iterations are been taken into account for anonymous assignment.

The iterations are unbounded and variable [1]. Newton's identities and Strum's theorem is used in the concept of data mining and the distributed solution of polynomials over the finite fields boost the scalability of the algorithm. Also the representation of Markov chain is used to determine the statistics of the iterations that are required.

1.2 Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud

The main goal of Mona is to share the data with other users through the un-trusted cloud server and also supports dynamic group interaction. A new user can decrypt the data files without contacting the data owner. The revocation of the user is provided by the revocation list without updating the secret keys for the remaining users [2]. The concept of access control is used in group to ensure that user in the particular group can use the cloud resources and at the same time the identities are revealed only by the manager of the group.

4.3 Sharing Cloud Services: User Authentication For Social Enhancement Of Home Networking

Cloud services has used Zero Knowledge Proof based authentication scheme. User-centric approach is been used in social-home based networks to allow the personalized content sharing and network based services that are sophisticated through TCP/IP infrastructure [3]. Decentralized interactions are kept secured by trusted third party. An authentication framework is been represented. The decision of ZKP techniques for authentication protocol allows the user to share the data with simple username and password authentication. The authenticating device has the username/password which sets the security level as high and cracking the authentication is restricted for the trusted home environment.

4.4 Privacy Preserving Policy Based Content Sharing In Public Clouds

A broadcast group key management (BGKM) is a policy based content sharing used to improve the weakness in public clouds when symmetric key cryptosystem is used. BGKM also realizes when the user needs to utilize the public key cryptography and it can derive the symmetric keys dynamically during the process of decryption in the receiver side. Concurrently, attribute based access control mechanism is to decrypt the contents if the identity of the user satisfy the content of providers policies [4]. The fine-grained algorithm uses access control vector for the purpose of assigning secrets for the users based on the attributes of the identity. Also it allows the users to derive the symmetric key that is based on the secrets and on other public information. This BGKM has an great advantage for adding and revoking users and for updating the access control policies.

4.5 Toward Secure And Dependable Storage Services In Cloud Computing

Homomorphism token and distributed erasure-coded data has been introduced in distributed storage integrity auditing mechanism to improve the security and storage services that are dependable in cloud environment. The auditing of cloud storage is done by the users by using lightweight communication overloads and with computational cost. The result ensures the correctness of cloud storage and locating the error present in the given data in a faster manner. When the data files are stored dynamically in the cloud storage then the scheme helps data operations that are dynamically outsourced. The scheme [5] is against modification attack on data and colluding attacks in the server.

4.6 Ensuring distributed accountability for data sharing in cloud

In cloud environment, ensuring the distributed accountability for the sharing of data in cloud is decentralized framework that is used to track the user's data usage in cloud computing. An object centered approach [6] is proposed for enabling the logging mechanism for the user's policies and data. A mobile and dynamic object is been created by Java Archives (JAR). This mechanism is executed to strengthen the user's data control and it is efficient and effective.

II. TYPES OF PRIVACY PRESERVING PROTOCOLS AND ACCESS CONTROL MECHANISMS

Privacy preserving protocols are classified into:

2.1 Enhancing Privacy and Dynamic Federation in IdM for Consumer Cloud Computing

Managing the privacy in cloud environment has become an important issue and it is to be solved in order to overcome the attacks. It also improves the trust of the user by accessing the CE devices in the cloud environment. Regarding the legislation, it is different for each country and national legislation for the privacy. The privacy policy identified is suitable for all the countries. Privacy-aware IdM [7] architectures are designed in such a way that it has various guidelines for the cloud services, cloud services are minimization of customer's personal data, preserving the sensitive user's data, maximization of user control, allowing user's choice. Data usage limitation and also the feedback provided with privacy for the customer. Regarding the privacy, the ever is ensured with the cloud services and they can share the digital content without using any true identity for the users. The privacy of the user is monitored by enabling the trace-off using a framework and personalizing the degree of the privacy in different type of services. Therefore, the module designed improves the awareness of user's identity by using tools for the purpose of monitoring and a personal cloud to audit the data sharing.

2.2 A Privacy-Preserving Remote Data Integrity Checking Protocol with Data Dynamics and Public Verifiability

The technology that is crucial in cloud environment is checking the integrity of remote data. Data dynamics is provided by focusing on many works and the type of protocol is verifiable to the user. The protocols which have been proposed before supports the feature of both with the help of the third party auditor. The protocol [8] which is proposed does not need any third party auditor. The protocol also has an additional advantage that it does not leak any confidential information of the user to the third party. The security and correctness of the protocol is analyzed formally. The proposed system has a good and better performance is proved in the theoretical analysis.

2.3 An Efficient Privacy-Preserving Publish-Subscribe Service Scheme for Cloud Computing

A novel computing paradigm is given by cloud environment for the purpose of storing the information of the enterprises and the storage of data is in transparent manner. Since the data storage is transparent, security and privacy of the information is increased. By using the Zero-Knowledge Proof and homomorphic cryptography the privacy-preserving scheme [9] is been published in cloud. This achieves the authentication, integrity, confidentiality and privacy of the data stored. The evaluation and analysis of performance and security are validated. The proposed scheme verifies the data stored in the cloud and achieves the integrity, confidentiality and authentication by using privacy preserving scheme for cloud PS services. The enhanced system will achieve the aggregation of message from multiple publishers between multiple cloud service providers in a secure manner without any information.

2.4 A Novel Privacy Preserving Location-Based Service Protocol with Secret Circular Shift for -NN Search

Location-based service (LBS) is growing up in the coming years for the mobile devices and it is also an emerging technology for the cloud computing paradigm. The privacy of the user becomes a significant task in LSB. When the query result is accurate then the [10] privacy-preserving LSB becomes a successful one. The protocol has a public-key homomorphic cryptosystem and a space filling curve. The Points of Interest (POIs) is first marked on a map in order to a circular structure. The circular structure is aided of with a Moore curve. Secret circular shifts are performed by homomorphism of Paillier cryptosystems which is related to the information of point of interest that is stored in the server side. When the user queries for the information the LSB providers has no knowledge about the location of the user because the number of shifts are been encrypted. A secret circular shift is pre-described before each query and also the protocol prevents the information from the correlation attack. It also supports the scenario of multi-user access. The robustness of the protocol is similar to the encryption of one time pad scheme. The result value is very near to the secrecy and no trusted third party is involved.

Table 1. Comparison of Protocols

Property	ABE	SLE	TLE	SAPA
Cryptosystem	Asymmetric	Symmetric	Symmetric	Symmetric
Secure attribute based group communication	Yes	Yes	Yes	Yes
Efficient revocation	No	Yes	Yes	Yes
Delegation of access control	No	No	No	Yes

5.5 TMACS: A Robust and Verifiable Threshold Multi-Authority Access Control System in Public Cloud Storage

The tool that guarantee the control over the data by cryptographic method in public cloud storage is considered as the Attribute based Encryption (ABE). The older version of ABE considers only the authority of single person maintained in the whole set of attributes that can bring a bottle-neck problem which affects both the performance and the security of the data. The schemes that are proposed as multi-authority maintains the data in a disjoint attribute subsets, separated by multiple authorities. The problem of single-point bottleneck remains the same. The paper is about a threshold multi-authority CP-ABE control access scheme in public cloud storage is been implemented. In TMACS [11], the multiple authorities manage the attribute set jointly in a uniform manner. The master key is been shared between the multiple authorities and at the same time the authorized user can generate the secret key for further interaction among the authorities. The performance and security analysis of TMACS states that it is verifiable secure and the authorities are been compromised.

5.6 Privacy-Preserving Public Auditing for Secure Cloud Storage

In cloud environment, the users can outsource the data over the network and also can use on-demand high quality applications. The services can be shared from the pool of data storage that is configurable to the resources without any maintenance for the data storage that is local. The user who outsourced the data over the cloud network does not have all the permission to share the data stored in the cloud storage. In this, the integrity of the data can be lost and it becomes a drawback in the cloud storage. The user can use the cloud storage data in a local manner, means that the user has no control over the integrity of the data. Therefore, the public auditing is done for the cloud storage system [12]. The auditing of the data stored in the cloud storage is done by third party auditor. The process of auditing reduces the vulnerabilities in the privacy of the data and there is no worry for the user.

5.7 Secure Overlay Cloud Storage with Access Control and Assured Deletion

The data is outsourced to the third-party storage in order to minimize the cost for managing the data. The data that is outsourced to the third-party should be secure and so, [13] FADE is implemented. FADE is a secure cloud storage overlaid on the system which is fine-grained, policy based access control and assures the deletion of files. The outsourced file has access control policy and the files deleted are unrecoverable. The security goal is achieved in FADE which are self-maintained with the key managers of third-party clouds.

5.8 Towards Temporal Access Control in Cloud Computing

The most significant security mechanism in cloud storage is access control. The encrypted data and the policies provided for the access control is integrated by the data owners to make the Attribute-based access control scheme a flexible one. The privileges and policies of the data user has enforced and specified to explore the attributes temporally in cloud environment. The paper provides the [14] temporal access control scheme for encryption of data used on cloud services using comparison cryptographic integer concurrently performing re-encryption mechanism with is proxy-based method. In this way, the access control of the data is kept secured and the results improve the performance of the scheme.

5.9 Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds

Anonymous authentication is been supported in cloud for secure data storage, a new decentralized access control scheme has been proposed. In this scheme, the identity of the user is verified and authenticated before storing the

data in cloud storage. The scheme also adds the access control only to the authorized user for the purpose of decrypting the data. The prevention of the attacks such as replay, modification is also done. Also it supports in creating, reading and modifying the data stored in cloud. The process of revocation is also done. The authentication scheme is robust and decentralized [15], while the other control access schemes are centralized. The overheads of communication, computation and storage are comparable with the centralized approaches.

III. CONCLUSION

The paper concludes that the privacy-preserving access of authority sharing achieves the accessing of data in cloud environment. The integrity and the confidentiality of the data is been achieved by authentication. The anonymity of the data is also been achieved because the values are wrapped during the process of transmission. The access request is made anonymous so that the privacy of the user has enhanced. The access request is informed privately to the cloud server about the desires of the access request. The correlation of the session is prevented by the identifiers of the session by the forward security. It indicates that the scheme is possibly applied for privacy preservation in cloud applications.

REFERENCES

[1] L.A. Dunning and R. Kresman, (Feb 2013) "Privacy Preserving Data Sharing with Anonymous ID Assignment," IEEE Trans. Information Forensics and Security, 402-413.
[2] X. Liu, Y. Zhang, B. Wang, and J. Yan, (June 2013) "Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud," IEEE Trans. Parallel and Distributed Systems,1182-1191.
[3] S. Grzonkowski and P.M. Corcoran, (Aug 2011) "Sharing Cloud Services: User Authentication for Social Enhancement of Home Networking," IEEE Trans. Consumer Electronics, 1424-1432.
[4] M. Nabeel, N. Shang and E. Bertino, (Nov 2013) "Privacy Preserving Policy Based Content Sharing in Public Clouds," IEEE Trans. Knowledge and Data Eng., 2602-2614.
[5] C. Wang, Q. Wang, K. Ren, N. Cao and W. Lou, (June 2012) "Toward Secure and Dependable Storage Services in Cloud Computing," IEEE Trans. Services Computing, 220-232.
[6] S. Sundareswaran, A.C. Squicciarini, and D. Lin, (Aug 2012) "Ensuring Distributed Accountability for Data Sharing in the Cloud," IEEE Trans. Dependable and Secure Computing, 556-568.
[7] F. Almenares, P. Arias, D. Diaz-Sanchez, R. Sanchez and A. Marin (Dec 2012) "Enhancing Privacy and Dynamic Federation in IdM for Consumer Cloud Computing" IEEE Trans. Consumer Electronics.
[8] H. Zhuo, S. Zhong, and N. Yu, (Sept 2011) "A Privacy-Preserving Remote Data Integrity Checking Protocol with Data Dynamics and Public Verifiability," IEEE Trans. Knowledge and Data Eng., 1432-1437.
[9] Y. Xiao, C. Lin, Y. Jiang, X. Chu and F. Liu, (Dec 2010) "An Efficient Privacy-Preserving Publish-Subscribe Service Scheme for Cloud Computing," Proc. IEEE GLOBECOM '10.
[10] I.T. Lien, Y.H. Lin, J.R. Shieh, and J.L. Wu, (June 2013) "A Novel Privacy Preserving Location-Based Service Protocol with Secret Circular Shift for K-NN Search," IEEE Trans. Information Forensics and Security, 863-873.
[11] Wei Li, Kaiping Xue, Yingjie Xue and Jianan Hong, (May 2016) "TMACS: A Robust and Verifiable Threshold Multi-Authority Access Control System in Public Cloud Storage," IEEE Trans. Parallel and Distributed Systems.
[12]Cong Wang, Sherman S.M. Chow, Qian Wang, Kui Ren and Wenjing Lou, (Feb 2013) "Privacy Preserving Public Auditing For Secure Cloud Storage," IEEE Trans. Computers, 362-375.
[13] Y. Tang, P.C. Lee, J.C.S. Lui, and R. Perlman, (Nov/Dec 2012) "Secure Overlay Cloud Storage with Access Control and Assured Deletion," IEEE Trans. Dependable and Secure Computing, vol. 9, 903-916.
[14] Y. Zhu, H. Hu, G. Ahn, D. Huang, and S. Wang, (Mar 2012) "Towards Temporal Access Control in Cloud Computing," Proc. IEEE INFOCOM, 2576-2580.
[15] S. Ruj, M. Stojmenovic, and A. Nayak, (Feb 2014) "Decentralized Access Control with Anonymous Authentication for Securing Data in Clouds," IEEE Trans. Parallel and Distributed Systems, vol. 25, 384-394.