International Journal of Advanced Information Science and Technology (IJAIST) ISSN: 2319:2682
Vol.3, No.8, August 2014 DOI:10.15693/ijaist/2014.v3i8.28-33

Survey Of Cloud Security And Privacy Preservation

Arumugam.K
Research Scholar/PG & Research Department of Computer Science, Government Arts College, Coimbatore, INDIA.

Sumathi.P
Assistant Professor/PG & Research Department of Computer Science,Government Arts College, Coimbatore, INDIA.

***Abstract*—The growth of cloud computing infrastructure carries innovative ways to make and control computing system by means of the flexibility present with virtualization technologies. However, security is the most important issue that occurs in the cloud environment. In the cloud, the data may reside in somedata centres where some of the data centre may leak the data. The cloud resource users will seek for cloud resources with the secured data management. Some of the cloud users may prefer a privacy enhanced data management while they are sharing their personal data over the public cloud. The focal point of this paper is security concerned privacy enhancement of data in the cloud environment.In this work, the various security and privacy enhancement methods that are evaluated in the previous works have been analyzed and discussed. This would serve as the promising analysis to know about the strengthening approach used for resolving the privacy issues and the security threats occurred in the cloud resources.**

Index terms:Cloud computing, Virtualization, Privacy enhancement, Security management.

I. INTRODUCTION

The cloud providers enable authenticated and authorized users to access the shared data in the cloud and it allows user to store their data in the public cloud. The user can access or process the data whenever they require it, without consideration of the data location. Cloud computing is a platform for sharing resources exclusive of the knowledge of the infrastructure and can formulate it possible to access the applications and itconnects data from wherever at any time. Cloud environment offers the four types of cloud. Those are Public cloud, Private cloud, Hybrid cloud andCommunity cloud.

National Institute of Standards and Technology (NIST) defines [8] cloud type present in the cloud computing environment offersthree types of services based on various requirement from the users. Those are Software as a service (SaaS), Platform as a service (PaaS), and Infrastructure as a service (IaaS).Among these services IaaS is the lowest level layer which will provide the infrastructure service to the users like storage, processing capacity, etc., PaaS is the middle layer service which will provide the platform related services to the users like front end and back end for running the programs. Moreover, it is used to provide the complete platform for a user to run his application. SaaS is a topmost layer in the cloud computing environment which will provide the completely developed application to the users like software packages, games etc.

In the cloud computing environment there are many of the issues are present. Those are identity management of cloud users without collision, providing security over data sensitive applications, privacy preserving for the users those who do not want to reveal their identity and maintaining life cycle control over the outsourced data. The outsourced data are nothing but which are shared publicly among multiple users.

Cloud computing environment provides many advantages to the user, still user doesn't prefer to get into the cloud. Because the many of the analysis shows that first most important issue present in the cloud computing is security threats. Due to the security threat the original data of users may colluded.

The second important issue in cloud computing is privacy preservation for the users. Cloud computing provides flexible and scalable access to users without need to maintain the large amount of server in their place. In that case privacy is the main concern predicted by the user's where they do not want to reveal their identity information to the users.

A. Types of security attacks possible in the cloud

When the user gets into the cloud to share their personal data, they should concentrate on security threats that are possible to attack their data. The cloud service provider should give their trust value to the users in order to gain their service at the most level. The possible types of security attacks present in the cloud computing environment are SQL injection attacks, Cross site scripting attacks, Man in the middle attack, Denial of service attack, and Sniffer attack.

B. Issues that privacy preservation in cloud

The privacy preservation of the cloud user is the most important role of the service providers where the most confidential information of users is stored in the cloud. The users do not want to share their information with others where their data are shared publicly among the cloud. Some of the issues,leads cloud service providers to attain privacy is insufficient user control, Information disclosure, unauthorized second storage, uncontrolled data proliferation, and Dynamic provision

II.RELATED WORKS

In this Survey relative mechanisms and the methods which are employed earlier to attain a security and privacy are discussed. And also the advantages and disadvantages of each technique are discussed. According to the survey of the earlier mechanism, it finds that the current system implemented has more advantages.

C.Wang, Q.Wang, K.Ren, N.Cao and W.Lou, [3] focuses on achieving secured and dependable storage in the cloud environment where the data are outsourced publicly in distributed manner. The effective way of achieving secured cloud storage is analysed. To overcome this problem a flexible distributed storage integrity auditing mechanism is proposed. The framework of this work consists of three components, namely user, cloud server (CS), Third party auditor (TPA). Cloud provider is responsible for providing significant storage space to the cloud user for storing their data. TPA is responsible for providing trusted access. This work evaluates dynamic data verification in order to provide secure dependable data storage.

Dynamic data verification is nothing but ensuring the correctness of data where, the user accessing the data and modifying it in the local server as well as in the global servers. The erasure correcting code is used in this work in order to replicate the data files redundantly across multiple servers. The data modification is done dynamically in order to assure the data integrity in the dynamic nature of cloud service providers. The mechanism used in this work ensures the following properties:

- Storage Correctness: Data integrity checking is done periodically to ensure the data are stored in the cloud appropriately.
- Fast Localization: Error occurred on the server and data collusion is detected effectively.
- Dynamic data support: Providing same level access permission given to the users at the start in the case of dynamic data changes also.
- Dependability:Minimizing of data errors and server failure effects.
- Light weight: Ensures storage correctness check with minimum overhead.

The method proposed in this work [3] is highly efficient and resilient to Byzantine attacks. However the redundant copies present in multiple servers may lead to the memory unavailability and high cost. Data integrity cannot be performed accurately due to the dynamic nature of behaviour at multiple copies stored in multiple servers.

The efficiency of the data sensitive application can be improved by data redundancy. However, data redundancy in the cloud may lead to the cost effective problems as described in [3] where the clouds are the pay per use model. N.Cao, [7] proposed a secure cloud storage service to overcome the reliability problem with optimal performance. In order to maintain the data integrity, the data owner has to maintain his state in the online itself where it will increase the burden of data owners. This problem is overcome by an exact repair solution where none of the data need to be generated during the process. This reliable and secure data storage service design is proposed to attain a following performance metric:

Availability: The data should be capable accessing the data from anywhere at any time.

Reliability: The malfunction happened in the server should be repaired by the other healthy servers.

Security: Data integrity is checked periodically to provide the promising data confidentiality

Offline Data Owner: The data owners need not to be in the online state for checking data error correction after outsourcing their data.

Efficiency: This approach is effective for data owners, data user and cloud servers with the minimized storage, communication and computation cost.

The LT-Codes based secure and reliable cloud storage service (LTCS) approach used in this work is implemented to provide an effective data storage service for data owner and data users. This method consists of several stages. Those areSetup, Data outsourcing, Data retrieval, Integrity check and Data repair. This mechanism overcomes the drawbacks present in previous method called erasure based coding method. This method is used to achieve less storage cost, and fast data retrieval.However, it concerns only about maintaining the data integrity in all redundant copies of data and assuring the data security effectively.

The possibility of redundant copy exists in the cloud environment may degrade the performance of cloud service providers. The data integrity checking is the most important factor which is used to maintain the consistent copy of data's across many cloud servers [7]. Retrieving entire data check data integrity periodically with the data owner is the burden to the users which may degrade the performance. TPA [3] mechanism is used to reduce the burden of data owner from checking data integration. TPA cannot be trusted who may leak out the sensitive information about users.

C.Wang, S.M.Chow, Q.Wang, K.Ren and W.Lou,[4]evaluated a privacy-concerned method witha public auditing mechanism which ensures zero-knowledge leakageby using the cloud information. Cryptographic measures are not only enough to provide security over the cloud data centres where large amount of datais shared publicly.Because the data stored in the cloud are highly dynamic and that are outsourced publicly with the other users to share their knowledge.To overcome these problems in this paper TPA concept is introduced. Homomorphic authenticator and random masking assures that TPA could not gain any knowledge during the process of auditing. It enablesTPA to access the data from the cloud storage to share the confidential data of users. This auditing scheme works based on two phases and four algorithms. Those algorithms are KeyGen, SigGen, Genproof and VerifyProof. In these first two algorithms reside in initialization phase and second two algorithms reside in audit phase.In the initialization phase Meta data for verification is generated by using an initialized security parameter.In the auditing phase, auditing is done in order to verify the correctness of data.These experiments are done in Amazon Elastic Cloud(EC2) to prove the effects of this mechanism.

Most of the organization starts to store their data in a cloud environment to share it among their staff members effectively. It will give an economic feasibility and flexibility, access to the group members. In previous works the privacy and security issues are discussed only in single user data sharing whereas it cannot be applied to the multiple users. In the group sharing of data there may be the issues introduced like introducing new staff members and revoking already existing users.

X.Liu, Y.Zhang, B.Wang, and J.Yan, [10] introduces a method for sharing data in a multi owner manner. This approach is used to achieve a privacy preservation of data and identity of data owner information. This method imposes a concept of sharing data among the multiple clouds with the different characteristics by any user in the group. Sharing data in a multiple cloud by any user instead of data owner will leads to a security threats in the untrusted cloud. This problem is overcome by using the approach, namely SecureMulti Owner Data Sharing (MONA). The goal of this work is to achieve access control, data confidentiality, anonymity, traceability and efficiency. The dynamic data sharing among the dynamic groups is attained by combiningthe group signature concept and dynamic broadcast encryption technique. In this approach, the group manager is allowed to compute the revocation parameter and move them to the public cloud for sharing the data. The computation overhead occurred when the user computing the revocation parameter individually can reduce it considerably.

User revocation is supported efficiently by enabling the group manager to compute the revocation parameter. Thus MONA approach support efficient user revocation and new user joining. User revocation is done by allowing the group manager to create a revocation parameter without updating the private keys of every user. It leads to the satisfaction of security requirement and efficiency.

In the public cloud computing environment, the cloud service providers are responsible for storing and managing the data shared by the user. Every operation like user revocation [10], auditing the data integrity [3],[4] will be controlled by the cloud service providers. Due to the untrusted nature of cloud service providers, the data stored in the remote areas like cloud environment by the user may be modified or corrupted.

H.Wang, [5] concentrate on enabling user to controlthe security over remote data. Remote data possession is the most complexproblem to be achieved by the users when the user is in the outside areas from remote area like being in prison, being in the battlefield etc., In this case proxy provable data possession has to be provided. To overcome this problem, the Proxy Provable Data Possession (PPDP) protocol is evaluated in this work. This PPDP protocol consists of a six phases. Those are SetUp, TagGen, SignVerify, CheckTag, GenProof, and CheckProof.In PPDP design,CheckTag is added to each and every client those who are accessing the data in order to prevent from the malicious client. The performance of this protocol is analysed by using the two parameters, namely communication overhead and computation overhead. This PPDP protocol is proved to be a secured one to provide an efficient data possession checking of remote data by users. This approach uses the public verifiability concept to prove that data in not changes by the unauthorized persons. By using this approach anyone can use this method to prove their correctness.

Y.Zhu, G.Ahn, H.Hu, S.Yau, H.G.An, and C.J.Hu [11] proposed a novel dynamic audit service for the untrusted and outsourced data from the cloud. The main goal of this approach is to provide a data integrity check when the data are shared to the untrusted cloud. This work tries to achieve the security metric given in the following list to check the performance of this approach. Those security metrics arePublic auditability, Dynamic operation, Timely detection, Effective forensic, Lightweight.

The architecture of this work consists of four entities, namely data owner, Cloud service providers, Third party public auditor and authorized application. The audit service in this approach comprises of three processes. Those areTag Generation, Periodic sampling audit, Audit for dynamic operation.The performance of TPA and storage service providers is enhanced by introducing the concept of periodic sampling audit mechanism.

The virtualized nature of cloud computing will cause many of the security attacks in the cloud. The data will be gathered in the one place of cloud for effective management where there are lots of possibleDDoS attacks like Html and Xml are available.It will create the threat to the cloud environment which will also affect the cloud service consumers. D.Asha and R.Chitra [1] proposed an intrusion detection system in the Virtual machines in order to prevent it from the DDoS attacks.

This is achieved by evaluating the Service oriented system architecture in the cloud virtual machines. Before transmitting any of the data, the Simple Object Access Protocol (SOAP) protocol will be transmitted between the client and the service provider. Soap messages are sent via the Xdetectors. It is used to capture the DDoS attacks like Html and Xml attacks.In this technique DDoS filtering technique is used to capture the DDoS attacks that are traversed throughout the cloud service providers. In this filtering technique the SOAP message will be transmitted towards the service oriented traceback the architectureof the proxy server. It will create an identity mark on the original client file which is to be retrieved. If any of the files other than the identity marked files are received, then it will be rejected. Only the files with the source identification mark will be accepted. This method concentrates to provide a security layer over an application in the cloud storage, whereas previous approaches only concentrates on providing security over application interfaces.

B.Wang, B.Liand H. Li, [2] Proposedanother public auditing mechanism by analyzing the work of C.Wang, S.M.Chow, Q.Wang, K.Ren and W.Lou [4] where the data correctness are checked by public auditing mechanism. In

this work new public auditing mechanism is proposed, namely Oruta (One ring to rule them all).It ensures a privacy of data as well as user identity information.This approach hides the user information from the third party public auditor. Also, it proves the correctness and unforgeability when the public auditing is done.

Correctness: Data Integrity checking after processing the retrieved data

Unfoegeability: Only user from the group can access the data with signature

Compared with [4], this work handles the preservation of identity privacy of users effectively.The framework of this approach consists of three entities, namely the cloud server, TPA and the users. There are two types of users are present, according to the access permission of data. Those are original user (owner of the outsourced data) and group users. The original user is responsible for controlling the flow of data in the cloud. TPA is responsible for correctness verification of data through auditing. To overcome this problems Homomorphic Authenticable Ring Structures (HARS) scheme is used in this work. This work consists of three algorithms, namelyKeyGen, RingSign and RingVerify.These algorithms are used forachieving the privacy-preserving auditing. Still, these approaches don't concentrate about the attaining data integrity in the dynamically grouped users.

L.Ferretti, M.Colajanni, andM.Marchetti, [6] proposed a novel approach to provide a secured data access over a distributed concurrent database. Cloud environment is the virtualized environment where the data are shared publicly. Security threat occurs in the cloud environment when data owners' placing a sensitive data on the cloud providers which may cause the collision of data. In this work secureDBaas framework is designed to allow multiple clients who act independently to connect with the untrusted Dbaas without any intermediate servers.

SecureDBass consists of sensitive information which will enable the client to access it in a secured manner. The information present in the SecureDBaas is plaintext data, encrypted data, metadata, and encrypted metadata. SecureDBaas supplies three confidentiality attributes. Those are columns, multi-column and database.

Column: Each column in the database will be encrypted with unique encryption keys which are not used by other columns when the SQL statements are operated.

Multi-Column: When the joint operation is invoked by the SQL command this concept will be used. It is used to encrypt the two columns with the same encryption key.

Database: It is invoked when multiple columns are involved in the operation. The special encryption key will generate and that will share among the multiple columns in order to encrypt it.

To manage these encrypted databases efficiently secureDBaas will generate a Meta data which will contain necessary information to manage the SQL statement. Two types of Metadata are used by the SecureDBaas. Those areDatabase Meta data, Table Meta data. This approach can support any type of platform.

S.Ruj, M.Stojmenovic and A.Nayak, [9] propose a novel approach to provide anauthentication to the appropriate users, which will avoid a security conflict. In the centralized network it will be complex to manage the data present in the data storage. The burden of the network to handle data access and operations will be increased in the case of centralized environment. In order to avoid the burden of cloud service providers, the decentralized access control is introduced in this work which enables user to access their data from any servers.

The users with sensitive data will not want to reveal their information to the public cloud. For example, in medical field none of the patients would want to reveal their information. To overcome this problem anonymous authentication is provided for all data that are stored in the cloud. The data anonymization is achieved by proposing a scheme called Attribute based encryption and Attribute based signature. This scheme consists of a four phases. Those are System initialization, key generation and distribution by KDC's, Encryption and Decryption.The effective signature is created to provide an authentication to all the users. This ABS scheme performs in the following 6 steps. Those are System Initialization, User Registration, KDC Setup, Attribute Generation, Sign, and Verify.

All the works discussed above clearly show the different methodologies used to provide a privacy and security prevention for the cloud data users as well as for cloud data owners. All of the above discussed technologies are meant to be solved various types of security threats and also possible ways to provide privacy.

Analysis of Quality of service Routing Mechanisms are summarized in table 1.

S. No	TITLE	AUTHOR	METHOD	ADVANTAGES	DISADVANTAGES
1	Towards Secure and Dependable StorageServices in Cloud Computing	Cong Wang,Qian Wang,KuiRen, Ning Caoand Wenjing Lou	Distributed storage integrity auditing mechanism	• Dynamic data verification • Resilient against Byzantine failure and malicious data modification	• High redundant copies are present which may cause high memory occupation • Data Integrity is not

				attack	achieved
2	LT Codes-based Secure and ReliableCloud Storage Service	Ning Cao, Shucheng Yu, Zhenyu Yang, Wenjing Lou, Y. Thomas Hou	LT codes-based cloud storage service	• Efficient and fast data retrieval • Less storage cost	• Need to retrieve entire data to check data integrity • TPA is not trustable
3	Privacy-Preserving Public Auditingfor Secure Cloud Storage	Cong Wang,Sherman S.M. Chow, Qian Wang,KuiRenand Wenjing Lou	Privacy-preserving public Auditing mechanism	• Assures zero knowledge leakage • Better privacy preservation	• Group access of data cannot be secured
4	Mona: Secure Multi-Owner Data Sharingfor Dynamic Groups in the Cloud	Xuefeng Liu, Yuqing Zhang,Boyang Wang, and Jingbo Yan	Secure multi owner data sharing scheme	• Better security over group of users • User revocation is handled effectively	• Remote data integrity is not considered
5	Proxy Provable DataPossession in Public Clouds	Huaqun Wang	Proxy provable data possession	• Efficient user controlled data management	• Public verifiability may causes intruders collision on data
6	Dynamic Audit Services forOutsourced Storages in Clouds	Yan Zhu,Gail-JoonAhn,Hongxin Hu, Stephen S. Yau, Ho G. An, and Chang-Jun Hu	Dynamic audit services	• Less communication overhead • Less memory storage	• Highly causes from security attacks
7	Securing cloud from ddos attacks using intrusion detection system in virtual machine	D Asha and R Chitra	DDoS Filtering technique	• Prevention from security threats over application in cloud services	• If Http is considered an relying protocol then the web browser should also be in Http format
8	Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud	Boyang Wang,Baochun Liand Hui Li	ORUTA	• User identity information are hided from TPA	• Data freshness is not concentrated
9	Distributed, Concurrent, and Independent Access to Encrypted Cloud Databases.	Luca Ferretti, Michele Colajanni, and MircoMarchetti	Novel architecture that integrates cloud database services with data confidentiality	• Guaranteed data confidentiality	• High computational cost
10	Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds	SushmitaRuj, Milos Stojmenovic,and AmiyaNayak	Decentralized access control scheme	• Less computation, communication and storage overhead	• Publicly stored access policies and attributed which may cause collision attack

III. CONCLUSION

Cloud computing is an emerged technology used by the many consumers to store and share the data publicly where the security and privacy is the main concern. In this paper theoretical analysis of various kinds of security threats and various issues that affect the privacy preservation of the data users are analysed.Also the methodologies used to solve the security threats occurred in the real time cloud environment is discussed. The ways to solve the issues that are preventing the privacy preservation arealso analysed. The detail explanation of these techniques is briefed and also summarizes the advantages with parameters of the different techniques in cloud computing environment. Various types of possible ways to overcome these issues are discussed and different types cryptographic mechanisms that are used to resolve the security threats are analysed. At the end of this survey, conclude that effective cryptographic mechanism is

proposed to provide the effective prevention from the security attacks as well as better privacy preservation for the data owners and data consumers.

REFERENCES

[1] Asha.D and R.Chitra, "Securing Cloud from DDoS attacks using Intrusion Detection System in Virtual Machine", International Journal of Research in Engineering& Advanced Technology, Volume1, Issue 1, March, 2013, ISBN: 978-1-4244-5727-4

[2] Boyang Wang,Baochun Liand Hui Li, "Oruta: Privacy-Preserving Public Auditingfor Shared Data in the Cloud", IEEE transactions on cloud computing, vol. 2, no. 1, January-March 2014, ISSN: 2159-6182

[3] Cong Wang, Qian Wang, KuiRen, Ning Cao and Wenjing Lou, "Towards Secure and Dependable Storage Services in Cloud Computing", IEEE Transactions on Cloud Computing Volume: 5 , Issue: 2, April-June 2012, ISSN: 1939-1374

[4] Cong Wang, Sherman S.M. Chow, Qian Wang, KuRen and Wenjing Lou, "Privacy-Preserving Public Auditing for Secure Cloud Storage", IEEE transactions on computers, vol. 62, no. 2, February 2013, ISSN: 0018-9340

[5] Huaqun Wang, "Proxy Provable Data Possession in Public Clouds", IEEE Transactions On Services Computing, Vol. 6, No. 4, October-December 2013, ISSN: 1939-1374

[6] Luca Ferretti, Michele Colajanni, and MircoMarchetti, "Distributed, Concurrent, and Independent Access to Encrypted Cloud Databases", IEEE Transactions On Parallel And Distributed Systems, Vol. 25, No. 2, February 2014, ISSN: 1045-9219

[7] Ning Cao, Shucheng Yu,Zhenyu Yang, Wenjing Lou and Y. Thomas Hou, "LT Codes-based Secure and ReliableCloud Storage Service", Proceedings of IEEE Infocom, 2012, ISSN: 0743-166X

[8] Peter Mell and Timothy grance, "The NIST Definition of cloud computing", National Institute of Standards and Technology, Information technology laboratory, 2011

[9] SushmitaRuj, Milos Stojmenovic and AmiyaNayak, "Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds", IEEE Transactions On Parallel And Distributed Systems, Vol. 25, No. 2, February 2014, ISSN: 1045-9219

[10] Xuefeng Liu, Yuqing Zhang, Boyang Wang, and Jingbo Yan, "Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud", IEEE transactions on parallel and distributed systems, vol. 24, no. 6, June 2013, ISSN: 1045-9219

[11] Yan Zhu, Gail-JoonAhn, Hongxin Hu, Stephen S. Yau, Ho G. An, and Chang-Jun Hu, "Dynamic Audit Services for Outsourced Storages in Clouds", IEEE Transactions On Services Computing, Vol. 6, No. 2, April-June 2013, ISSN: 1939-1374

Authors Profile

Dr.P.Sumathi is working as an Assistant Professor in the Department of Computer Science, Government Arts College, and Coimbatore. She did her PhD in the area of Grid Computing in Bharathiar University. She has done her M.Phil in the area of Software Engineering in Mother Teresa Women's University. She did her MCA degree at Kongu Engineering College, Perundurai. She has published many national and International journals. She has about seventeen years of teaching and research experience. Her research interests include Data Mining, Distributed Computing and Software Engineering.

K.Arumugam is pursuing his PhD in Computer Science, Government Arts College, and Coimbatore. He has done his MPhil in the area of Network Security in Alagappa University, Karaikudi. He did his MCA degree at Anna University of Technology, Coimbatore. His research interests include Computer Networks, Network Security and Cloud Computing.