A Survey on Cloud Data Security Methods and Future Directions

Srividhya. S.T[1], Rexshana. S.K[2], Charulatha. T[3], Sivaramakrishnan[4]

[1,2,3]UG Student, Department of Computer Science KPR Institute of Engineering and Technology, Arasur, Coimbatore, India
[4]Assistant Professor, Department of Computer Science KPR Institute of Engineering and Technology, Arasur, Coimbatore, India

---***---

Abstract:- *Cloud computing is a new paradigm that provides on-demand services to its users over Internet. The services include storage, software and applications. Despite the advantages of cloud computing, cloud adaption is not wide due to several security concerns. As the user stores the data at an unknown remote location, he/ she don't have physical possession of data. Hence, several security risks arise. Integrity, privacy and availability are the three major security risks associated with cloud computing. In this paper, we presented a detailed survey of recent research works focused on cloud data integrity and highlighted the challenges, comparison and future research direction for the efficient deployment of a cloud storage system.*

Keywords: confidentiality, integrity, privacy, availability

I. INTRODUCTION

Cloud computing is now everywhere and is one of the most attractive areas of technology. The cloud was defined by the US NIST (National Standard Technology Institute). A cloud on a local network or on the Internet often refers to a remote network location, while computer resources such as server, data storage, application platform, networking, cloud data analytics. Cloud storage is used to remove the burden and associated complexities of hardware management. Cloud data integrity risk, confidentiality and availability. The cloud model has five key features, on-demand, broad network access, resource pooling, fast elasticity and measured services. There are three services: Iaas, Paas, Saas and four mode deployment. The cloud professionals save costs, reliability, manageability, strategic edge where cloud computing is downtime, security, vendor lock and limited control. Service denial, shared cloud computing services, loss of employee negligence data and inadequate data backup, phishing and social engineering attacks, system vulnerability are distributed security threats. Development of quantum computers requires the design of a signature scheme that can withstand quantum computer attacks, because the difficult problems in the traditional cryptography system can be solved in polynomial time, thus threatening the security of different encryption schemes [1]. The explosive increase in data places a heavy burden on users to store transparent data.

There are more companies and people like to save their data in the cloud. The data stored in the cloud would, however, be corrupted or lost using the remote integrity auditing scheme. We can verify that computing and its shared processing data and resources are provided to the user when required by using NIST, It is a model that enables on-demand access to resources that are shared and that data can be stored correctly or not quickly in the cloud [2]. It was defined as a network based with minimal administration effort. It offers the user various capabilities for storing and processing their data in the cloud server. It improves the storage constraint of local devices.

By using cloud support, multiple group users can share the code and can access, modify and execute it anywhere [3]. The cloud storage service provides the user with large storage space for outsourced data efficiently so that the user can put his data in the cloud to avoid heavy local hardware and software expenditures. This is convenient to share your data with the user. This is convenient for the user to share their data with each other through cloud services, as the cloud can be accessed wherever many cloud storage providers, such as drop box and Icloud, are presented as a primary service. It is difficult for the user to know if the data that is stored in the local storage is altered or not [4]. Cloud services can operate on a distributed network using a networking protocol and a standard internet connection. Cloud service provider provides cloud users with plenty of storage space, but still has some disadvantages such as missing data and data can be deleted [5]. The cloud computing model enables convenient computing of resources and network access on demand for network storage applications servers and services, for example. Data fixed and transaction costs can be reduced by using computer power. Cloud computing technology in many of its applications increases efficiency [6].

II. SECURITY ISSUES

i) Data breaches

ii) Weak identity, credential and access management

iii) Insecure interfaces and APIs

iv) System and application vulnerability

v) Account hijacking

vi) Malicious insiders

vii) Advanced persistent threats

viii) Data loss

ix) Insufficient due diligence

x) Abuse and nefarious use of cloud services

xi) Denial of service

xii) Shared technology issues

A. *Data Breaches*

Infringements of data can be caused by a variety of reasons, such as theft. It is an incident that has the potential to inform the unauthorized party of sensational data. One of the major security concerns in the literature is cloud computing data breaches.

B. *Weak Identity, Credential and Access Management*

To gain access to systems and cause havoc, hackers still use weak credentials and identity and access management policies. Security in any system is primarily concerned with ensuring that the right entity only has access to the authorized data in the authorized format at the authorized time and from the authorized place. In this regard, identity and access management (IAM) is of primary importance for Indian companies [15].

C. *Insecure Interfaces and API's*

Cloud computing providers expose a number of software interfaces or APIs that customers use to manage and interact with cloud services. This interface can provide, manage, orchestrate and monitor and must also be designed to protect against both accidental and malicious policy bypass attempts to bypass policy. In addition, organizations and third parties often rely on these interfaces to offer their customers added value services. This introduces complexity and increases the risk, so that organizations may have to distribute their credentials to third parties to enable their organization.

D. *System and Application Vulnerability*

Vulnerability in the application is a system error or weakness in an application that could be used to compromise the application's security. Once an attacker has found a fault or vulnerability in the application and determined how to access it, the attacker can exploit the vulnerability in the application to facilitate cyber crime. These crimes focus on the confidentiality, integrity or availability of the resources of an application, its creators and its users. Attackers typically use specific tools or methods to discover and compromise vulnerabilities in the application [17].

E. *Account Hijacking*

Account hijacking is a process whereby an individual's email account, computer account or other account connected to a computer device or service is hijacked by a hacker. It is an identity theft in which the hacker uses the information on the hijacked account to perform unauthorized activities. The hacker uses an email account to change the owner of the account and it is done by phishing, sending spoofed emails to the user, creating a password. In many hacking areas an email account is connected to the different online services of a user, such as social networks and financial accounts. The hacker uses these accounts to collect the personal information of the person and carry out financial transactions, create new accounts and ask the contacts of the account owner for money [11].

F. *Malicious Insiders*

The malicious threat to insiders is referred to as a threat to the security of an organization. These threats are usually a reason for employees or former employees and are also caused by others. The evil insider classifies threats as either malicious or accidental [12].

G. *Advanced Persistent Threats*

The APT is a long and targeted cyber attack, in which intruders can gain access to a network. The point of view of a persistent and advanced threat attack is used to monitor network activity and to steal data instead of damaging the network or organization [13].

H. *Data Loss*

Loss of data is an event that disperses, deletes and makes data unreadable by the user and any application or software. It only occurs if one or more data cannot be used or requested by the user. It is also referred to as data leakage [14].

I. *Insufficient Due Diligence*

Enterprise architects may not confirm whether their on- the- spot security controls will be effective in the cloud. Hiring agencies must also ensure that they choose a cloud provider that will not try to block them if the service is unsatisfactory or if the organization wants to use services from another provider. If the relationship needs to be terminated, the old CSP must be prepared and able to proceed securely and efficiently and delete the data of the organization.

J. *Abuse and Nefarious Use of Cloud Services*

This threat is due to relatively weak cloud computing registration systems. Anyone with a valid credit card can register and use the service in the cloud computing registration process. This facilitates anonymity, which allows spammers, malicious code writers and criminals to attack the system.

K. *Denial of Service*

DOS is an attack in which the user tries to prevent access to the services. Usually, the attacker sends messages to request the server to authenticate the request. The attacker has an invalid return address, so that the server cannot find the return address of the connection of the attacker. After the connection is closed, the attackers send multiple authentication messages with invalid address, so that this server will wait and start the process time and time again. When an attacker sends authentication authorization to the server, the server must wait before SHARED TECHNOLOGY ISSUES Cloud computing is a data sharing resource and has an underlying infrastructure component. If security requirements and protocols are not integrated into this infrastructure, vulnerability could occur [20].

L. *Shared Technology Issues*

The Cloud provides high- end scalability with its IaaS functionality by enabling users to access shared devices. A hypervisor can connect to other physical resources by a guest operating system. This puts the cloud at risk as the guest operating system even gains access to the unnecessary levels that affect other network systems.

III. LITERATURE REVIEW

Guangyangyang et al [1**]** the cloud storage vices are widely adopted by the diverse organization through this the user can be able to share their data's to others conveniently. This constraint identity can lead to the new problem that is the group member can modify the shared data maliciously without being identified. An efficient public auditing solutions is used to preserve the identity privacy and the identity traceability for group members.

WentingShen et al [2] has proposed an identity based data integrity auditing scheme for secure cloud storage it supports data sharing with sensitive information hiding. In this approach file stored in the cloud can be shared and used by others. It will used to protect the sensitive information of the file, the pros of this approach is it is able to execute efficiently besides the remote data integrity auditing. The sanitizer is used to sanitize the data blocks which it corresponds to the sensitive information of the file. It achieves the security and efficiency.

Shubhamsingh et al [3] cloud computing is an important storage platform. It provides many services to the users among them one of the important services is cloud storage which makes the data outsourcing a rising trend. But the integrity and seclusion is the major one associated with outsourced data, where users require that their data to be secure from any modification and unauthorized access. To verify that whether the data is modified or not, it increases the need of secure remote data auditing. It uses the auditing scheme based on vector commitment, identity based ring signature and group key agreement protocol on bilinear paring. It is more efficient and secure. It increases the need of secure remote data auditing, the ring signature scheme it requires the lesser time to compute signature for small group for message when it is compared to the group signature scheme. The performance analysis is more efficient in the small group.

Rajatsaxena et al [4] suggest the information from the paper is that it is better and efficient integrity verification technique for the data. The paillier homomorphic cryptography system with homomorphic tag and combinatorial batch codes. To demonstrate this the author has implemented an application based on hadoop, map reduce framework. This application has been tested based on various parameters where in the paillier homomorphic cryptography the key generation, encryption, decryption algorithms are used. This approach is suitable for cloud storage because of the efficiency of homomorphism tag and pro's of paillier homomorphic cryptography. It supports dynamic data operations with less overhead. The major pro's of the cloud service provider server does not require any additional data structure to manage data operation. It also provides better security in the Man in the Middle attack (MITM). This approach is not bounded with the disk I/O. The performance is more efficient and secure.

Yunxue Yan et al [5] has developed the quantum computer by making the traditional cloud storage program, data integrity verification protocol is not that much of safe. It is used to focus on security of user data privacy the file and user signature sending to the cloud service provider and third party access. It is used to improve the privacy of signature information which is in data calculation cloud storage .The lattice and bloom filter are the two methods used in this approach it integrity and it improves the utilization of cloud storage space.

Jens priifer et al [7] has design an institution attenuating the problem: the two layered certification scheme built around a private and nonprofit organization called cloud association. Where these association is governed by the both users and cloud service providers. It is shown that how this institution incentives providers to produce high data security and users with strong privacy preference to trust them and pay for their services. The cloud computing technologies offers to both producers and users, where lack of trust is a consequence of several interrelated problems stemming from asymmetric information betweennot only against the quantum computer attack but also based on realization of dynamic integrity and it improves the utilization of cloud storage space.

Jianxua et al [6] has proposed the WBAN'S (wireless body area network), is a kind of small networks with a wide range of application. The light weight privacy is used in this approach, it is efficient and can protect the integrity and confidentiality. This model is secure and efficient and it has great practicability in health care cyber physical system (cps). Sellers, buyers and third parties supporting their transactions.

Jianhongzhang qiaocui dong et al [8**]** has proposed cloud storage can make data users to store and access their files anytime from anywhere and with any device it requires large amount of computational cost it brings the heavy burden to the auditor in the multiuser per settings. To overcome this problem the efficient id based auditing protocol cloud data integrity id based cryptography. The public key infrastructure is more suitable to the large scale cloud storage system.

Authors	Data Integrity	Confidentiality / Privacy	Availability	TPA
Guangyangyang et al. [1]	✓	✓		✓
WentingShen et al. [2]	✓		✓	
Shubhamsinghsumila Thokchom et al [3]	✓			
RajatSaxena et al:[4]	✓	✓		
Yunxue Yana et al [5]	✓	✓		✓
Jain.Xu et al [6]		✓	✓	
Jens prufer et al [7]		✓	✓	
Jianhongzhang qiaocui dong et al [8]	✓	✓		✓
P. Ravi Kumar et al. [9]		✓		✓
Yung hu et al:. [10]	✓	✓		

P.Ravikumar et al [9] has explores many different varieties of data security issues in cloud computing. This cloud describes the cloud computing model such as deployment model and service delivery model. In some business of cloud computing data are exceptionally important data leaking or corruption can broke the confidence of the people and can lead to collapse of that business data. Cloud computing is used directly and indirectly in many business and if nay data has been broken in cloud that will affect the whole cloud computing as well as the company business.

Yung hu et al [10] has proposed cloud data auditing is extremely essential for securing cloud storage where it enables cloud users to verify the integrity of their out sourced data efficiently. The computation increases on both the cloud server and the verifier. Most of the data auditing scheme is public key infrastructure. The drawback of this protocol is it is mandatory to verify the validity of the public key certificates before using any public key. The implemented ID-CDIC protocol is very practical and adoptable.

IV. CONCLUSION

Cloud storage service becomes more prevalent and tremendous amount of data is being stored in cloud every day. Hence, it becomes highly essential to secure users data. In this study, we provided an overview of literature based on cloud data security, which emphasizes on the recent mechanisms to ensure cloud data integrity, confidentiality and availability. The comparison at a glance, on related works and aforementioned cloud data security issues addressed by recent researhers is summarized in tabular form at the end of Section 3. We can conclude that addressing the above mentioned parameters and mechanisms in a cloud environment would improve data security.

REFERENCES

1) Guang yang yang, "Enabling Public auditing for shared data in cloud storage supporting identity privacy and traceability ", The Journal of systems and software 113(2016)130-139.

2) Wenting Shen, "Enabling Identity-Based Integrity Auditing and Data", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 14, NO. 2

3) ShubhamsinghsumilaThokchom et al:"public integrity auditing for shared dynamic cloud data"6th International Conference on Smart Computing and Communications, ICSCC 2017, 7-8 December 2017,125 (2018) 698–708.

4) RajatSaxena et al:"Cloud Audit: A Data Integrity Verification Approach for Cloud computing", Twelfth International Multi-Conference on Information Processing-2016 (IMCIP-2016)89(2016) 142 – 151.

5) Yunxue Yana et al:"A dynamic integrity verification scheme of cloud storage data based on lattice and Bloom filter", journal of information security application 39(2018)10-18.

6) Jain.Xu et al: "Privacy-preserving data integrity verification by using lightweight streaming authenticated data structures for healthcare cyber physical system, Future Generation Computer Systems (2018).

7) Jens prufer et al;"Trusting privacy in the cloud," information economics and policy of (2018) doi.

8) Jianhongzhang qiaocui dong et al:" Efficient ID-based public auditing for the outsourced data in cloud storage", Information Sciences 343–344 (2016) 1–14.

9) P. Ravi Kumar et al: "Exploring Data Security Issues and Solutions in Cloud Computing", Procedia Computer Science 125 (2018).

10) Yung hu et al: "Identity-based Remote Data Integrity Checking with Perfect Data Privacy Preserving for Cloud Storage&quot;,1109/TIFS.2016.2615853, IEEE Transactions on Information Forensics and Security

11) https://www.techopedia.com/definition/24632/account-hijacking

12) https://searchsecurity.techtarget.com/definition/insider-threat

13) https://searchsecurity.techtarget.com/definition/advanced-persistent-threat-APT

14) https://www.techopedia.com/definition/29863/data-loss

15) https://www.sciencedirect.com/topics/computer-science/identity-and-access-management

16) https://cloudsecurityalliance.org/topthreats/csathreats/p

17) https://www.researchgate.net/.../324562008_Threats_and_Vulnerabilities_of_Cloud_ Computing

18) https://arxiv.org/ftp/arxiv/papers/1308/1308.5996.pdf

19) https://www.eci.com/blog/153-cloud-security-threats-in-the-cloud.html

20) https://downloads.cloudsecurityalliance.org/assets/research/top-threats/treacherous-12-top-threats.pdf.