International Journal of Modern Electronics and Communication Engineering (IJMECE) ISSN: 2321-2152
Volume No.-7, Issue No.-2, March, 2019

Review in Cloud Computing: Data Security

Mandeep Kaur1st
Computer Science
Sri Guru Granth Sahib World University
Fatehgarh Sahib, India
mandeepghangas358@gmail.com

Er. Usvir Kaur2nd
Computer Science
Sri Guru Granth Sahib World University
Fatehgarh Sahib, India
usvirkaur@gmail.com

Abstract: Cloud Computing is an archetype based on network and computer applications. Cloud computing is a model that authorize access to a shared pool of configurable computing resources for cloud users in an on-demand or pay-per-use, style. Cloud computing offers several benefits to users and organizations, in terms of capital expenditure and savings in operational expenditure. Despite the existence of such benefits there are some obstacles that place restrictions on the usage of cloud computing. Data security is a major issue that always considered. This paper will focus on data security challenges that are faced by users.

Keywords: Cloud Computing, Data Security, Models, Cloud Characteristics.

I. INTRODUCTION

Cloud computing is basically an internet based service provider, which allows the users to share resources like data, software, system on demand etc. The National Institute of Standards and Technology's (NIST) interpret cloud computing as, "Cloud Computing is an archetype for providing the suitable and when needed access to the internet, to a collective pool of programmable grids, storage, servers and software with minimal management effort or service provider interaction"[1][2]. It is composed of various essential characteristics, three service models and four deployment models.

II. ESSENTIAL CHARACTERSTICS

- **On-demand self service:** Cloud computing provides end user a simple, efficient and adaptable way to carry on the provided storage, services resources and computing power anytime, anywhere, according to their needs.[3]
- **Elasticity:** Elasticity in cloud computing means ability to provide scalable services to client. Elasticity of resources should be rapid that is scale up and down for the users for effective and efficient functioning of cloud environment. [4]
- **Resource pooling:** Cloud Service Provider serves many clients with same set of provisioned scalable services and resources. Cloud Service Provider(CSP) allocate infinite resources available to user by controlling and managing resources. According to cloud user's demand, resources are allocated and de-allocated. Purpose of resource pooling is to separate client response from actual handling of management of resources regardless of their location. [5,1]
- **Pay-per-use:** Based upon the services used and duration at which the resources are used by the user, the user has to pay for that particular service.[6]
- **Reliability:** Cloud computing creates data security, provides reserve of data, disaster retrieval and allows business stability, as records can be kept at numerous redundant locations on the cloud system. [7]

III. LAYERED STRUCTURE OF CLOUD COMPUTING

Cloud Computing can be viewed as collection of services presented as layered architecture, as shown in fig 1.

Software as a Service(Saas): This model is a software distribution model where software are hosted and managed by cloud provider, for the users over the network. By Saas users are not requried to purchase and install software on their devices, they can directy access from cloud. It consist majority of cloud service provider.SaaS model: Google Apps, Salesforce, Domain Consistence Server(DCS).[2]

SaaS (Software as a Service)
Paas (Platform as a Service)
Iaas (Infrastructure as a Service)

Fig. 1 Layered Structure of Cloud Computing

Platform as a Service (PaaS): Platform as a Service model is used for development, testing, running, customizing and deployment of applications. All these features can be carried out by user in a quick, simple and cost effective manner. Users of application need only to manage application, other management services, storage, networking and operating system are done by Cloud Service Provider(CSP).[8]

Infrastructure as a Service (Iaas): This is the cloud service model that deals with cloud infrastructure. IaaS providers manage virtualization. Servers, storage and networking. In IaaS model, a third party provider provides hardware, software, storage and other components of infrastructure and manages them according to user needs. IaaS models are: Amazon Web Services(AWS), Amazon Elastic Cloud Computing(EC2).[1]

IV. DEPLOYMENT MODEL

- **Public Cloud:** Public cloud is basically the normal cloud computing environment. In Public Cloud model the infrastructure and services are made available to the general public. In public cloud, a large number of clients are provided with resources, applications and services by the cloud service provider using same shared framework over internet.[13]
- **Private Cloud:** Private cloud is also called internal cloud of an organization. In private cloud, only the specified client can operate. It provides higher level of privacy and security, much higher control on cloud access control. It is executed within the organization firewall or corporate cloud.[11]
- **Hybrid Cloud:** Hybrid Cloud is a cloud computing environment which is combination of both public cloud and private cloud. Organization can control of their internally managed private cloud while count on public cloud when needed. It allows workload to move between private and public cloud.[10]
- **Community Cloud:** It is multi-user infrastructure that is shared by number of organization to carry out computing objectives. Objectives can be related to performance requirements such as host applications or related to regulatory compliance as audit. It is combination of public cloud and private cloud.[4]

V. DATA SECURITY CHALLENGES

With increase in popularity and wide adoption of cloud computing various cloud data security issues are introduced given below:

- **Data Integrity:** Integrity is defined as the data which is accessed or modified by authorized entities alone. Integrity checks can be performed with or without third party audit. In cloud based environment, data integrity must be maintained correctly to avoid the data lost.[1]
- **Data Leakage:** Once the data is accessed by multi-tenant, the issues of data leakage arises. Or we can say when cloud computing begins to run out, two changes are done over user data. One is storing the user data in location other then user location and second is data turns from one run to multiple run. So this arises the issues of data leakage.[7]
- **Data Recovery:** Data Recovery is a process of accessing data which is corrupted or damaged from the storage media.[3]
- **Data Location:** Storage as a service is completely dependent on the location of the data. Since the location of the data is not known to the users, users hesitate to store their sensitive data in the cloud. It is one of the common issues faced by organizations. The unknown location of data leads to questions of security, legal and requirements of regulatory compliance. This is one of the challenging issues due to untrusted cloud service providers. [8]
- **Data isolation:** Non-sensitive and sensitive data should be separated properly. Data should be isolated from unauthorized users through use of access control and encryption schemes. Lack of care in handling leads to VM to VM attack, there-by losing the confidentiality of the users. [12]
- **Data segregation:** Segregation of data refers to full separation between the cloud users in a virtualized environment. Cloud providers should use highly secured protocols and encryption algorithms to achieve data segregation. Data Segregation vulnerabilities araise due to data validation, insecure storage and SQL injection flaws. Meeting the specified uses in a multi-tenant environment, is of great help in mitigating the problem of data segregation challenge. [2]

VI. LITERATURE SURVEY

Qian Wang et al [3] has provided a verification scheme for storage security by integrating data integrity and dynamic data operations. In this scheme, an auditor verifies the integrity of storage data. The dynamic data operations include block insertion and deletion using Merkle Hash Tree (MHT) technique. They have applied the technique of bilinear aggregate signature for maintaining multiple auditing tasks. But it does not provide confidentiality and authorization.

N. Subramanian et al [4] has focused and explore the security challenges that are faced by cloud entities. These entities include Cloud Service Provider, the Data Owner and Cloud User. Cloud computing is an archetype that enables access to a shared pool of computing resources for cloud users in an on-demand or pay-per-use, fashion. Cloud computing offers several benefits to users and organizations, in terms of capital expenditure and savings in operational expenditure. Despite the existence of such benefits, there are some obstacles that place restrictions on the usage of cloud computing. Security is a major issue that is always considered. The lack of this vital feature results in the negative impact of

the computing archetype thus resulting in personal, ethical, and financial harm.

Li et.al [5] has proposed a framework which addresses issues and challenges regarding multiple Personal Health Records (PHR) owner and user have. Key Management complexity is reduced when compared with other related technologies. It gives a method offers enhanced privacy with sealable and secure sharing of data. The proposed method divide user into two domain- public and personal domain. Public domain include health care and insurance domain. Personal domain have personal health records key have all access to data and can grant access privileges to public domain. In proposed framework system attribute based encryption is used to encrypt patients health record.

Sarkar M et.al [6] The research has presented an overview of data storage security in cloud computing and proposed a framework based on encryption scheme. To ensure the security of user's data in cloud storage, there has been proposed an effective and efficient encryption strategy for enhancing security on data-a-at-rest. It has been showed that scheme almost guarantees the security of data when it is stored in the data center of any Cloud Service Provider (CSP). It will help to build a model to secure the data in the field of cloud computation. This architecture is able to improve the customer satisfaction to a great extent and it will attract many investor in this field for industrial as well as future research farms. This model is able to handle the large number of security threats in a fairly big environment. It has been compared with some other related scheme, it has new features.

Q. Zhang et.al [7] The aim of the research is to provide a better understanding of the design challenges of cloud computing and identify important research directions in this increasingly important area. Cloud computing has recently emerged as a new paradigm for hosting and delivering services over the Internet. Cloud computing is attractive to business owners as it eliminates the requirement for users to plan ahead for provisioning, and allows enterprises to start from the small and increase resources only when there is a rise in service demand. However, despite the fact that cloud computing offers huge opportunities to the IT industry, the development of cloud computing technology is currently at its infancy, with many issues still to be addressed. Research present a survey of cloud computing, highlighting its key concepts, architectural principles, state-of-the-art implementation as well as research challenges.

Shulan Wang et al [8] have proposed an improved two-party key distribution protocol. In this protocol, any user's secret key cannot be compromised by either the key authority or CSP. They also included weights for each attribute to enhance the expression of attributes from binary to arbitrary level. Because of this, the storage cost and encryption cost are reduced. But the access policy is not hidden and the single TA may be subjected to failure.

Singh et.al [9] surveyed various encryption algorithms for data security. Encryption algorithm converts plain message to cipher text. Only the legitimate authorized user can read message. Large number of information is stored on computers and transferred over network. Security of data is an important issue against different attacks. Cryptography has also become complex for making information more secure. Different encryption algorithms are used for security purpose. All algorithms have some positive and negatives factors. All algorithms RSA, AES, DES and 3DES are compared based on factors like key length, rounds cipher text speed and security. Among all it has been concluded that AES is the best high speed encryption algorithm for security purpose.

S.Rajeswari et.al [10] Data Security and Consumer Data Privacy are the key challenges in cloud computing era. The security and privacy of data stored in cloud may be compromised because of limited security for data owners. This paper present an extensive extensive survey on data and storage security challenging issues in cloud computing. The security of cloud data is further analyzed in terms of data integrity, access control and attribute based encryption. The survey analyze each category in detail.

M. Kanti et.al [11] The research has presented an overview of data storage security in cloud computing and proposed a framework based on encryption scheme. To ensure the security of user' data in cloud storage, research proposed an effective and efficient encryption strategy for enhancing security on data-a-at-rest. The scheme almost guarantees the security of data when it is stored in the data center of any Cloud Service Provider (CSP). It will help to build a model to secure the data in the field of cloud computation. This architecture is able to improve the customer satisfaction to a great extent and it will attract many investor in this field for industrial as well as future research farms. This model is able to handle the large number of security threats in a fairly big environment. Though in model error localization can't be addressed and communication delay is remained. Though compared with some other related scheme, it has new features.

Potey M et.al [12] Cloud computing is a broad and diverse phenomenon. Users are allowed to store large amount of data on cloud storage for future use. The various security issues related to data security, privacy, confidentiality, integrity and authentication needs to be addressed. Most of the cloud service provider stores the data in plaintext format and user need to use their own encryption algorithm to secure their data if required. The data needs to be decrypted whenever it is to be processed. This paper focuses on storing data on the cloud in the encrypted format using fully homomorphic encryption. The data is stored in DynamoDB of Amazon Web Service (AWS) public cloud. User's computation is performed on encrypted data in public cloud. When results are required they can be downloaded on client machine. In this scenario users data is never stored in plaintext on public cloud.

VII. CONCLUSION

Cloud Computing is an archetype for delivering and hosting services over the internet. Cloud Computing is also flexible and cost effective business model. Cloud Service Providers (CSP) delivers security polices for cloud data storage. Availability ,Confidentiality, Integrity and Data Recovery are essential fundamentals in security. The research focused on data security issues in cloud computing. Finally, Cloud Computing still have some security issues. In the future, research will be encompassed by providing new mechanism for data security issues in Cloud Environment.

REFERENCES

[1] Hu F, Qiu M, Li J, Grant T, Tylor D, McCaleb S, Butler L, Hamner R "Review on Cloud Computing: Design Challenges in Architecture and Security", Single Processing Computing and control, Journal of Computing and Information Technology, vol-11, pp 122-132, 2017.

[2] C. Linda Hepsiba, J.G.R.Sathiaseelan "Security Issues in Service Models of Cloud Computing", IJCSMC, Vol. 5, Issue. 3,pp.610 – 615, , March 2016.

[3].Qian Wang,Cong Wang,Kui Ren and Wenjing Lou, "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing",IEEE,2009.

[4] N. Subramanian, A. Jeyaraj, "Recent security challenges in cloud computing", Computer and Electrical Engineering, Elsevier, vol-15, pp 28-42, 2018.

[5] Li, Ming, et.al "Scalable and secure sharing of personal health records in cloud computing using attribute based encryption" , Parallel and Distributed Systems, IEEE Transactions, 131-143, 2013.

[6]Sarkar M, Kumar S, "A framework to ensure data storage security in cloud computing" ,Annual Ubiquitous Computing, Electronics and Mobile Communication Conference, UEMCON, IEEE, 2016.

[7] Q. Zhang, L. Cheng, "Cloud computing: state-of-the-art and research challenges" J Internet Serv Appl, Springer, vol- 12, pp-7-18, 2010.

[8]Shulan Wang, Kaitai Liang, Joseph K. Liu,Jianyong Chen, Jianping Yu, and Weixin Xie, "Attribute-Based Data Sharing Scheme Revisited in Cloud Computing", TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, IEEE, VOL. 11, NO. 8, AUGUST 2016

[9] G. Singh, A. Supriya, "A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security." International Journal of Computer Application, vol-6, pp 33-38, 2013.

[10] S. Rajeswari, R. Kalaiselvi, "Survey of Data and Storage Security in Cloud Computing" ,Circuits and Systems, IEEE, vol-5, pp 76-81, April 2018.

[11] Mrinal Kanti Sarkar , Sanjay Kumar, "A Framework to ensure Data Storage Security in Cloud Computing".7th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), IEEE, 2016

[12] Potey M, Dhote C, Sharma D, "Homomorphic Encryption for Security of Cloud Data." Procedia Computer Science, Elsiver, 2016.

[13] Divya K, Jeyalatha S, "Key technologies in Cloud Computing", Proceedings of 2012 International Conference on Cloud Computing Technologies, Applications and Management, ICCCTAM, 2012.