Journal of Advances and Scholarly Researches in Allied Education
Vol. 12, Issue No. 2, January-2017, ISSN 2230-7540

The Study on Security Challenges in Cloud Computing

Sonia Narang[1]* Dr. Kalpana Midha[2]

[1] Research Scholar of OPJS University, Churu, Rajasthan

[2] Assistant Professor, OPJS University, Churu, Rajasthan

Abstract – Cloud computing is another technology regularly utilized virtualized with assets to give dynamically scalable assistance through the web. In the cloud computing, clients can access to the assets by utilizing a different gadgets, for example, workstations, PCs, advanced mobile phone, and so on to get to various assistance, for example, storage, projects, and application-improvement platforms, over help that gave by cloud suppliers through the web. This paper expects to give a safe, powerful, and adaptable technique to improve data storage security in cloud computing. Client with cloud computing can utilize the cloud services anyplace, all over, on-request and dependent on pay per use standard. Cloud computing has two sorts of models: services models (SaaS, PaaS, and IaaS), and organization models (Public, Private, Community, and Hybrid cloud).

Keywords – Cloud Computing, Security Challenges in Cloud, Cloud Security Attacks, Security Issues Face by Cloud Computing

----------X----------

1. INTRODUCTION

Cloud computing is the transmission over the Internet of computing administrations. Cloud management allows people and organizations to use technology and resources in remote areas that are monitored by outsiders. Cloud administrative instances include online document collection, local social networking, webmail, and applications for online business[1]. The cloud computing representations permit somewhere which network association is available to access database data. Cloud computing offers a pool of shared assets, including additional information space, infrastructure, PC planning resources, and integrated business and client applications. Because of these benefits, every relationship[2]. Thusly, there is a need to guarantee that data against unapproved administration access, change or disavowal, and so on. Cloud computing has a lot of advantages and it also has many disadvantages. The major advantages of cloud computing are on-demand self-service, ubiquitous network access, location-independent resource pooling, lower costs, ease of utilization, quality of service, and reliability. The greatest challenge with cloud computing are privacy and security[3]. User privacy is likely to be compromised since the data is being accessed from anywhere in the world. Nobody likes their data being hacked or for the data to go to the wrong hands. Information security means keeping the data secure in all ways. Handing over confidential information to another company makes a person feel unsecure. Companies are spending a lot of time on research on the security issues associated with cloud computing. Another issue which is prominent is latency, which is the delay from request for data to the time when it is actually delivered. These concerns or challenges cause reluctance in the user from shifting to cloud computing[4].

1.1 CLOUD COMPUTING

Cloud Computing helps in providing deliverable computing services through the Internet. It provides services at a minimum cost from a network of configurable computing resources such as servers, applications, networks, storage and services as and when it is required by the user. Individuals and organizations get the services they require through the cloud[5]. Still although cloud compute has numerous benefits, organizations are hesitant to invest in cloud computing principally because of security concerns[6]. One of the principle challenges that frustrate the development of cloud computing is security. SPs endeavor to lessen the threats over the clouds and to improve the reliability to build trust between the SPs and the cloud consumers. The main objective of cloud computing is to provide both software and hardware services. Cloud computing provides services such as Service Software (SaaS), Service Platform (PaaS) and Service Infrastructure (IaaS)[7-8]. These services are utilized for the management of organizations,

businesses and individual researchers. In order to reduce the expenses that incur in the setup of new companies and yet to remain in line with the most recent technologies, the users and companies have been considering services over the cloud in order to reduce the expenses. In spite of the numerous services over the cloud, it is complemented with many security issues. Even though the cloud provides enormous services, it has some serious problems, namely security, privacy and trust problem between the user and the SP. In the cloud, the services are accessed by only registering the user identities in the cloud environment, it is possible that these identities are corrupted by intermediates. Thus, the security and privacy should be managed in the cloud environment because it helps to establish the trust between the user and the SP.

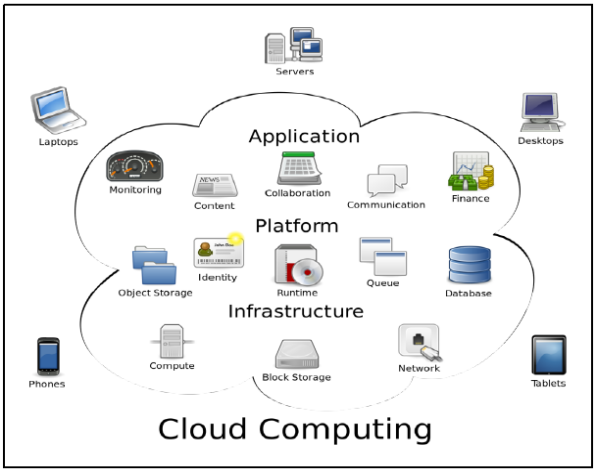

Figure 1.1 Sample Cloud Computing Service

In the cloud environment, a large pool of systems is connected in public, private and hybrid manner to achieve the dynamic infrastructure for application access and file storage process. This cloud based infrastructure helps small scale businesses, such that their expenditure is less but once again privacy and security is an important matter. Some companies and government organizations build their own private cloud data centers such that they can integrate cloud services into their software and infrastructure. Organizations like Salesforce.com and Google build and offer cloud services.

1.2 CLOUD COMPUTING SERVICE DEPLOYMENT MODELS

Cloud services can be distributed in multiple models categorized according to who owns the software and who uses it. The following is a list of popular cloud-based deployment models:

1.2.1 Private Cloud

A company operates and supports the cloud computing services and infrastructure. A private cloud is used to optimize the use of the organization's computing resources. An organization with high security and privacy issues may find that the private cloud model is the preferred option for sharing resources with other organizations over other cloud models.

1.2.2 Community Cloud

Many companies that have common specifications and applications own and use the cloud tools. On the one side, as the costs are spread among the organizations involved, the group cloud adds more cost-effective value than the private cloud. On the other hand, there is a need for some trust relationship between community member organizations, especially on the member organization that is responsible for community cloud management.

1.2.3 Public Cloud

Typically the term cloud computing is used to refer to the concept of public cloud implementation. The cloud services are available to the public mainly through the Internet and are supplied by companies. This delivery model, which offers consumers the most cost-effective services but also faces more challenges, especially in terms of security and privacy, is also more closely related.

1.2.4 Hybrid Cloud

This model is a mixture of two or more other models of delivery, i.e. social, collective and public clouds. The advantages of each model can be used by using more than one model to provide cloud services. For example, a company may use public cloud as part of its application requiring high computing resources, but not high security requirements. A private cloud can be used to host the data and applications that require security and privacy for applications that require a more secure environment.

1.2.5 Virtual Private Cloud

Amazon Web Services (AWS) first used the Virtual Private Cloud (VPC) deployment model to provide cloud services through a Virtual Private Network (VPN). The consumer primarily monitors and configures the VPN. While the VPC is still a new concept under development, it demonstrates a need to preserve the rapid elasticity and cost-effectiveness of public cloud services although giving users of this service more control over their resource primarily to improve the privacy and security of their cloud data and applications[9].

1.3 SECURITY CHALLENGES IN CLOUD

Security is a major concern for some organizations that accept the cloud to store and support

information. A minor error in any of the client apps will clear a path to the hackers to access all information about the cloud storage system. The unauthorized client may get to, degenerate, change, or erase the cloud records on the off chance that there is a vulnerability in the cloud. In the sending models, administration models and system, the security challenges emerge. It is the security administrator's duty to define an association's protection structure based on assets, threat and vulnerability risk assessment frameworks. The three principles of information security are confidentiality, honesty and availability[10]. Data security is important at a place where basic information is stored with multi-client access on a remote server.

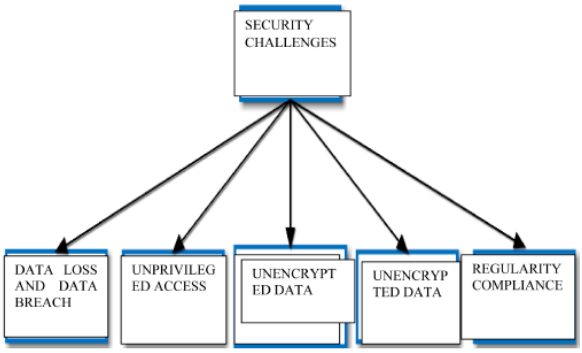

Figure 1.2. Security challenges in cloud computing.

1.4 CLOUD SECURITY ATTACKS

1.4.1 Side Channel Attack

Side-channel attack suggests the need for encryption strategies to eliminate security threats to cloud networks. The durability of the cryptographic scheme against side-channel attacks must therefore be assessed.

1.4.2 Authentication Attack

Authentication is a major weakness and is also aimed at centralized and automated networks. There is a broad range of client verification methods available. The methods used to obtain the verification procedure and the techniques used are consecutive goals of the attackers. At present, as for SaaS, IaaS, and PaaS engineering, this strategy for data security and information encryption is given just by IaaS.

1.4.3 Man-In-The-Middle Attack

This attack is performed when two users are imposed by an attacker. Any time attackers will position themselves in the path of communication, there is the risk that communication can be interfered with and changed.

1.5 SECURITY ISSUES FACE BY CLOUD COMPUTING

- Data Access Control: Generally confidential information will be accessed illegally due to lack of secure access management of information. Sensitive information emerges as a major security issue in an excessively cloud-based system in an excessively cloud-based environment. Information exists in an excessively cloud for an extended period of time, the highest chance of unauthorized access[39].

- Data Integrity: Data integrity includes the following cases once some human error occurs when information is entered. Errors may occur when information is transmitted from one laptop to another; otherwise, some hardware malfunctions, such as disk crashes, will cause errors. Software bug or virus may even produce viruses. Consequently, many customers and suppliers of cloud computing services have accessed and updated information at a constant time. Therefore, in the cloud there is a desire for some methodology of information integrity.

- Data Theft: Cloud computing uses the same price love information system and is scalable for service. Therefore, there is an ability to purloin knowledge from an external server.

- Data Loss: In cloud computing, data loss can be a terribly big problem. If all the principles of banking and business transactions, research and growth go down online, unauthorized persons will be able to access the shared data. Even though everything is secure what if a server is going down or crashing or attacked by a scourge, the entire system would go down and there might be a loss of information. If the seller closes due to money or legal issue, the customer or user will lose information. As a result of the data, the customer will not be able to access these information as additional information is not available to the customer.

- Privacy Issues: Server protection Personal data is extremely essential for cloud computing purposes only. Most of the server is external, so the seller will make sure the alternative operators are well protected.

- Security problems in supplier level: Only a decent security is provided by the seller to

the shoppers by a cloud is sweet. Supplier should build a decent layer of security for the customer and user. And may make sure that the server is well protected from all the external threats that it will be facing.

- User level Issues: User will ensure that there should be no loss of information or infringement of information for alternative users who victimize constant cloud as a result of their own actions[11].

1.6 CHARACTERISTICS OF CLOUD COMPUTING

There are several characteristics of cloud computing, which are described below

- Virtualization- Through cloud computing, users can use any type of terminal to get service anywhere.

- High Reliability- Cloud uses tolerant data fault to ensure the service's high reliability.

- Versatility- Cloud computing can make multiple cloud-based applications, and one cloud can support different sequential programs.

- On Demand Service- Cloud is an enormous asset pool that can be purchased by the user in accordance to their requirements; cloud is like operating water and gas which can be reimbursed by the number used by user.

- Extremely Inexpensive- Centric cloud management means that the company does not need to address the data center management costs that increase very rapidly. The flexibility will increase the rate of usage of available resources compared to traditional program, allowing users to take maximum advantage of low cost[12].

2. LITERATURE REVIEW

In the cloud, a CSP continuously monitors the amount of service being processed, bandwidth, storage levels and the number of user accounts. Thus, cloud computing is controlled and managed both by the consumer and provider side which provides the transparency. The cloud has three different service models which share similarities, but it has its own significant features. The three major service models are Infrastructure as a Business (IaaS) Platform as a Service (PaaS) and Software as a Service (SaaS)[13]. The next significant cloud infrastructure aspect is the implementation models used to reflect the form of cloud environment, the control of the services, the size and access authorization of the services. There are three different cloud delivery models[14], such as corporate, public, hybrid and group models. The cloud has several services that are used to establish and aid in starting up business with less expense. There are various cloud applications such as Email Communication, Game, Finance, Monitoring, content, collaboration, Google Apps suite, Workday, Squarespace, Blogger, Freshbooks and so on.[15]

Cloud computing has several disadvantages in which security is the major challenge while accessing the resources over the Internet. There are various security issues in cloud computing, which are affected by several technologies such as database, networks, operating system, virtualization, transaction management, resources scheduling, load balancing, memory management and concurrency control[16]. The SP establishes the services to the consumer and manages their security details. Even then, the user identities are hacked by eavesdropper and the major security related issues are: data issues, user authentication, infected application and security issues [17].

This segment explains the different cloud protection methods used to handle user accounts in terms of authentication, the authorization method. 18] addresses various models of cloud computing and associated useful cloud services. In this article, the author discusses how cloud protection and privacy are managed and regulated with the aid of a variety of conventional cloud management frameworks and the latest technologies. These cloud technologies are used to control the total cloud computing system. [19] presents various cloud security problems such as security, cost model, service level agreements and cloud interoperability issues. Out of the various issues that were considered, the authors describe that security is one of the major problem which can be improved by applying several cloud computing technologies.

The various authorization processes to establish security in the cloud environment is considered here. Authorization and authentication process needs to be implemented to overcome the security challenges such as data integrity, confidentiality, availability and data integrity[20]. In the cloud environment, different servers' users are accessing the resources which are needed to be maintained by applying symmetric and asymmetric cryptographic techniques. This technique will allow authorizing each user while accessing the resources in the cloud. E-mail based authorization process while accessing services or resources in the cloud was proposed. Initially the user's exact e-mail ids are registered in the provider server and the authorization is performed with the help of the global authorization process which provides the access token for each authorized user. This

process increases the security in the cloud environment[21].

3. CONCLUSION

Cloud computing will have a lot of benefits and a lot of drawbacks. The main advantages of cloud computing are also on-demand self-service, ubiquitous network access, location-independent pooling of resources, lower costs, ease of use, quality of service and reliability. Companies are spending a lot of time on research on the security issues associated with cloud computing. Another issue which is prominent is latency, which is the delay from request for data to the time when it is actually delivered. These concerns or challenges cause reluctance in the user from shifting to cloud computing. Thus, the proposed system achieves better security, authentication, authorization, privacy with minimum time and cost. The established security is used to maintain security between the user and the provider.

REFERENCES

[1]. Shaikh, R., & Sasikumar, M. (2013). Identity Management in Cloud Computing. International Journal of Computer Applications, Volume 63(11), pp. 0975 – 8887.

[2]. Birrell, E., & Schneider, F. B. (2013). Federated Identity Management Systems: A Privacy-Based Characterization. IEEE Security & Privacy, 11(5), pp. 36-48.

[3]. Nunez, D., Agudo, I., & Lopez, J. (2012). Integrating OpenID with proxy re-encryption to enhance privacy in cloud-based identity services. Cloud Computing Technology and Science (CloudCom), 2012 IEEE 4th International Conference on. Taipei.

[4]. Nunez, D., Agudo, I., & Lopez, J. (2013). Leveraging Privacy in Identity Management as a Service through Proxy Re-Encryption. Ph.D Symposium of the European Conference on Service-Oriented and Cloud Computing (ESOCC) 2013. Málaga, Spain.

[5]. Bhat,, M., & Panjeta, P. (2015). Comparison of Different Authentication Protocols Used for Federated Identity Management in Cloud. 5(4), pp. 1-5.

[6]. Ahn , G.-J., & Ko, M. (2007). User-centric Privacy Management for Federated Identity Management. Collaborative Computing: Networking, Applications and Worksharing, 2007. CollaborateCom 2007. International Conference on. New York.

[7]. Alva, A., Caleff, O., Elkins, G., Lum, A., & Pasley, K. (2013). The Notorious Nine Cloud Computing Top Threats in 2013. Cloud Security Alliance

[8]. Agudo , I., Nuñez , D., Giammatte, G., Rizomiliotis , P., & Lambrinoudakis, C. (2011). Cryptography goes to the Cloud. In Secure and Trust Computing, Data Management and Applications Springer, 190-1997.

[9]. Sulton Aldossary And William Allen (2016), “Data Security, Privacy, Availability And Integrity In Cloud Computing: Issues And Current Solutions”, International Journal Of Advanced Computer Science And Applications, pp. 485-498.

[10]. Joseph K. Liu, Kaitai Liang And Willi Susilo (2016), “Two-Factor Data Security Protection Mechanism For Cloud Storage System”, Ieee Transactions On Computers, Vol. 65, No. 6, pp. 92-104.

[11]. Poulakis, D. and Rolland, R. (2015) A Digital Signature Scheme Based on Two Hard Problems. Springer International Publishing, New York, pp. 441-450. https://doi.org/10.1007/978-3-319-18275-9_19

[12]. Anitha Y, “Security Issues in Cloud Computing-A Review” International Journal of Thesis Projects and Dissertations (IJTPD), Vol. 1, Issue 1, PP: (1-6), Month: October-December 2013.

[13]. Keiko Hashizume1*, David G Rosado2, Eduardo Fernández-Medina2 and Eduardo B Fernandez1,”An analysis of security issues for cloud computing”, Journal of Internet Service and Applications 2013(a Springer Open Journal).

[14]. Grobauer, B., Walloschek, T., & Stöck, E. (2011). Understanding Cloud Computing Vulnerabilities. IEEE Computer And Reliability Societies, pp. 50-57.

[15]. Hashizume, K., Rosado, D. G., Fernández-Medina , E., & Fernandez, E. B. (2013). An analysis of security issues for cloud computing. Journal of Internet Services and Applications in Springer, 4(5), pp. 1-13.

[16]. Goel, N., & Sharma, T. (2014). Cloud Computing- SPI Framework, Deployment Models, Challenges. International Journal

of Emerging Technology and Advanced Engineering, 4(1), pp. 19-24.

[17]. Harauz, J., Kaufman, & Potter, B. (2009). Data Security in the World of Cloud Computing. IEEE Computer and Reliability Societ, pp. 61-64.

[18]. Li, H., Dai, Y., & Yang, B. (2011). Identity-Based Cryptography for Cloud Security. Retrieved from https://eprint.iacr.org/2011/169.pdf

[19]. Shade O, K., Frank, I., & Oludele, A. (2011). Cloud Computing Security Issues and Challenges. International Journal of Computer Networks (IJCN), 3(5). Retrieved from http://www.researchgate.net/publication/259072387.

[20]. Gajra, N., Khan , S. S., & Rane , P. (2014). Private cloud security: Secured user authentication by using enhanced hybrid algorithm. International Conference on Advances in Communication and Computing Technologies in IEEE (pp. 1-6). Mumbai: Advances in Communication and Computing Technologies (ICACACT).

Corresponding Author

Sonia Narang*

Research Scholar of OPJS University, Churu, Rajasthan