International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2014): 5.611

A Review on Security Concerns in Cloud Computing

Sharanjeet Kaur[1], Ramandeep Singh[2]

[1]Student - Department of Computer Science and Engineering, Lovely Professional University, Punjab, India

[2]Associate Professor - Department of Computer Science and Engineering, Lovely Professional University, Punjab, India

Abstract: ***The cloud computing is the technique which provides services to various users for data storage on virtual servers. In the architecture of cloud computing, it has cloud server, virtual machines, third party and virtual servers. The user can access cloud services through cloud service provider but before that user have to authenticate with the virtual machine. The user information like user credentials can be stored on the third party. The second major role of virtual machine is to provide data security to the user data. This paper mainly focuses on security concerns of cloud computing like authentication, access control, data confidentiality, integrity and availability.***

Keywords: Authentication, Access control, Data confidentiality, Data integrity and Data availability

1. Introduction

Cloud computing is like on-demand computing and also internet based computing in which resources are shared and the information is provided to users when they require it. It is like a model which is ubiquitous (present every-where) and on-demand (it provides access to shared computing resources when users want to access these resources). Cloud computing provides its users with capabilities like processing and storing their data in third party data-centers.

Cloud computing is like a model which is present every-where, convenient, available when required, and gives users network access of shared pool of computing-resources (applications, servers, network, services and storage) which can be provisioned quickly and also free with minimum management efforts.

In simple words cloud computing focus on increasing the effectiveness of shared-resources and to make it clear that the network in cloud has high performance which allow users to put their data on cloud and get services from the cloud with the presence of internet. The users see the virtual view when they are using cloud services, the services and data of cloud are distributed at different places in cloud.

Cloud computing has three well-known and commonly used service models: *software as a service*(SaaS) according to this model, softwares are given to the users as services and according to the user's requirements, enables users to use that services which are hosted on the server of cloud.

Platform as a service (PaaS) in this model, the clients are given with the platform access which enables the clients to put their applications and customized softwares over the cloud. *Infrastructure as a service* (IaaS) network capacity, storage, rent processing and some other computing resources are allowed enable users to manage the applications, operating systems, network connectivity and storage.

On the basis of access scope, cloud has three types: *public cloud*, the cloud in which services are openly available over the network is a public cloud. *Private cloud*, organizations use private cloud. Private cloud is better than public cloud in terms of security level because it is not available for all, only the members of the organization will access the data, web applications and services. *Hybrid cloud*, combination of public and private cloud is a hybrid cloud.

Cloud computing has number of challenges, security and privacy is one of them. Cloud computing is vulnerable for attacks and threats because of its openness feature. Security of cloud is an important factor for cloud because without security it is insecure to store the data on cloud. Security concerns in cloud are access control, authentication, data confidentiality, integrity, availability and privacy etc.

Sara Qaisar et al. [1] discusses about cloud computing, its types, attacks possible in cloud and their countermeasure. Cloud-computing is an idea which uses internet and remotes servers for storing and maintaining data and the applications. They discuss about network issues of cloud-computing which are denial-of service attack, when an intruder overflows the network with unwanted requests and the server is not able to respond the authorized user's requests. Cloud is shared by unlimited number of users which can make DOS attack happens in cloud. To reduce this type of attacks, reduce the user privileges. Man-in-middle attack, when attacker places himself between two communication parties then there is this type of attack. Communication parties are unaware of the attacker. Attacker may modify the original data. Sometimes these parties communicate with unencrypted data then the attacker can easily receive the information and modify it. In Network-sniffing attack, intruder can hack the passwords, which are not encrypted properly during communication. To reduce this kind of attacks use encryption methods to secure the data. Port-scanning is used by hacker as Port 80(HTTP) which is always available to provide web services to the clients. Some ports are not opened all the time, they open only when they are required therefore the ports can be secured by encryption. To reduce this type of attack use firewalls. Sql-injection attack is a special type of attack in which the hacker use special type of characters like an argument with

value 1=1 may return the desired output because this is always true. Cross-site-scripting is an attack when user enters the correct URL of a website but the hacker redirects the user into their own website and hack the credentials of that user. This paper also discuss about some security issues for example Browser-security, protection of data, flooding-attack etc.

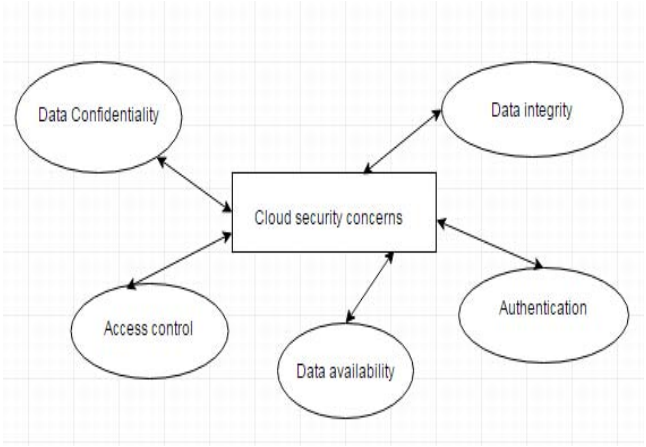

Figure: Security concerns in cloud computing

2. Access Control

Access control means to check whether the services are accessed by authorized users or unauthorized users and to make it sure that cloud resources are not in illegal use. Access control decisions are taken by comparing the credentials to an access control list.

Bibin K Onankunju [2] proposed a technique which allows an application to trust the identity of other application. This paper proposed a hierarchical structure, which has four parts: untrusted cloud, Cloud owner, Cloud user and clock. When data owner wants to upload a file in the untrusted cloud firstly he will encrypt that file and after that he will upload it. The users want to access any file firstly they send request to the cloud and the cloud forwards that request to the higher authorities (owner), then owner checks the attribute set of the user and if the user is authorized owner will send key and the clock will start. After a particular time period that key becomes invalid. So it's necessary for the user to access file within that time limit. This ensures access control and security in cloud computing. Operations discussed in this paper are Registration, File upload, File download and file deletion.

Shin-Jer Yang et. al [3] this paper works for identity management of users and access control. Access is given to the users according to their role. The proposed method assigns the resources with access privileges to the cloud users in order to improve quality of service, security, processing performance and privacy of the cloud system. While capturing user's roles and privileges, the proposed technique separate the online tenants from cloud users.

3. Authentication

Authentication ensures that only legitimate users are accessing the cloud system. Authentication involves confirming and assuring the identity of a person by checking his/her identity documents and verifying the authenticity with a digital certificate etc.

Yogesh Patil et al. [4] discusses about authentication, single level password authentication is not as much secure and suspected to some attacks like brute force attack, shoulder surfing attack , dictionary attack etc. Once harmful user logs into the account then he can have full access to all services. The proposed work aims at securing user's data in cloud by implementing multi-level authentication. They use server side architecture which has two sites. First site has Application server which is responsible for authentication, access control and authorization. Database server will store user's data, ticket and captcha. Second site has data center. This paper also tells about algorithms to generate secure pin and generate secure captcha.

Jen-Ho Yang et al. [5] proposed a model which is designed by one-way hash functions and exclusive-or (XOR) operations so it reduces computation costs. In cloud system, it is easily applied to multi-server environments and does not require verification table on the server side thus the storage space and the verification time can be reduced. The proposed scheme has the ID provider, the users and the server. The ID provider is responsible for registration of users and authentication process. There are two phases first is registration phase and second is mutual authentication phase. In registration phase the users send identity of user and identity of server, then IDP computes some values and then sends that values to respective user and server. In mutual authentication phase user chooses a random number to compute values and Timestamp is used to check the validations.

Jaidhar C.D [6] discusses about a scheme which has password change phase which is vulnerable to Denial of Service attack. To overcome these security flaws, enhanced mutual authentication scheme is introduced. The proposed scheme has 4 phases which are (i) Registration, (ii) Login verification, (iii) Mutual authentication and (iv) password change phase. In this scheme mutual authentication phase has two steps, one is at Cloud Server Side and other is at Smart Card Side. The Security analysis of this scheme are resistant to insider attack, withstands Replay attack, resistant to DOS attack, resistant to Masquerade attack, Perfect Forward Secrecy attack, Online and offline Guessing attacks, valid period Extending attack, and resistant to attacks based on lost tickets.

4. Data Confidentiality

Data confidentiality mainly concerns with data privacy and has two aspects first aspect is no unauthorized individual can access the secret data and second aspect is safety of secret information, the secret data must be disclose only in front of authorized users. Data confidentiality means data must be secret between sender and receiver. The main aim of confidentiality is the prevention of unauthorized users from knowing and accessing secret information.

Khaled M. Khan et al. [7] proposed an approach that splits each row and column of the matrices to change the actual dimensions of the matrices with shuffling and adding

random noise to ensure data confidentiality and privacy. Matrices are sent to server without any encryption. While the server computes on matrices, it is enable to derive actual values either from matrices.

Yuhong liu et al. [8] works for data confidentiality by enabling Cloud service users to (1) encrypt the plaintext and perform data correctness verification by using basic encryption scheme in which the document is divided into multiple small blocks. Sequence of pseudorandom bits is also used. Encryption is done by applying bitwise exclusive OR operation on plaintext data Bi with pseudorandom bits Ti. For data correctness verification they adopt erasure correcting code. Beta-Function-based trust model is used to evaluate the trustworthiness of Cloud service provider which is based on its responses. On the basis of trust value of cloud service provider a cloud service user can make decision about whether to allow the cloud service provider to conduct certain type of data consumption.

5. Data Integrity

Data integrity is one of the important elements in information system. Data integrity mainly concerns with maintaining the consistency and accuracy of data. In simple words only authorized person can modify and alter the data. It is easy to maintain data integrity in standalone systems having single database and is maintained via database transactions and constraints. Data integrity can be achieved by techniques like RAID and digital signatures. Maintaining data integrity in distributed systems is a complex task.

Mohammed Faez Al-Jaberi et al. [9] represents an effective mechanism which is used to provide data integrity verification without granting third party to break the privacy of data. The proposed model has four components- Client application portal (CAP), Key management and storage service (KMSS), Integrity checking service (ICS), and Cloud storage service provider (CSSP). Advanced encryption standard (AES) technique is used to encrypt user's data and RSA-based partial homomorphic encryption is used to encrypt the keys used in AES. Client's local machine and implementation of algorithms is represented by CAP. KMSS main job is to keep encrypted keys. ICS detects any modification done in data which is performed by hacker. CSSP supports hashing which is required for data integrity verification.

Rajkumar Chalse et al. [10] worked for data integrity in cloud computing. They propose architecture for cloud storage. The proposed architecture has three entities- (i) Clients who have authorization to access and modify stored data, (ii) Cloud service providers which are providing services to authorized users (iii) Trusted third party. A cooperative PDP (Provable Data Possession) is used to examine integrity of data stored in all CSPs.

6. Data Availability

Data availability means data should be available to authorized users whenever they require it. Data availability is interrupted by DOS and DDOS attacks. Distributed Denial of service (DDOS) attack makes the system unavailable for the legitimate users by sending lots of unauthorized request to the server. Data availability concerns with whenever any failure occurs like hard disk damage and network failures the extent that user's data can be recovered.

Aman Bakshi et al. [11] proposed an idea how to detect and reduce DDOS attack in infrastructure of cloud. IDS, similar to snort are installed on your virtual switch to examine the incoming and outgoing record of data. If there is spike in the graph then it checks for acknowledgement from senders, if SYN-ACK is yes then goes back to the previous step otherwise if SYN-ACK is no then IDS requests Honeypot to show how much time taken by packet to reach the IP addresses given by hacker. If there is no reply means Distributed Denial of Service attack, then botnet formed by all Zombie machines is blocked. Then move that server to other virtual server by update the routing tables.

R. Anitha et al. [12] proposes the Cloud Bloom Filter (CBF) a mechanism for metadata management in the cloud computing database which raises the search effectiveness of data. They propose a three layered cloud metadata architecture that provides a systematic retrieval of exact data from cloud data server by minimizing the search space. The metadata model attributes are designed in a way that the query is mapped to the exact location of data in the database server which leads to the fast retrieval of data. Global Bloom Filter (GBF) provides a protocol used for placing the metadata file in its server and its own replica location. Local Bloom Filter (LBF) in the metadata server effectively decreases the time taken to update the respective file with the limited updating overhead. The proposed scheme significantly decreases the time taken to retrieve the data from the database server.

7. Conclusion

Cloud computing is a bright and good technology for the next generation of IT applications. The hurdle towards the quick growth of cloud computing are cloud computing security issues like authentication, access control, data integrity, data confidentiality and data availability. Reducing these types of risks is mandatory for cloud computing vendors to gain the trust of any organization so that they store their confidential data on cloud because no one will store their data on cloud until the trust is built between cloud users and cloud service providers. There are number of techniques proposed for data security to achieve highest level of security in cloud computing. There are still many security gaps that need to be filled by making existing techniques more powerful and effective. Further more efforts are required in cloud computing security to make it trustable by users that are using cloud services. This paper surveyed number of techniques about authentication, access control, data integrity, data confidentiality and data availability on data storage.

References

[1] Qaisar, Sara, and Kausar Fiaz Khawaja. "Cloud Computing: Network/Security Threats And Countermeasures" published on Interdisciplinary

Journal Of Contemporary Research In Business on January 2012."

[2] Onankunju, Bibin K. "Access Control in Cloud Computing." *International Journal of Scientific and Research Publications* 3, no. 9 (2013): 1.

[3] Yang, Shin-Jer, Pei-Ci Lai, and Jyhjong Lin. "Design role-based multi-tenancy access control scheme for cloud services." In *Biometrics and Security Technologies (ISBAST), 2013 International Symposium on*, pp. 273-279. IEEE, 2013.

[4] Patel, Yogesh, and Nidhi Sethi. "Enhancing Security in Cloud Computing Using Multilevel Authentication. " *International Journal of Electrical Electronics & Computer Science Engineering* 1, no. 1 (2014).

[5] Yang, Jen Ho, and Pei Yu Lin. "An ID-Based User Authentication Scheme for Cloud Computing." In *Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), 2014 Tenth International Conference on*, pp. 98-101. IEEE, 2014.

[6] Jaidhar, C. D. "Enhanced mutual authentication scheme for cloud architecture." In *Advance Computing Conference (IACC), 2013 IEEE 3rd International*, pp. 70-75. IEEE, 2013.

[7] Khan, Khaled M., and Mahboob Shaheen. "Data Obfuscation for Privacy and Confidentiality in Cloud Computing." In Software Quality, Reliability and Security-Companion (QRS-C), 2015 IEEE International Conference on, pp. 195-196. IEEE, 2015.

[8] Liu, Yuhong, Jungwoo Ryoo, and Syed Rizvi. "Ensuring data confidentiality in cloud computing: an encryption and trust-based solution." In Wireless and Optical Communication Conference (WOCC), 2014 23rd, pp. 1-6. IEEE, 2014.

[9] Al-Jaberi, Mohammed Faez, and Anazida Zainal. "Data integrity and privacy model in cloud computing." In Biometrics and Security Technologies (ISBAST), 2014 International Symposium on, pp. 280-284. IEEE, 2014.

[10] Chalse, Rajkumar, Ashwin Selokar, and Arun Katara. "A new technique of data integrity for analysis of the cloud computing security." In Computational Intelligence and Communication Networks (CICN), 2013 5th International Conference on, pp. 469-473. IEEE, 2013.

[11] Bakshi, Aman, and B. Yogesh. "Securing cloud from ddos attacks using intrusion detection system in virtual machine." In Communication Software and Networks, 2010. ICCSN'10. Second International Conference on, pp. 260-264. IEEE, 2010.

[12] Anitha, R., and Sayan Mukherjee. "CBF: Metadata management in cloud computing." In Computational Intelligence and Information Technology, 2013. CIIT 2013. Third International Conference on, pp. 272-278. IET, 2013.