Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 5, May 2015, pg.639 – 643

SURVEY ARTICLE

Different Data Security Issues of Cloud Computing: A Survey

Samjot Kaur[1], Vikas Wasson[2]

Research Scholar of Master of Engineering, Chandigarh University Gharuan, Punjab, India 140413[1]

Assistant Professor, Dept. of Computer Science, Chandigarh University Gharuan, Punjab, India 140413[2]

samjotkaur@gmail.com [1], vikaswasson.cse@gmail.com [2]

Abstract— Cloud computing has been emerged as one of the most exciting paradigms in IT industry and is gaining more importance, as it offers storage of data at lower costs and is available all the time on net. Although cloud computing provides data at lower costs, easier maintenance, and availability of services anywhere, anytime, a key challenge is how to ensure that cloud can secure user's data efficiently. Security in cloud relates to the risk areas in the same manner with exterior storage of data, lack of control, multi-user availability and combining these factors with internal security. The main purpose of this paper is to focus on the security issues of protecting user's data in cloud.

Keywords— Cloud computing, security, security issues.

I. INTRODUCTION

Cloud computing attracts people for various services provided by it at lower costs. In cloud computing, services are provided to users according to their needs. Service providers can adjust the content to be offered according to user's requirements. For instance, user can seek disparate amount of storage, degree of data encryption, speed of transmission, and other services [11]. Cloud computing provides on demand access to shared pool of resources such as servers, storage, network and applications that can be granted and unleashed with minimal management effort and reduced service provider interaction.

Cloud computing service providers provide services to users according to service models which are as follows:

- ***Infrastructure as a Service (IaaS)*:** According to IETF (Internet Engineering Task Force), computers or virtual machines, computing power and other physical resources like storage space are provided on demand by the IaaS providers.
- ***Platform as a Service (PaaS)*:** In PaaS models, computing platform such as web server, operating system, database and the background for programming language execution is provided by the service providers.
- ***Software as a Service (SaaS)*:** In SaaS model, databases and application softwares can be accessed by the users on demand. That's why it is often called as "on-demand software" [17].

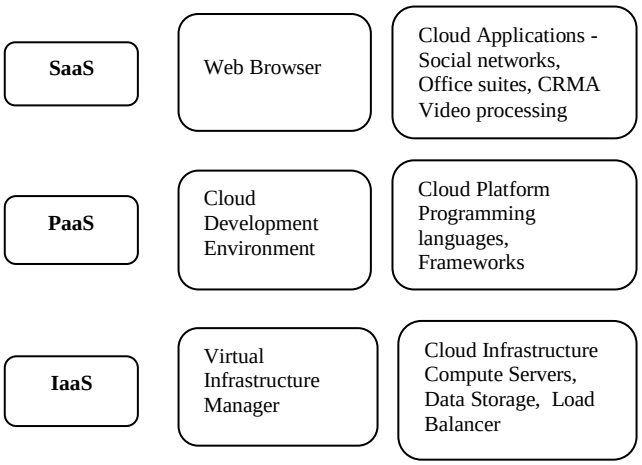

Figure 1: Service model of cloud

The deployment models of cloud computing are as follows:

- ***Private Cloud*:** In private cloud, all the services are provided to a single organization, whether managed internally by the organization or externally by the third party.
- ***Public Cloud*:** Public cloud is a cloud where services are issued over a network which is available for public use. These services may be available for free.
- ***Hybrid Cloud*:** Hybrid cloud is formed by combining two or more cloud types such as private, public, community etc. and offers the benefits of numerous deployment models [17].

Cloud computing has specific characteristics that differentiate it from classical service and resource provisioning environments. Cloud computing unveils following key attributes: [18], [17]

- ***Cost Reduction*:** Cloud computing reduces the cost associated with under-provisioning (i.e. availability of less resources), over-provisioning (i.e. availability of resources more than requirement) and under-utilization (i.e. utilizing available resources inadequately).
- ***Multitenancy*:** Multi means diverse and tenancy means clients. So, Multitenancy means numerous customers can store their data and access the applications on the cloud.
- ***Location and device independence*:** This means users can access the services despite their location and the tool they are using to access the services (such as, PC, mobile phone etc.).
- ***Maintenance*:** Applications and implementations are easier to maintain in cloud computing as they are not required to be installed on every user's computer.
- ***Storage Capacity*:** There is more than required space available for user on cloud. So, they do not need to worry about the storage space to save their data.
- ***Productivity*:** Numerous users can work simultaneously on same data as a substitute of saving data and then e-mailing it. Hence, increasing productivity. Users do not need to upgrade their softwares on their computer.
- ***Utility based pricing*:** Pay-per-use pricing is used in cloud computing as a standard. So, users will have to pay only for what they use.

II. ISSUES IN CLOUD COMPUTING

Although, cloud computing has numerous attractive characteristics to prove itself better but still there is a long way to prove itself better with regards to the security of users data. There are mainly security, privacy, and trust issues which are of main concern for users using cloud services.

- ***Security Issues*:** Security of data is mainly related to availability, integrity and confidentiality of user's data. Availability of data means any information of data must not be available to unauthorized users. Integrity means any unauthorized user should not be able to amend or delete any information. Confidentiality means any information must not be disclosed to unauthorized users [19]. There are six sub-categories in which security issues have been divided:

a) How to avoid hijacking of service such as phishing, fraud, exploitation which are most critical issues in IT.

b) How to trace or monitor cloud server, so that security mechanisms should be granted.
c) How to avert malicious insiders.
d) How to maintain multi-precedent in multi-possession virtual environment.
e) How to keep each user's sensitive information confidential.
f) How to develop and implement appropriate law and legal jurisdiction.

- ***Privacy Issues*:** Privacy refers to the ability of individuals to reveal their information to others. It mainly includes the information of the user that could be revealed to other users, how the user needs to get informed about his information which has been requested by someone else, and to what extent, user's information should be revealed to other users. The privacy issues can be divided into four sub-categories:

a) How to avoid leakage, data loss and unauthorized modification and to ensure replication of data in consistent and jurisdiction state.
b) Degree of involvement of cloud sub-contractors in processing could be checked, identified and ascertained.
c) How users can have control over their data when their data is saved and handled in cloud.
d) Which party is bound to legal requirements of each user's personal information.

- ***Trust Issues*:** Trust have umpteen of security attributes such as trustfulness, belief, dependability, reliability, confidence, honest, security and alike. Trust issues can be divided in four sub-categories in cloud computing, which are given below:

a) How to handle information which is recommended as malicious.
b) How to adjust, reflect, and monitor trust relationship potent change with space and time.
c) Which attributes should be used to define and evaluate trust in cloud computing.
d) According to which degree of trust, level of security should be provided.

III. HOMOMORPHIC ENCRYPTION

Encryption helps to achieve properties of data protection [18]. Homomorphic encryption is used to convert unencrypted text to ciphertext. Any information that a sender needs to deport to receiver is called as plaintext or unencrypted text. Ciphertext is the text which has been encrypted and is not understandable until its decryption with the help of a key [21]. Homomorphic encryption alludes to encryption where plaintexts and ciphertexts both are treated with a correspondent algebraic function. Now the plaintext and the ciphertext might not be connected but the algebraic operation that works on both of them. Structured encryption scheme encrypts structured data in such a way that it can be queried through the use of a query-specific token that can only be generated with knowledge of the secret key [22]. In addition the query process reveals no useful information about either the query or the data. There are two technique FDE (fully disk encryption) and FHE (fully homomorphic encryption). FDE offers excellent performance and ease of development but it does a little to secure privacy at the required grate whereas FHE on the other hand, pushes the privacy envelope in the other direction by removing data visibility entirely from both the server and application developer.

IV. RELATED WORK

In this paper [1] they proposed different techniques and their merits and demerits like Message Authentication Code(MAC) which protect the data from integrity. The owner of any information verified the data integrity by recalculating the message authentication code of data received by others but recalculation is possible if the amount of data is very large. A hash tree is used for large files. Third party auditor is used to relieve the large data into small parts of maintenance and security. The proposed algorithm describes data integrity and dynamic data operations. They use encryption to ensuring the data integrity. Public key is also defined which is based on homomorphic authenticator. A hash function is used for proof of retrievability. The proposed algorithm has a main drawback that it requires implementation of the higher resources cost. In this paper [2] Dynamic mobile token application is introduced. This is the application in mobile phones which is used to generate a code with the help of OTP (One Time Password). This OTP code is used only for one time to login session. In this paper, they describe one of the methods of OTP. There are two phases in it Registration phase and Login phase. User first register itself by fill credentials in the form and then enters to the Login phase. In login phase, OTP will generate for the login session. OTP is generated by three parameters: The current time, 4-digiti PIN code and Init-secret. This code is valid for three minutes only. This ensures protection against eavesdroppers attack and man-in-middle attack. Hence, they prove OTP is very secure. In this paper [3] a design and architecture is proposed that can help to encrypt and decrypt the file at the user side which provides data security in both cases while user is at rest or is transferring data. In this paper they used the Rijndael Encryption Algorithm along with EAP-CHAP. This algorithm has five steps which need to be follow for the data security. The users are always concern about the privacy protection and security issues before storing their data on cloud.

So in this the focus is on client side security in which only the authorized user can access the data. Even if some intruder (Unauthorized user) gets access of the data then the data will not be decrypt. Encryption must be done by the user to provide better security Algorithm . For this, Rijndael Encryption algorithm is used. In this paper [4], two techniques are discussed: Virtualization and Multi-tenancy which provides security about cloud computing. As data is organized by third party organizations, that offer SaaS and PaaS which is important for the security. So, Virtualization and Multi-tenancy techniques are used for the security purposes. Virtualization is a way of making a physical computer function as if it were two or more computers where each non-physical or virtualized. There are two types of virtualization: Full virtualization and Para virtualization and two architectures of virtualization: Hosted and Hypervisor architecture. Multi-tenancy is the ability to provide computing services to multiple customers by using a common infrastructure and code base. Multi-tenancy can be applied to different levels i.e. application level, middleware level, operating system, hardware level. Then security of virtualization and multi-tenancy has been discussed. In this paper [5] they discussed different issues related to cloud computing security. To protect cloud computing system and to prevent various attacks many security mechanisms have been developed. To improve the security of cloud computing new technologies has been developed by the researchers. Different types of attacks like SYN flood, malware injection, account hijacking are discussed in this paper. The main focus of this paper is on detecting and preventing SYN flood in cloud computing. The author developed two algorithm one detecting algorithm and one preventing algorithm. They will implement and test these algorithms on cloud computing.

V. CONCLUSION

This paper presents a comparative review of numerous issues associated to data security in cloud computing. It explains the concerns of users about their personal information and the security, privacy and trust issues associated to it. The main purpose of this paper is to get in touch with the issues of securing data in cloud.

We hope this comparison will give better understanding of data security issues to those researchers who are trying to learn about security issues in cloud computing.

REFERENCES

[1] Bhavna Makhija, VinitKumar Gupta, 2013 "Enhanced Data Security in Cloud Computing with Third Party Auditor", International Journal of Advanced Research in Computer Science and Software Engineering, pp 341-345

[2] Vimmi Pandey, 2013 "Securing the Cloud Environment Using OTP" International Journal of Scientific Research in Computer Science and Engineering vol-1, Issue-4

[3] Sanjoli Singla, Jasmeet Singh, 2013 "Cloud Data Security using Authentication and Encryption Technique" International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, Issue 7, July 2013, pp 2232-2235

[4] Ankur Mishra, Ruchita Mathur, Shishir Jain, Jitendra Singh Rathore, 2013 "Cloud Computing Security" International Journal on Recent and Innovation Trends in Computing and Computation, pp 36-39

[5] Punithasurya K, Esther Daniel, Dr. N. A. Vasanthi, 2013 "A Novel Role Based Cross Domain Access Control Scheme for Cloud Storage" International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, Issue 3, March 2013, pp 942-946

[6] Barron, C., Yu, H., & Zhan, J., 2013 "Cloud Computing Security Case Studies and Research". Proceedings of the World Congress on Engineering 2013 Vol II

[7] Craig Gentry, 2009,"full homomorphic encryption scheme"

[8] Dawn Song, Elaine Shi, 2012 "Cloud Data Protection for the Masses" IEEE Computer Society, pp 39-45

[9] Deyan Chen, Hong Zhao, 2012" Data Security and Privacy Protection Issues in Cloud Computing" International Conference on Computer Science and Electronics Engineering, pp 647-651

[10] Deepanchakaravarthi Purushothaman[1] and Dr.Sunitha Abburu[2] ,2012" An Approach for Data Storage Security in Cloud Computing" IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 2, No 1.

[11] Dian-Yuan Han, Feng-qing Zhang, 2012 "Applying Agents to the Data Security in Cloud Computing" International Conference on Computer Science and Information Processing(CSIP), pp 1126-1128

[12] Dr Nashaat el-Khameesy,Hossam Abdel Rahman, 2012 "A Proposed Model for Enhancing Data Storage Security in Cloud Computing Systems" vol-3

