International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)
Web Site: www.ijettcs.org Email: editor@ijettcs.org
Volume 6, Issue 4, July- August 2017 ISSN 2278-6856

Security Issues in Cloud Computing: A Survey

Narander Kumar[1], Jitendra Kumar Samriya[2]

[1] Department of Computer Science B. B. A. University (A Central University), Lucknow, UP, INDIA.

[2] Department of Computer Science B. B. A. University (A Central University), Lucknow, UP, INDIA.

Abstract

Cloud computing is an emerging trend in computer science. We can define cloud computing as "pay as per use" service. Today, cloud computing infrastructure is most demanding due to its low-cost of network and storage services. With the increasing number of users, data and network security becomes the major issue in cloud environment. However, there are many approaches available, perspective of security of data, e.g. Authentication for accessing the data, network communication mechanism, third party assignment policy. In this paper, we survey about the security issues related to cloud computing. Here we describe some major security issues and challenges in cloud computing.

Keywords: Component Cloud Computing, Cloud infrastructure, Security issues.

1. INTRODUCTION

Cloud computing is need of modern computing environment of tomorrow. The goal of this computing facility is to provide resources as per user requirement and decrease the cost of the whole computing system by sharing application. It provides data center with the hardware and software. Cloud computing provided various functionality e.g. Infrastructure management, on- demand accessibility of data. It depends on the related organization to reduce the cost, energy and other services used in cloud computing.

It is used today, in all our everyday need in life such as shopping, personal data storage, satellite launching etc. According to survey report of International Data Corporation (IDC)'s, in 2019 the expenditure on IT cloud services will be more than US$141 billion worldwide [1]. Cloud computing contains scarce resources (e.g. Servers, applications and storage) to provide service to end user by service provider. The Web browser is responsible to access on-demand cloud services to users also.

Basically Cloud computing infrastructure contains 3-layer architecture: SAAS, PAAS, IAAS. SAAS is generally identified as top most layers in cloud infrastructure, called software-as-a-service. It is also known as application layer, which allows application run on cloud to fulfill the user's requirement, e.g. VMware, Amazon Elastic, etc. PAAS named Platform-as-a-services or platform layer, act as a middle layer in cloud infrastructure. This layer designed to provide a development environment for user to use relevant applications. It provides the control over the application deployment e.g. Google Docs, Google Talk etc. Finally, Third layer is Infrastructure-as-a-service is bottom layer, known as IAAS [3]. It includes servers, network devices, memory and storage etc. The resources are available for user's on-demand services. It also uses virtualization technique, which capable to form complex network infrastructure via virtual machines.

Many techniques can be used in several ways in security aspect in cloud like: Authentication of data in the cloud, Authentication of user, Encryption of data, Denial of service over the network, QoS infrastructure management. Here we illustrate all the policy which handles the cloud computing security challenges.

This paper mainly focused on the security issues relevant to Cloud computing. When the data sharing is done with a third party cloud users wants to leave an uncertain cloud provider because information may be in many forms, e.g. Medical records, Credit card details or any other private information. So the security is must to be added to secure important and confidential information of the user stored on Cloud [2].

2. REVIEW OF LITERETURE

To secure data in the cloud platform, generally we used the textual password technique. With this technique, it is easy for attackers to guess the information. It may lead to eavesdropping, shoulder surfing and dictionary attack problem. M. Potey et al. [4], proposed the color scheme authentication (CCA) is used to overcome textual based password problems. This is implemented on private cloud using JavaScript, CSS, jQuery, PHP and MySQL. This CCA scheme solves the shoulder surfing. It also uses a challenge response system (CRS). Javaid Zeeshan and Ijaz Imran proposed [5], a model to prevent and show directly the authentication credentials. In this model devoted firewall defines between the cloud host and the clients supported by VPN, to arrange whole traffic passed by the tunnel. This model helps to reduce the computational cost of complex schemes. Through this model configuration, there is no need to use traditional devices eg. USBs or smart cards, these are generally used by researcher to secure the system. Using tunneling the sniffed data treat as garbage data for an interloper. Chen chin-ling et. al. [6], defines an authorization process model, specially designed for healthcare system on cloud platform, which combine mobile devices and cloud platform using cryptographic approach for remote areas medical services. In this healthcare model, the patient must have to register his/her mobile device's International Mobile Equipment (IMEI) to

login to a public cloud. On the other hand the hospital must login with registered physical address (MAC) of network card. Then both of above mentioned devices authenticate each other. A session key is also used here by producing secret parameter produced by public cloud for request the cloud services. Trimala et. al. [7], presents an analysis relates it with an incident the online hijacking of The New York Times. Here also explained all possible prevention strategies to solve above problem or incidents. In this paper all the incident described step by step and guide for preventing phishing attacks. Maghrabi Louai A. [8] discussed possible threats over the cloud platform. In this paper the problems generally found in cloud discussed in two manners. One, the experts concerned about the security issues and threat in the cloud, as the other questionnaire session used to know perception of the students of University of the West of England on the security issue on the cloud in perspective of data. Ali Mazhar et. al. [9], proposed DROPS (Division and Replication of data in the Cloud for Optimal Performance and Security) techniques to prevent data leakage for by dividing the data file using multiple number of nodes to store a single file. This fragmented file used for replication of cloud. Purohit Bijayalaxmi and Singh Pawan Prakash [10], classified the leakage of information in three categories in the cloud platform as: Unintentional leak, intentional leak and malicious leak. Further the data loss prevention is being handled by the open source software, MyDLP. Kalra Sheetal et. al. [11], proposes an anti-phishing protocol, which allows only valid user of the cloud. This protocol provides better security and minimum cost due to cutting edge technology of elliptical curve cryptography (ECC). In this technique first we have to authenticate the valid users using any service on cloud platform. Here a single password is used for particular client. Chen Yu-Jia et. al. [12], mainly focused on link-eavesdropping performance model. However, both nodes eavesdropping and link-eavesdropping problem, but the investigation is done on recovering data in the inter-cloud storage system, by link-eavesdropping. It compares the eavesdropping techniques used before with link-eavesdropping.

Jeffery Yi Han et. al. [13], proposed a new balanced virtual machine allocation policy against such threat, the coresident attacks in cloud platform. It helps to prevent unauthorized users who build a side channel to get private data from virtual machines. In this paper the mainly focused on the initial virtual machine allocation strategies. Kranmai B. et. al. [14], introduced a new approach to identify attack at client side and service provider too. Here IDS (intruder detection system) is used to identify attack using it virtual machine on back end. Yan Qiao et. al. [16], proposed software difined networking and distributed denial of service attack relate it to cloud computing. Software difined networking changes the way of defeat distributed denial of service attacks in cloud environment. Software defined networking is used as a tool here to prevent DDoS attack. Fábio D. Rossi et. Al. [17], explained the energy consumption issues. With the increasing number of resources on demand for customer, application migration on Cloud, energy consumption is also rapidly used. But most of the cases we ignore this problem and compromise the performance of the servers. Due to this sometime data center handler can lose the task to substantial performance loss in its critical time. With the energy problem, it also affect to QoS (Quality of Services), SLA (Service level agreement) and Security (Both level Network and system) also. Uranium Ehsan, Taheri Hassan et.al [18], discussed about the working of Dynamic Voltage and Frequency Scaling (DVFS) technique used for energy consumption on cloud platforms. A DVFS-aware algorithm for solving a problem of on-line consolidation and proposed a way to handle the inconsistencies between DVFS techniques and consolidation. Yinggjie Zhang [19], describes about the evaluation technique on energy efficiency and analysis of the machine tools, machining systems. It described all the related work which emphasis on the techniques which motivated on reducing the energy. It also described energy saving model for machine tools and peripheral components or subsystem. As the increasing the number of users, high storage capacity application is also increasing on the distributed networks. The application reduces access latency by requesting relevant data centers. The data center is also geographically distributed. Because of this energy consumption is a more effective field for attention Fan Yuqu et. al. [20]. Hammanmi Ali, Simoni Noemie and Salman Rasha [21], proposed an architectural model and QoS control techniques which fulfill the user requirements and the address cloud security. The above project model named as UBIS (Ubiquity and Integration of Services). Tao chen et.al. [22], explained a survey report by introducing and describing hardware on data center networks. It classifies a detailed architecture of networks of data center with switch and server centric architecture. Joshi Bansidhar, Joshi Bineet and Rani Kritika [23], explained the issue on data segregation and encryption strategies used in cloud computing and proposed probabilistic method for secure private data using Private Data Bucket (PDB) and Non-Private Data Bucket (NPDB). A key is also commonly used for both of above bucket techniques. Durairaj M. and Manimaran A. [24], identifies most possible issues which affects cloud based E-Learning. Now a day, e-learning is used by many countries, due to its better accessibility, flexibility for user and availability on demand facility. Due to many attacks faced in cloud based data accessing, this paper defines security attacks which bound the e-learning facility, from data and network perspectives on cloud environment. This paper also proposed a security model, based on cloud for E-Learning. The secured layer and 3rd party provider are used to design this security model. Kumari D. Aruna et. al. [25], described encryption and decryption process. Here is also a small introduction is also defined related to Data-Encryption Standard (DES), Advanced-Encryption Standard (AES), Asymmetric Key Algorithm-RSA. There are many encryption and decryption algorithms e.g. AES, DES, RSA, Cipher Block chaining is discussed. By using above algorithms, proposed a Magnified Cipher Block Chaining mode using

DES. Here data is encoded, encrypted, and encrypted data is stored on Cloud. We can access the encrypted data by decrypt the data using the same algorithm.

From the extensive review of work to provide the security in cloud environment and find that there is need of such techniques which provide the security in cloud environment. This paper presents such major issues which will be helpful to provide the security in cloud environment.

The organization of this research paper is as section 1 presents the Introduction. Review of work is discussed in section 2. Section 3 presents major issues and challenges. Conclusion has been given in section 4.

3. ISSUE AND CHALLENGES

Now a day's Cloud Computing considers as a vulnerable area for Researcher. But due to massive data storage in data centers, it is hard to maintain, to secure the data and network. There are major issues and challenges found in the cloud platform, as follows:

A. AUTHENTICATION IN CLOUD:

Cloud computing is emerging trend for tomorrow uses. The application is also used in distributed computing. Authentication and verification of the user as well as data is very important in distributed computing and cloud computing for security point of view. Authentication is also further divided in two categories:

(a) Security within the cloud
(b) Security outside the cloud.

An authentication technique depends on the secure channel and effective authenticate scheme. In the Authentication process, we can use text-base password based protection techniques. Some users used color-based password techniques including one time-password (OTP) [4], somewhere used zero knowledge and hashing with biometrics, single sign on. [5].

B. Session Hijacking:

Since Cloud computing offers the amazing accessibility feature to the user, therefore the users/organizations are rapidly adopting cloud computing environment. But due to several Cyber-Attacks, it prevents the organization to use cloud for most private work. Session hijacking / traffic hijacking or service hijacking is one of them. It is also a kind of account identity theft of relevant organizations. An example, hijacking is described in detail of world's most famous magazine New York Times [7]. Attackers capture user's private details like password, OTP etc. and use these details to prevent user.

C. Data Segregation and leakage:

Cloud computing environment uses location sharing, means data storage of two or more users can be located along with each other. This may cause problems in data segregation. To proper data segregation user should be well known to protocols, rules and encryption methodology. Using few constraints, data e.g. validation, SQL injection flaws can separate. Data leakage is also a major problem occurring in cloud computing. Data loss or data leakage may be deleted or change by the attacker in many ways e.g. DDoS, increasing network traffic etc. Encryption, API security and network security policies are solution to overcome the data leakage problem [8].

D. Phishing:

Phishing is a methodology used for theft private information. It may be formed of Account name, password hint or fraud email. Phishing attacks are also an issue in cloud computing, which affect data accessibility, flexibility and privacy. By the end of 2008 the phishing problem increases by 258% from 2007 in cloud computing [11]. For better accessibility on the cloud data phishing problem should be solve to prevent cyber-attack.

E. Eavesdropping:

Eavesdropping is also a threat which limits on cloud uses. It prevents the feature of confidentiality of cloud data. Due to Eavesdropping, it may cause affect the relationship between Cloud user and Cloud Service Provider.

F. Virtual Machine Allocation Policy:

Cloud computing provide on-demand accessibility of data to its consumers. Virtual machine helps to create an environment to access the data of another environment. There are few problems or issue related to virtual machine allocation. With the time attacker's policies are more harmful for cloud data. Sometimes users' makes the side channel and get extremely secure information from virtual machines located on the same physical server [13].

G. SLA, QoS based Energy Efficiency:

After deploying all the data on cloud environment, it should be ensured about the data privacy and quality, availability and reliability. Above discussed features are Service level agreement (SLA) policies of cloud data. SLA principle needs to integrate user feedback and personalize property into the SLA framework [24]. On the other hand cloud data center consumes the bulk amount of energy due to migration of applications on the cloud. The resources are increasing day by day on data centers. Resource utilization and energy consumption is proportion to each other. It is a more challenging task today to reduce the consumption of energy of data centers [17]. It will make cloud environment effectiveness and follow Quality of Service (QoS) feature.

4. CONCLUSION

In the modern age, each person wants to space in cloud for storage the personal, financial, medical etc information to use and reuse or even wants to online treatment and maximize online transaction also. Therefore, there are the need for emphasize the research work in this line. This paper presents an effective analysis and technical review which are related to various security issues or challenges

such as Authentication in the cloud, session hijacking, Phishing problem, Eavesdropping, Virtual machine allocation policies, Service level agreement, Quality of Service and energy efficiency. All the above discussed issues and challenges we will try to provide the solutions as future work.

References

[1] Zh Li, Haitao Xu and Yanzhu Liu, "A differential game model of intrusion detection system in cloud computing", International Journal of Distributed Sensor networks, XXIII(1), pp. 1-11, 2017.

[2] Mohammed A. AlZain, Eric Parded, ben Soh, James A. Thom, "Cloud Computing Security: From Single to Multi-Clouds", 45th Hawaii International Conference on System Sciences: IEEE Computer Society, pp. 5490-99,2017.

[3] Chou Te-Shun, "Security Threats on Cloud Computing Vulnerabilities", International Journal of Computer Science & Information Technology (IJCSIT), V(III), pp. 79-88, June 2013.

[4] Manish M. Party, Dr C. A Dhote, Deepak H. Sharma, " Secure Authentication for Data Protection in Cloud Computing using Color Schemes", International Conference on Computational Systems and Information Systems for Sustainable Solutions, IEEE, pp. 424-427, 2016.

[5] Zeeshan, Imaran Ijaz, " Secure User Authentication in Cloud Computing.", IEEE, 2013.

[6] Chen Chin-Ling, Yang Tsai-Tung, Leu Fang-Yie, Huang Yi-Li, "Designing A Health Care Authorization Model Based On Cloud Authentication", Intelligent Automation & Soft Computing; Taylor & Francis, XX(III), pp. 365-379, 2014.

[7] Sremath Sreenivas Tirumala, Hira Sathu, Vijay Naidu, " Analysis and Prevention of Account Hijacking based INCIDENTS in Cloud Environment",14th International Conference on Information Technology:IEEE, pp. 124-129, 2015.

[8] Maghrabi A. Loauai, The Threats of Data Security over the Cloud as Perceived by Experts and University Students: IEEE; 2014.

[9] Mazhar Ali, Kashif Bilal et.al.,"DROPS: Division and Replication of Data in Cloud for Optimal Performance and Security", IEEE TRANSACTIONS ON CLOUD COMPUTING, 2015.

[10] Bijayalaxmi Purohit, Pawan Singh, " Data leakage analysis on cloud computing", International Journal of Engineering Research and Applications (IJERA), III(III), PP. 1311-1316, 2013.

[11] Sheetal Kalra, Sandeep Sood, "ECC-based anti-phishing protocol for cloud computing services", International Journal of Security and Networks,VIII(III), (2013.).

[12] Yu-Jia Chen, Li-Chun Wang, Chen-Hung Liao, " Eavesdropping Prevention for Network Coding Encrypted Cloud Storage Systems", IEEE Transactions on Parallel and Distributed Systems, 2015.

[13] Yi Han, Jeffrey Chan, Tansu Alpcan, Christopher Leckie, " Using Virtual Machine Allocation Policies to Defend Against Co-resident Attacks in Cloud Computing",IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING,2015.

[14] B. Kranmai, Prof. A. Damodaram, "Extenuate DDoS Attacks in Cloud",2nd International Conference on Applied and Theoretical Computing and Communication Technology (ICATCCT):IEEE, pp. 235-238,2016.

[15] Seviş Nur Kamile , Şeker Ensar. "Survey on Data Integrity in Cloud", IEEE 3rd International Conference on Cyber Security and Cloud Computing: IEEE, pp. 167-171,2016

[16] Qiao Yan, Richard Yu, "Distributed Denial of Service Attacks in Software-Defined Networking with Cloud Computing", SECURITY AND PRIVACY IN EMERGING NETWORKS:IEEE Communication Magazine, pp. 52-59, April 2015.

[17] Rossi D, Miguel G. Xavier, Rajkumar Buyya, "E-Eco: Performance-aware energy-efficient cloud data center orchestration", Journal of network and Computer Applications: Elsevier, 78, pp. 83-93,2017.

[18] Ehsan Arianyan, Hassan Taheri, Vahid Khoshdel, "Novel Fuzzy multi objective DVFS-aware consolidation heuristics for energy and SLA efficient resource management in cloud data centers", Journal of network and computer applications:Elsevier,78, pp. 43-61, 2017.

[19] Zhang Yingjie,"Energy efficiency techniques in machining process: A review", International journal of Adv Manuf. Technology: Springer, pp. 1123-1132, 2014.

[20] Fan Yuqu, Hongli Ding, Lusheng Wang, Xiaojing Yuan, "Green latency-aware data placement in data centers"; Computer Networks: Elsevier, 110, pp. 46-57, 2016.

[21] Hammami Ali, Simoni Noemie and Salman Rasha, "Ubiquity and Quality for Cloud Security", 41st International conference on parallel processing Workshops, pp. 277-278, 2012.

[22] Tao Chen, Xiaofeng Gao and Guihai Chen, " The features, hardware, and architectures of data center networks: A Survey", Journal of Parallel Distributing Computing: Elsevier, 96, pp. 45-74 , 2016.

[23] Bansidhar Joshi, Bineet Joshi and Kritika Rani, "Mitigating Data Segregation and Privacy Issues in Cloud Computing", Proceedings of International conferences on communication and networks, Advances in Intelligent systems and computing: Springer", 508, pp. 175-182, 2017.

[24] M. Durairaj and A. Manimaran, "A Study on Security issues in Cloud based E-Learning", Indian journal of Science and Technology, VIII(VIII) , pp. 757-765,

April 2015.

[25] D. Aruna Kumari, M. Chandrika and B. Surekha Ratnam Bhardwaj, Indian journal of Science and Technology, IX(XVII), May 2016.