International Journal of Engineering & Technology, 7 (3.34) (2018) 758-761

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

A Survey on Security Issues in Cloud Computing

Pushpalatha V1, Sudeepa K B 2, Mahendra H N3

1,2Department of Computer Science and Engineering, NMAMIT, Nitte
3Deaprtment of Electronics and Communication Engineering, Alva's IET, Moodbidri
**Corresponding author Email: 1pushpav27@gmail.com , 2sudeepa@nitte.edu.in , 3mahendrahn@aiet.org.in*

Abstract

Cloud computing is an approach to elaborate the limit and adding the endowment without adding the resourcesinto the modern framework, organizing new process, or authorizing new programming. Cloud computing is the major outcome of the composition of the traditional enrolling development and system development like matrix multiplication, distributed computing, parallel computing and etc. The cloud computing will allows the information allocation that consists of software, policy and infrastructure, which defines the virtualization. Cloud computing is the design which provides the services through internet on paper use access to store the information like storage, servers and applications, without its physical existence. This paper gives outlines that what is meant by the cloud computing means, various cloud computing models such as cloud deployment model, and the cloud service models and the security issues that is faced by the cloud computing model, and the various existing security solutions. This paper is a survey of security issues and security challenges in the world of cloud computing which provides the various aspects of cloud computing.

Keywords: Cloud Computing, Security Issues, Cloud Security,Encryption, Authentication.

I. Introduction

Cloud computing is a web build enrolling which depends regarding sharing of the advantages, for instance, server, storing, applications through web and the goal is to give predominant figuring. The cloud computing can be defined as the parallel and distributed system which includes the collection of inter-connection information based on the service-level agreements (SLA). The single security method cannot give the solutions for the security and the privacy in cloud [1]. There are different service models in cloud computing to provide services to cloud; they are Platform-as-a-service (PaaS), Infrastructure-as-a-service (IaaS), and Software-as-a-service (SaaS) [10].

It has a power to empowerment, reliability, scalability, availability, agility, performance, multi-tenancy, security and maintenance. The US National Institute of Standards andTechnology (NIST) defines cloud as follows: "Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with a minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three delivery models, and four deployment models" [18].

Cloud computing is a conveyed engineering that consolidate the server data in a systematic way so that it provides the computing information services when the user is request. The cloud service provider (CSP) allows the cloud infrastructure to their customer to use and to establish their own web services like Internet Service Provider (ISP), High-Speed broadband [9]. The cloud computing integrate the various range of computing concepts and technologies, such as, Service Oriented Architecture (SOA), virtualization, web 2.0 and many other technologies which dependent on internet,

supplying commonplace business programs online via net browsers to fulfil the user requirements in the cloud computing, at the same time as their softwareand statistics are stored on the servers [11].

There are three cloud service models and four cloud deployment models are discussed in this paper. Mainly there are 4 types of clouds are defined such as public cloud, private cloud, community cloud and the hybrid cloud [10].

2. Cloud Computing Models

The cloud computing models is divided into two major models namely, cloud service model and the cloud deployment model.

2.1. Cloud Deployment Model

There are four different deployment models of cloud computing they are public cloud, private cloud, community cloud, and hybrid cloud.

1) Private cloud: The private organization uses the privatecloud model. The private cloud can be maintained either by the organization or by the third party [7]. The private clouds are owned and managed by the organization or a third party, and it may exists either within the organization premises or may exists out of the organization premises[9].

2) Public Cloud: The cloud operational permission is givento numerous users and it is handled by an outsider, it exist beyond the firewall of the company. The public cloud can be hosted and managed by the cloud designer and they are fully responsible for installation, management and maintenance of the cloud [9]. The user allowed to access the cloud via web browser. These clouds are based on the pay-per-use model.

These public cloud provides the less security when compare to the private cloud, because these clouds are allowed to access by many users so it's less secure [7].

3) Hybrid Cloud: A hybrid cloud is a combination of two ormore different types cloud. The hybrid cloud should contain at least one public cloud and one private cloud [7]. The clouds are linked in such a way that data transfer takes place between each other without affecting each other. The hybrid cloud should provide the security for the user in such way that the customer payments information should not be accessed by the unauthorized user, like employee payroll processing. Thevarious sources must be gained and provisioned from different provided services as though they started from a particular one source area, and conservation between the public and private parts can make the usage much more elaborate [9]. Amazon Web Services are the example of a hybrid cloud.

4) Community Cloud: The cloud establishment isprovisioned for remarkable utilized by technique for a choose group of customers from clusters that have shared concerns (e.g., mission, wellbeing necessities, policy, and consistence contemplations) [9]. The main concern of the community cloud is to have many active organizations to understand the advantages of the public cloud like multi-tenancy and pay-as-you-go billing structure with having a high privacy, security and policy compliance, it is usually associated with the private cloud [7]. A community cloud can be used either on premise or off-premise of the organization.

platform that consists of many server, and operating systems. [1]. Platform-as-a-service (PaaS) is an application advancement and deployment platform is also delivered as a service to the cloud provider on the internet [15]. PaaS is the registering stage and the arrangement organized as a service, and it doesn't require to download the software or no need of provider or developer to install the software to the computing system [9].

3) Software-as-a-Service: The Software-as-a-Service (SaaS) is also defined as a processes in which Application Service Provider (ASP) which provides unique software application over the web. This service makes installation and usage of the application made easy to the user, it means that user or the customer can freely get the usage of the service and also this service eliminates the risk of maintain the software [9]. Providing the security and privacy for the service is responsibility of the service provider [13]. The service provider will allow the user to use the service. To purchase or own the software is not required for user, but they use the software on the internet and the customer need to pay to use the software [10]. SaaS is periodically executed to provide the business programming importance to big business users who require small or no exertion while enabling those users to secure similar applications of monetarily approved, inside worked programming without the related multifaceted nature of foundation, organization, reinforce, allowing, and high starting cost [16].

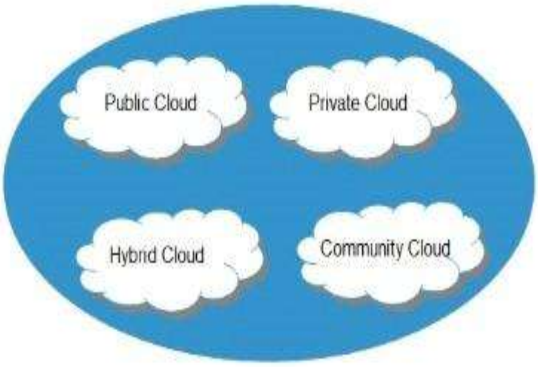

Fig. 1: Cloud Deployment Models

2.2. Cloud Service Models

The following security thought with the different cloud computing service models. There are 3 different models they are: Infrastructure-as-a-Service (IaaS), Software-as-a-service (SaaS), and Platform-as-a-service (PaaS).

1) Infrastructure-as-a-Service:The IaaS it delivers thevirtual machine images as a service and the machine can be designed based on the developer's needs. The user or customer can use this service as a resource instead of buying the servers, software, data centre information, network machines, and the expert person to operate them [10]. The cloud developer should provide basic and low-level data protection capabilities [13].

2) Platform-as-a-Service: The main goal of the service is to enable cloud provider to develop their own applications on reference to the platform provided [13]. The virtualized

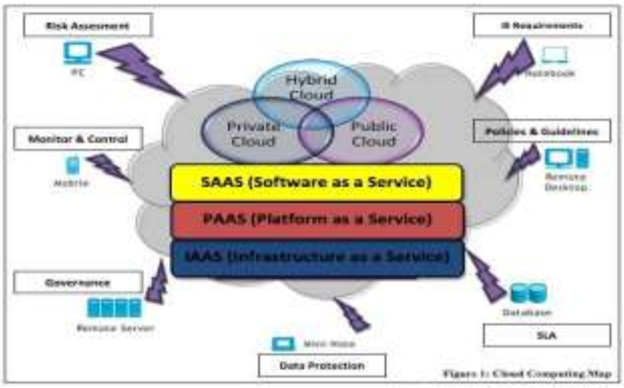

Fig. 2: Cloud Computing Map

3. Cloud Computing Security Issues

In this section discuss about different security issues in cloud computing.

3.1. Components Affecting Cloud Computing

There are many security issues that are affecting the cloud computing as it support many innovation, it also consists of virtualization, resource allocation, management, database, operating system, memory management. Since many systems are connected to each other the cloud must be secure in the could network to maintain the security of the cloud over the internet. Encryption and decryption are the technique used to secure the data. Concurrency control involves encrypting the data and also it ensure that specific proper approach or method is used in data sharing [1].

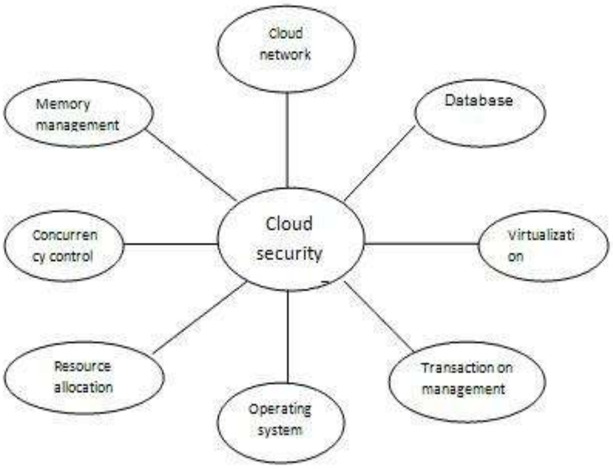

Fig. 3: Components Affecting Cloud Computing

3.2. Security Issues Faced By Cloud Computing

The service provider should take the responsibilities of the cloud and its security problem. The cloud provider should make sure that the user should not get any issues by using the cloud like data loss, data theft. Cloud provider or developer should use new approaches and the services which provide the more security for the cloud [1]. The security issues faced by the cloud computing are discussed in the following:
1) **Data Access Control:** In most of the cases the secret or theconfidential information is accessed unlawfully by the third party because of the not secure data access control.
2) **Data Integrity**: The data integrity occurs due to the wrong information that is entered by the human resource. The faults in the cloud may occur when the confidential data is being transformed by one system to the other system, or the error may occur because of the hardware breakdowns like disk crashes.
3) **Data Loss:** Data loss is the main problem in the cloudcomputing security. The unauthorized person or third party will be able to get the data shared when the works done in online like sharing of information of new development ideas, banking transactions, business information etc.
4) Data Theft: Usage of external data server for flexibility of the operations may causes the data theft.
5) **Privacy Issues:** Since most of the server external in thecloud security for the personal information of the customer is difficult.
6) User level Issues: Data loss or data theft may happen because of customer. The customer should make sure that because of their own changes made in the cloud, should not allow the third party or the unauthorized person to access the data.
7**) Security Issues** in Provider Level: Providing the goodsecurity to the cloud is the major responsibility of the service provider. They should provide strong security layer between the customer and user.

4. Exiting Security Solutions

The existing security solution for the cloud computing is discussed below.

4.1. Identity Based Authentication

Identity based encryption (IDE) is also called as public key strategy, where the ace public key and the ace private key will be generated by using private key. The ace private key is generated for client kind of data. The customer can decrypt the particular file and get access by using the ace private key. Private Key gives the identity of the customer [20]. The principle disadvantage in the identity based encryption will completely trust the private key because it consists of all the private keys [19]. The identity based public key system is an alternative for the public key cryptography which provide the privacy to the each user. The user and the trusted third party i.e. the private key generator. Identity based public key system that overcome the drawback of the public key cryptography. The key generator is responsible for creating a unique private key to the each user using the identity information of the user [21].

4.2. Role Based Model

The information proprietor should encrypt the data in their personal system before loading the original data into the cloud system then the user can deploy the data to the cloud which is encrypted by the information proprietor. The data is cannot easily accessed by the users which is stored in the cloud. Roles are given to the each user based on their responsibilities and qualification. The role is assigned to the each user by the role manager, if the user is failed to perform the role assigned then the role manager has an ability to take the role back which is assign to that particular user [20]. If the role is not properly assigned to the user then it's difficult to access the data from the cloud to the cloud provider, user and others. If the user found as unauthorized user then that user will be revoked from the roles [19].

4.3. Attribute Based Encryption

The attribute based encryption is a public key encryption.
Based on the user attributes, system allows the client to encrypt or decrypt the message. The attribute based encryption has two different types that is Key-Policy attribute based encryption and the Ciphertext-Policy attribute based encryption [22]. The trusted user will generate the keys for information proprietor and to the user. This technique generates the key based on the attribute [19]. The information proprietor will play major role to encrypt the data with the key provided to the client and the client is allowed to decrypt the data by using his own private key. The advantages of this type is, 1.The attribute based encryption decreases the communication that happen through the web. 2. The attribute based encryption gives the secure access control [20].

4.4. Key-Policy Based Encryption

The private key will be issued by the trusted party which is associated with the tree structure which helps to describe the user identity. The Ciphertext is combined with the set of attributes in the key-policy based encryption [19]. To identify the which types of encrypted data can be decrypted by using the access policy. The user key will issued by the trusted authority. The major disadvantage of key-policy based encryption is the owner will have no idea about who can encrypt the data [20].

4.5. Ciphertext Policy based Attributes Based Encryption

In the ciphertext policy based encryption, the private key is consists of set of attributes. To specify the encryption policy the ciphertext is developed with access structure. On the off chance that the qualities in the private key is completely fulfilled the entrance tree in the ciphertext at that point there will is an arrangement to the client or customer to motivate approval to unscramble the ciphertext. In the ciphertext policy based encryption the information proprietor holds the ascendancy about the encryption policy [19].

4.6. Hierarchical Attribute Set based Encryption

The ciphertext-policy attribute set based encryption is prior form of the hierarchical attribute set based encryption with the hierarchical structure. The encrypted data can be accessed by the users by using their own private key. To manage the lower-level data the master-key will be provided by the higher level authority. Client can recover the encoded information by utilizing their own particular private key [20].

4.7. Multi Authority

Multi-specialist Ciphertext-policy attribute based encryption is more reasonable for information get to control, different experts issued the credits to clients and utilizing get to approach the information proprietor share the information characterized over properties from various authorities. In this system, clients' characteristics can be changed powerfully. A client might be assign with new traits or denied some present qualities, at that point information access ought to be changed in like manner. Every datum proprietor before scrambling the information, they isolate the information into various parts and every part is encode with substance keys by utilizing symmetric encryption systems. At that point, the proprietor characterizes the entrance arrangements over traits from various property experts and encodes the substance keys under the approaches [20].

5. Conclusion

In this paper we have talked about significant security issues, different computing models and currently available solutions for the cloud computing security. The detailed discussion in the survey paper will gives complete information about security issues which is faced by cloud, and defiantly this will helps us to start research in the field of cloud computing.

References

[1] Randeep Kaur and Jagroop Kaur, “Cloud Computing Security Issues and its Solution: A Review”, IEEE International Conference on Computing for Sustainable Global Development, pp. 1198-2000, 2015.

[2] Jianfeng Yang and Zhibin Chen, “Cloud Computing Research and Security Issues”, IEEE international Conference onHYPERLINK "http://ieeexplore.ieee.org/xpl/mostRecentIssue.jsp?punumber=5676124" ComputationalIntelligence and Software Engineering (CiSE), 2010.

[3] Kui Ren, Cong Wang, and Qian Wang, “Security Challenges for the Public Cloud”, IEEE Computer Society, pp. 69-73, 2012.

[4] Pengfei You, Yuxing Peng, Weidong Liu, and Shoufu Xue, “Security Issues and Solutions in Cloud Computing”, pp. 573-577, 2012.

[5] Huaglory Tianfield, “Security Issues in Cloud Computing”, IEEE International Conference on Systems, Man, and Cybernetics, pp. 1082-1089, 2012.

[6] Akhil behl, Kanika behl, “An Analysis of Security Issues in Cloud Computing”, IEEE world congress on Information and communication Technologies, pp. 109-114, 2012.

[7] Mutum Zico Meetei and Anita Goel, “Security Issues in Cloud Computing”, 5th International Conference on Bio Medical Engineering and Informatics (BMEI 2012), pp. 1321-1325, 2012.

[8] Kevin Hamlen, Murat Kantarcioglu, Latifur Khan, Bhavani Thuraisingham, “Security Issues for Cloud Computing”, International Journal of Information Security and Privacy, pp. 39-51, 2010.

[9] Rabi Prasad Padhy, Manas Ranjan Patra, Suresh Chandra Satapathy, “Cloud Computing: Security Issues and Research Challenges”, IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS) Vol. 1, No. 2, pp. 136-145, 2011 .

[10] L. Ertaul, S. Singhal, , and G. Saldamli, “ Security Challenges in Cloud Computing” California Sate university, 2010..

[11] Keiko Hashizume, David G Rosado, Eduardo Fernández-Medina, and Eduardo B Fernandez, “An Analysis of security issues for cloud computing”, Journal of Internet Services and Applications, pp. 1-13, 2013.

[12] Nelson Gonzalez, Charles Miers, Fernando Red´ıgolo, Marcos Simpl´ıcio, Tereza Carvalho, Mats Na¨ slund and Makan Pourzandi, “A quantitative analysis of current security concerns and solutions for cloud computing”, Journal of Cloud Computing: Advances, Systems and Applications, A Springer Journal, pp. 1-18, 2012.

[13] Hassan Takabi and James b.d. JosHi, “Security and Privacy Challenges in /cloud Computing Enviornments”, The IEEE Computer and Reliability Societies, pp. 1540-7993, 2010

[14] Chaoqun Yu, Lin Yang, Yuan Liu, Xiangyang Luo, “Research on Data Security Issues of Cloud Computing” IEEE International conference on Cyberspace technology, May 2015.

[15] Awwab Mohammad, Sanna Mehraj Kak, M. Afshar Alam, “Cloud Computing: Issues and Security Challenges”, International Journal of Advanced Research in Computer Science, Volume 8, No. 2, pp. 26-28, March 2017.

[16] Kuyoro S. O., Ibikunle F., Awodele O, “Cloud Computing Security Issues and Challenges”, International Journal of Computer Networks (IJCN), Volume 3, pp. 247-255, 2011.

[17] Mr. G. Nanda Kishor Kumar and Mr. M. Naresh, “Security Threats in Cloud Computing”, International Conference on Emerging Trends in engineering, Science and Management, pp. 983-992, 2017.

[18] R. Kalaichelvi Chandrahasan, S Shanmuga Priya and Dr. L. Arockiam, “Research Challenges and Security Issues in Cloud Computing”, International Journal of Computational Intelligence and Information Security, March 2012 Vol. 3, No. 3

[19] R Charanya, M Aramudhan, “Survey on Access Control Issues in Cloud Computing’, IEEE International Conference on Emerging Trends, 2016.

[20] Neha Bairagi, Prof. Saurabh Kapoor, “Survey on User

[21] Chung-Peng Huang, “Identity-Based Encryption with Cloud Revocation Authority and Its Applications”, IEEE, Transaction on Cloud Computing, pp. 1-14, 2015.

[22] Tianyu Zhao, Lingbo Wei, Chi Zhang, “Attribute-Based Encryption Scheme Based on SIFF”, IEEE ICC 2016 Communication and Information Systems Security Symposium, 2016.