IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

A REVIEW ON CLOUD COMPUTING AND SECURITY

[1]Mr. Ravi Prakash Vishwakarma, [2] Dr. Habib Ur Rahman

[1]Research scholar, [2]Associate Professor,
Computer Science Engineering department
Kanpur Institute of Technology, Kanpur, India

Abstract: Cloud computing has become one of the most interesting topics in the IT world today. Cloud model of computing as a resource has changed the landscape of computing as it promises of increased greater reliability, massive scalability, and decreased costs have attracted businesses and individuals alike. It adds capabilities to Information Technology's. Over the last few years, cloud computing has grown considerably in Information Technology. As more and more information of individuals and companies are placed in the cloud, there is a growing concern about the safety of information. Many Companies that are considered to be giants in software industry like Microsoft are joining to develop Cloud services. Despite the hype about the cloud, customers are reluctant to deploy their business in the cloud. Security issues is one of the biggest concerns that has been affecting the growth of cloud computing. It adds complications with data privacy and data protection continues to affect the market. Users need to understand the risk of data breaches in the cloud environment. The paper highlights issues related to cloud computing.

Index Terms **- Cloud computing, security Issue.**

I. INTRODUCTION

Cloud means a wide range of scalable services that users can access via an Internet connection. Providers like Microsoft, Amazon, Google and many more provide various cloud-based services for which users can pay on the basis of service subscription and consumption. Many providers offer a wide range of Cloud services like Messaging, Social Computing, Storage, CRM, Identity management, Content Management etc. Cloud computing is dependent on resource sharing. Using internet enabled devices, cloud computing permits the function of application software. Cloud computing is also known as the cloud. Cloud computing serves a wide range of functions over the Internet like storage. Taking advantage of resource sharing, cloud computing is able to achieve consistency and economies of scale. Types of cloud computing can be classified on basis of two models. Cloud computing service models and cloud computing deployment models. It is a file backup shape. It also allows working on the same document for several jobs of different types. Cloud computing simplifies usage by allowing overcoming the limitations of traditional computer. A cloud service is used by clients as and when needed, usually on hourly basis. This pay as you go approach has made the cloud flexible such that where end user can have services the way they desire at any point of time and the cloud services is entirely monitored by the provider. There are some of the basic security threats that have exploited the usage of Cloud Computing. An example of security threat is botnets, the use of botnets to spread spam and malware. Of the 761 data breaches investigated in 2010 by the U.S. Secret Service, almost 63% occurred at companies with 100 or fewer employees. And a 2011 survey by security systems provider Symantec Corp. around 2,000 plus small and midsize enterprises indicated that close to 73% had been breached by a cyber-attack. One of the best features of cloud computing is pay-as-you-go model of computing as a resource. This model of computing has enabled businesses and organizations in need of computing power to purchase as many resources as they need without the need to put forth a large capital investment in the IT infrastructure. Other advantages of cloud computing are scalability and increased flexibility for a relatively constant price. Cloud is the new trend in the evolution of the distributed systems. The user does not need knowledge or expertise to control the infrastructure of clouds, it provides abstraction. Cloud providers deliver common online business applications which are accessed from servers through web browser

II. CLOUDE COMPUTING MODELS: Cloud hosting deployment models are classified by the proprietorship, size and access. It tells about the nature of the cloud. Most of the organizations are willing to implement cloud since it reduces the expenditure and controls cost of operation.

A. Public Cloud

It is a type of cloud hosting in which the cloud services are delivered over a network that is open for public usage. This model is actually true representation of cloud hosting. In this the cloud model service provider provides services and infrastructure to various clients. Customers do not have any control over the location of the infrastructure. There may be very little or no difference between public and private clouds structural design except the level of security that are offered for various services given to the public cloud subscribers by the cloud hosting providers. Public cloud is suited for business which require managing load. Due to the decreasing capital overheads and operational cost the public cloud model is economical. Dealers may provide the free service or license policy like pay per user. The cost is shared by all the users in public cloud. It profits the customers by achieving economies of scale. Public cloud facilities may be available for free an e.g. of a public cloud is Google.

B. Private Cloud

It is also known as internal cloud. This platform for cloud computing is implemented on cloud-based secure environment and it is safeguarded by a firewall which is governed by the IT department that belongs to a particular corporate. Private cloud permits only the authorized users and gives the organization greater control over their data. The physical computers may be hosted internally or externally they provide the resources from a distinct pool to the private cloud services. Businesses having unanticipated or dynamic needs, assignments which are critical management demands and uptime requirements are better suited to adopt private cloud. In private cloud there is no need for additional security regulations and bandwidth limitations that can be present in a public cloud environment. Clients and Cloud providers have control of the infrastructure and improved security, since user's access and the networks used are restricted.

C. Hybrid Cloud

It is a type of cloud computing, which is integrated. It could constitute an arrangement of two or more cloud servers, i.e. either of the combination of private, public or community cloud that is bound together but remain individual entities. Hybrid clouds are capable of crossing isolation and overcoming boundaries by the provider; therefore, it cannot be simply categorized into public, private or community cloud. It allows the user to increase the capacity as well as the capability by assimilation, aggregation and customization with another cloud package / service. In a hybrid cloud, the resources are managed either in-house or by external providers. It is an adaptation between two platforms in which the workload exchanges between the private cloud and the public cloud as per the needs and demand of organization.

D. Community Cloud

It is a type of cloud hosting in which the setup is mutually shared between a lot of organizations which belong to a particular community like banks and trading firms. It is a multi-tenant setup that is shared among many organizations that belong to a group which has similar computing apprehensions. Theses community members usually share similar performance and security concerns. The main intention of the communities is to achieve business related objectives. Community cloud can be managed internally or can be managed by third party providers and hosted externally or internally. The cost is shared by specific organizations within the community therefore, community cloud has cost saving capacity. Organizations have realized that cloud hosting has a lot of potential. To be the best one must select the right type of cloud hosting Therefore, one need to know the business and analyse his/her demands. Once the appropriate type of cloud hosting is selected, one can achieve business related goals easily.

III. SECURITY ISSUES

Cloud service models not only provide different types of services to users but they also reveal information which adds to security issues and risks of cloud computing systems. IaaS which is located in the bottom layer, which directly provides the most powerful functionality of an entire cloud. IaaS also enables hackers to perform attacks, e.g. brute-forcing cracking, that need high computing power. Multiple virtual machines are supported by IaaS, gives an ideal platform for hackers to launch attacks that require a large number of attacking instances. Loss of data is another security risk of cloud models. Data in cloud models can be easily accessed by unauthorized internal employees, as well as external hackers. The internal employees can easily access data intentionally or accidently. External hackers may gain access to databases in such environments using hacking techniques like session hijacking and network channel eavesdropping. Virus and Trojan can be uploaded to cloud systems and can cause damage. It is important to identify the possible cloud threats in order to implement a system which has better security mechanisms to protect cloud computing environments.

IV. THREATES IN CLOUDE COMPUTING

A. Compromised credentials and broken authentication

Organizations/companies at times struggle with identity management as they try to grant permissions appropriate to the user's job role. They sometimes forget to remove user access when a job function changes or a user leaves the organization. The Anthem breach exposed more than 80 million customer records, was the result of stolen user credentials. Anthem had failed to deploy multifactor authentication, so when the attackers obtained the credentials, it was all over.

B. Data breaches

Cloud environments face many of the same threats as traditional corporate networks, but since a large amount of data is stored on cloud servers, providers have become an attractive target. The severity of the damage tends to depend on the sensitivity of the data that is exposed. Personal financial information grabs the headlines, but breaches involving government information, trade secrets can be more devastating. When a data breach takes place, a company may be subjected to legal action. Breach investigations and customer notifications can rack up significant costs.

C. Hacked interfaces and APIs

Today every cloud service and application now offer APIs. IT teams use these interfaces and APIs to manage and interact with cloud services, including those that offer cloud provisioning, management and monitoring. The security and availability of cloud services depend on the security of the API. Risk is increased with third parties who rely on APIs and build on these interfaces, as organizations may need to expose more services and credentials.

D. Account hijacking

Phishing, fraud, and software exploits are highly prevalent today, and cloud services add a new dimension to the threat because attackers can eavesdrop on activities, manipulate transactions, and modify data. Attackers may be able to use the cloud application to launch other attacks. Organizations must prohibit sharing of account credentials between users and services and must enable multifactor authentication schemes where available. Accounts, must be monitored so that every transaction should be traced to a human owner. The key is to protect account credentials from being stolen

E. Permanent data loss

Hackers have in the past have permanently deleted data from cloud to cause harm businesses and cloud data centers are as vulnerable to natural disasters as any facility. Cloud providers may recommend distributing applications and data across multiple zones for better protection. Adequate data backup measures and disaster recovery are very important. Daily data backup and off-site storage are very important with use of cloud environments. The burden of preventing data loss is not only of cloud service provider, but also of data provider.

F. DoS attacks

DoS attacks have been around for a long time and have gained prominence again thanks to cloud computing because they often affect availability. Systems may run slow or simply time out. These DoS attacks consume large amounts of processing power, a bill the customer may ultimately have to pay. High-volume DDoS attacks are very common, but organizations should also be aware of asymmetric and application-level DoS attacks, which target Web server and database vulnerabilities. Cloud providers are better poised to handle DoS attacks than their customers.

V. CONCLUSION: Cloud Computing is a new concept that presents quite a number of benefits for its users. But it also raises some security problems which may affect its usage. Understanding about the vulnerabilities existing in Cloud Computing will help organizations to make the shift towards using the Cloud. Since Cloud Computing leverages many technologies and it also inherits their security issues. Traditional web applications, virtualizations have been looked over but some of the solutions offered by cloud are immature or inexistent. We have presented security issues for cloud models: IaaS, PaaS, and IaaS, which differ depending on the model. As described in this paper, storage and networks are the biggest security concerns in Cloud Computing. Virtualization that allows multiple users to share a physical server is a major concern for cloud users. Virtual networks are target for some attacks. We have focused on this distinction, where we consider important to understand these issues.

REFERENCES

[1] B. R. KANDUKURI, R. PATURI V, A. RAKSHIT, "CLOUD SECURITY ISSUES", IN PROCEEDINGS OF IEEE INTERNATIONAL CONFERENCE ON SERVICES COMPUTING, PP. 517-520, 2009.

[2] Wayne A. Pauley, "Cloud Provider Transparency – An empirical evaluation", the IEEE computer and reliability societies, IEEE, November 2010, pp: 32 – 39.

[3] Journal of Engineering Science and Technology, Vol. 3 No. 4, pp. 2672-2676, April 2011 http://www.infoworld.com/article/3041078

[4] Cong Wang, Ning Cao, Kui Ren, Wenjing Lou, "Enabling Secure and Efficient Ranked Keyword Search over Outsourced Cloud Data", IEEE transactions on parallel and distributed systems, IEEE, Digital Object Indentifier 10.1109/TPDS.2011.282, 2011, pp: 1 – 14.

[5] Rittinghouse JW, Ransome JF: Security in the Cloud. In Cloud Computing. Implementation, Management, and Security, CRC Press; 2009.

[6] Jamil, D., Zaki, H. "Security issues in cloud computing and counter measures", International Journal of Engineering Science and Technology (IJEST) , Vol. 3 No. 4, pp: 2672-2676.

[7] Morsy MA, Grundy J, Müller I: An analysis of the Cloud Computing Security problem. In Proceedings of APSEC 2010 Cloud Workshop. Sydney, Australia: APSEC; 2010.

[8] Mohamed Magdy Mosbah, "Current Services in Cloud Computing: A Survey," International Journal of Computer Science, Engineering and Information Technology (IJCSEIT), Vol.3,No.5,October 2013.