© 2018 IJSRST | Volume 4 | Issue 8 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X
Themed Section: Science and Technology

Security Challenges of Service and Deployment Models

Sudheer Kumar Shriramoju
Project Manager, Wipro InfoTech, Hyderabad, India

ABSTRACT

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. This paper provides the security challenges of service and deployment models.

Keywords : Cloud Models, Service Model, Deployment Model.

I. INTRODUCTION

Software Developers describe Cloud in a different way than a System Administrator, while a Database Administrator may have different definition. 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 these 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. Cloud computing also provides more agility because it allows faster access. These hosted services are normally separated into three broad categories: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS). 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 US. 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. [2]. 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 [3].

II. SECURITY ISSUES IN CLOUD

Cloud computing comes with numerous possibilities and challenges simultaneously. Of the challenges, security is considered to be a critical barrier for cloud computing in its path to success. The security challenges for cloud computing approach are somewhat dynamic and vast. Data location is a crucial factor in cloud computing security. Location transparency is one of the prominent flexibilities for cloud computing, which is a security threat at the same time – without knowing the specific location of data storage, the provision of data protection act for some region might be severely affected and violated. Cloud users' personal data security is thus a crucial concern in a cloud computing environment. In terms of customers' personal or business data security, the strategic policies of the cloud providers are of highest significance as the technical security solely is not adequate to address the problem. Trust is another problem which raises security concerns to use cloud service for the reason that it is directly related to the credibility and authenticity of the cloud service providers. Trust establishment might become the key to establish a successful cloud computing environment. The provision of trust model is essential in cloud computing as this is a common interest area for all stakeholders for any given cloud computing scenario. Trust in cloud might be dependent on a number of factors among which some are automation management, human factors, processes and policies. Trust in cloud is not a technical security issue, but it is the most influential soft factor that is driven by security issues inherent in cloud computing to a great extent. All kinds of attacks that are applicable to a computer network and the data in transit equally applies to cloud based services – some threats in this category are man-in-the-middle attack, phishing, eavesdropping, sniffing and other similar attacks. DDoS (Distributed Denial of Service) attack is one common yet major attack for cloud computing infrastructure. The well known DDoS attack can be a potential problem for cloud computing, though not with any exception of having no option to mitigate this. The security of virtual machine will define the integrity and level of security of a cloud environment to greater extent. Accounting & authentication as well as using encryption falls within the practice of safe computing - they can be well considered as part of security concerns for cloud computing. However, it is important to distinguish between risk and security concerns in this regard. For example, vendor lock-in might be considered as one of the possible risks in cloud based services which do not essentially have to be related to security aspects. On the contrary, using specific type of operating system (e.g. open- source vs. proprietary) might pose security threat and concerns which, of course,

is a security risk. Other examples of business risks of cloud computing could be licensing issues, service unavailability, provider's business discontinuity that do not fall within the security concerns from a technical viewpoint. Thus, in cloud computing context, a security concern is always some type of risk but any risk cannot be blindly judged to be a security concern. Allocation of responsibilities among the parties involved in a cloud computing infrastructure might result in experiencing inconsistency which might eventually lead to a situation with security vulnerabilities. Like any other network scenario, the provision of insider-attack remains as a valid threat for cloud computing. Any security tools or other kinds of software used in a cloud environment might have security loopholes which in turn would pose security risks to the cloud infrastructure itself. The problem with third party APIs as well as spammers are threats to the cloud environment.

As cloud computing normally means using public networks and subsequently putting the transmitting data exposed to the world, cyber attacks in any form are anticipated for cloud computing. The existing contemporary cloud based services have been found to suffer from vulnerability issues with the existence of possible security loopholes that could be exploited by an attacker. Security and privacy both are concerns in cloud computing due to the nature of such computing approach. The approach by which cloud computing is done has made it prone to both information security and network security issues. Third party relationship might emerge as a risk for cloud environment along with other security threats inherent in infrastructural and virtual machine aspects. Factors like software bugs, social engineering, human errors make the security for cloud a dynamically challenging one. Intrusion detection is the most important role in seamless network monitoring to reduce security risks. If the contemporary IDSs (Intrusion detection Systems) are inefficient, the resultant consequence might be undetected security breach for cloud environment.

The facets from which the security threat might be introduced into a cloud environment are numerous ranging from database, virtual servers, and network to operating systems, load balancing, memory management and concurrency control. Data segregation and session hijacking are two potential and unavoidable security threats for cloud users. One of the challenges for cloud computing is in its level of abstraction as well as dynamism in scalability which results in poorly defined security or infrastructural boundary. Privacy and its underlying concept might significantly vary in different regions and thus it may lead to security breach for cloud services in specific contexts and scenarios. Data loss and various botnets can come into action to breach security of cloud servers. Besides, multi-tenancy model is also an aspect that needs to be given attention when it comes to security. Security in the data-centres of cloud providers are also within the interests of security issues, as a single physical server would hold many clients' data making it a common shared platform in terms of physical server or operating system. The storage security at the cloud service providers data centres are also directly linked with the security of the cloud services. All the traditional security risks are thus applicable with added degree of potency in a cloud infrastructure which makes the ongoing success of cloud computing a quite challenging one. Confidentiality, availability and integrity are the generalized categories into which the security concerns of a cloud environment falls. Threats for a

cloud infrastructure are applicable both to data and infrastructure.

Different modes of data transfer and communication means (e.g. satellite communication) might need to take into account. Huge amount of data transfer is a common anticipation in a cloud environment, the communication technology used along with the security concerns of the adapted communication technology also becomes a security concern for the cloud computing approach. The broadcast nature of some communication technology is a core concern in this regard. Cloud environment is associated with both physical and virtual resources and they pose different level of security issues – having no sophisticated authentication mechanism to fully address the security threats is an existing problem for cloud computing. It has mainly resulted in the situations where grid computing has been taken as an embedded part of cloud computing. As the virtualized resources are highly coupled with a cloud infrastructure, intrusion related security concerns are of utmost priority as part of security issues. Arbitrary intermittent intrusion needs to be monitored in the operational context of a cloud computing infrastructure where the severity of possibility for a virtual machine to be compromised is to be taken into account. Some authors have argued that using Internet technologies is not a must for cloud computing- but the cost efficiency and globalization trends will enforce and motivate almost all the businesses to admit Internet and associated technologies to be the ultimate means towards cloud computing approach. As a result, total Internet related security concerns are anticipated to be automatically added on top of the cloud-specific security issues. Bringing portability is one of the means to make cloud services flexible. The portability of cloud services would also be associated with security concerns. Cloud portability enables the cloud users to switch among different cloud service providers without being affected with the necessity to change the ways to accomplish tasks in different ways. It is a clear provision on bargaining power for the cloud users; but at the same time, the security issues with cloud portability are to be counted. Cloud portability might bring severe degree of API based security threats.

The wide transition to mobile computing practices in recent years has made it imperative to include mobile computing and its associated technologies as an essential part of cloud computing. Resource scarcity as well as other constraints of mobile computing is barriers to cloud computing. The demand of huge data processing is a problem for mobile end-user devices which has been further complemented by the security concerns of mobile cloud computing. For mobile cloud computing, the device level limitations has inspired researchers to suggest the inclusion of another level of cloud termed as ‘mobile cloud’ to aid the processing of the specific computing and processing for mobile computing devices. The earlier explained broadcast nature of satellite communication and related security issues are equally applicable to the mobile cloud computing due to its being wireless communication. Besides, the addition of mobile cloud into the perspective would add another cloud with all its security issues for a service provider having both mobile cloud and conventional cloud. The addition of mobile cloud in the scenario would boost performance, but it would also add another layer of security issue not only to the mobile cloud users, but also to the total infrastructure of the cloud service provider. The hierarchical arrangement of cloud computing facilitates different level of extensibility for the

cloud users with varying degree of associated security issues. Security issues for cloud computing are described by some authors as an obvious one due to its nature. In a business model, the risks for the consumers are related to and dependent on the relevant approaches and policies of the cloud service providers the consumers are dealing with. Using cloud products or services may lead to security concerns for the consumers if they are not well aware with the type and particulars of the products or services they are to procure or to use in a cloud environment; this is also related to the cloud providers' identity and reliability. One of the inherent problems in this context is that, the consumers might normally not be able to identify or foresee all the risks involved in the specific cloud transaction they are dealing with or involved in.

III. SECURITY CHALLENGES OF SERVICE MODEL

Malicious attacks

Security threats can occur from both outside of and within organizations. According to the 2011 Cyber Security Watch Survey 21% of cyber-attacks were caused by insiders. 33% of the respondents thought the insider attacks were more costly and damaging to organizations. Generally, inside attacks were unauthorized access to and use of corporate information (63 %), and theft of intellectual property (32%). Malicious users can gain access to certain sensitive data and thus leading to data breaches. The malicious agenda can vary from data theft to revenge. In a cloud scenario, an insider can destroy whole infrastructures or manipulate or steal data. Systems that depend solely on the cloud service provider for security are at greatest risk.

Backup and Storage

The cloud vendor should ensure that regular backup of data is implemented that even ensure security with all measures. But the backup data is generally found in unencrypted form which can lead to misuse of the data by unauthorized people. Thus data backups lead to various security threats. More the server virtualization increases, an extremely difficult problem with backup and storage is created. Data de-duplication is one of the solutions to reduce backup and offline storage volumes.

Service hijacking

Service hijacking is means gaining illegal control on certain authorized services by unauthorized users. It can be through various techniques like phishing, exploitation of software and fraud. This is as one of the threats. Account Hijacking has been pointed as one of the most serious threats. The chances of hijacking account are incredibly high as no native

VM Hopping

The attacker can check the victim/users VM's resource procedure, alter the configurations and can even delete stored data which may be sensitive, therefore, putting it in danger the VM's confidentiality, integrity, and availability. A requirement for this type of attack is that the two VMs must be operating on the same host, and the attacker must be able to recognize the victim VM's IP address. Though PaaS and IaaS users have partial authority, an attacker may get hold of or decide the IP address using benchmark customer capabilities by using various tricks and combinational inputs to fetch user's IP. Thus it can be said that VM hopping is a rational threat in cloud computing.

IV. SECURITY CHALLENGES OF DEPLOYMENT MODEL

Platform-as-a-service (PaaS) security issues PaaS allows deployment of cloud-based applications without the cost of buying and maintaining the underlying hardware and software layers. PaaS depends on a secure and reliable network. PaaS application security constitutes two software layers: Security of the PaaS platform itself and Security of customer applications deployed on a PaaS platform.

Third-party relationships

PaaS along with traditional programming languages also offers third-party web services components such as mashups. Mashups can combine more than one source element into a single integrated unit. Therefore PaaS models have security issues which are related to mashups. PaaS users are dependent on both the security of web- hosted development tools and third-party services.

Development Life Cycle

From the point of view of the application development, developers may face the complexity of building secure applications that may be hosted in the cloud. The speed at which applications change in the cloud will affect both the security and System Development Life Cycle (SDLC). Software Developers have to keep in mind that PaaS applications must be upgraded frequently hence they have to make sure that their application development processes are flexible enough to keep up with changes. However, software developers should understand that any change in PaaS components can compromise the security of the applications. Other than secure development techniques, developers need to be educated and informed about data legal issues as well, so that data is not stored in inappropriate locations. Data may be stored in different places with different legal regimes that can include its privacy and security.

Underlying infrastructure security

In PaaS, software developers do not normally have access to the underlying layers, so providers are therefore responsible for securing the underlying infrastructure and the applications services. Even if developers are in control of the security, they do not have the assurance that the development environment tools provided by a PaaS provider are secure.

Cloning and Resource Pooling

Cloning means with replicating or duplicating the data.. Cloning can lead to data leakage problems which reveal the machine's authenticity. While [5] describes resource pooling as a service provided to the users by the provider to use various resources and share the same according to their application demand. Resource Pooling means unauthorized access due to sharing through the same network. Studies on Virtual and Cloud Computing by researchers state that a Virtual Machine can quite easily be provisioned, they can also be inversed to previous cases, paused and easily restarted and migrated between two servers, leading to non-auditable security threats

Unencrypted Data

Data encryption is a process that helps to solve various external and malicious threats. Unencrypted data is very vulnerable for susceptible data, as it does

not provide any security mechanism. Unencrypted data can very easily be accessed by unauthorized users. Unencrypted data risks the user data which leads to cloud server to escape various data information to unauthorized users. For example, the famous file sharing service Drop box was accused for using a single encryption key for all user data the company stored. These unencrypted, insecure data encourage the malicious users to misuse the data one or the other way.

V. CONCLUSION

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. This paper has provided the security challenges of service and deployment models.

VI. REFERENCES

[1]. J. and Hong, S. (2012). A Consolidated Authentication Model in Cloud Computing Environments. International Journal of Multimedia and Ubiquitous Engineering, 7(3), 151-160.

[2]. Kim, W. (2009). Cloud Computing: Today and Tomorrow. Journal of Object technology, 8(1), 65-72.

[3]. King, N.J. and Raja, V.T. (2012).Protecting the privacy and security of sensitive customer data in the cloud. Computer Law and Security Reviews, 28, 308-319.

[4]. Kumar, A. (2012). World of Cloud Computing & Security. International Journal of Cloud Computing and Services Science, 1(2), 53-58.

[5]. Kuyoro, S.O., Ibikunle, F. and Awodele, O. (2011). Cloud Computing Security Issues and Challenges. International Journal of Computer Networks, 3(5), 247-255.

[6]. Lee, K. (2012). Security Threats in Cloud Computing Environments. International Journal of Security and Its Application, 6(4), 25-32.

[7]. Sudheer Kumar Shriramoju,, “A Review on Database Security and Advantages of Database Management System”, Journal of Advances in Science and Technology, Vol. V, Issue No. X, August-2013

[8]. Sudheer Kumar Shriramoju, "Access Control and Density Based Notion of Clusters", International Journal of Scientific Research in Science and Technology (IJSRST), Online ISSN : 2395-602X, Print ISSN : 2395-6011, Volume 1 Issue 3, pp. 215-220, July-August 2015.

[9]. Sudheer Kumar Shriramoju, “Review on NoSQL Databases and Key Advantages of Sharepoint”, International Journal of Innovative Research in Science, Engineering and Technology, ISSN(Online): 2319-8753, ISSN (Print): 2347-6710, Vol. 7, Issue 11, November 2018.

[10]. Sudheer Kumar Shriramoju, “Capabilities and Impact of SharePoint On Business”, International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 2, Issue 6, November-December-2017.

[11]. Sudheer Kumar Shriramoju, “Security Level Access Error Leading to Inference and Mining Sequential Patterns”, International Journal of Scientific Research in Science, Engineering and

Technology, Volume 2, Issue 4, July-August 2016

[12]. Sudheer Kumar Shriramoju, “An Overview on Database Vulnerability and Mining Changes from Data Streams”, International Journal of Information Technology and Management, Vol. VII, Issue No. IX, August-2014

[13]. Sudheer Kumar Shriramoju, “A Comprehensive Review on Database Security Threats and Visualization Tool for Safety Analyst”, International Journal of Physical Education and Sports Sciences, Vol. 14, Issue No. 3, June-2019

[14]. Sudheer Kumar Shriramoju, “Integrating Information from Heterogeneous Data Sources and Row Level Security”, Journal of Advances and Scholarly Researches in Allied Education, Vol. IV, Issue No. VIII, October-2012

Cite this article as :

Sudheer Kumar Shriramoju, "Security Challenges of Service and Deployment Models", International Journal of Scientific Research in Science and Technology (IJSRST), Online ISSN : 2395-602X, Print ISSN : 2395-6011, Volume 4 Issue 8, pp. 733-740, May-June 2018.
Journal URL : http://ijsrst.com/IJSRST207494