Good argumentative essay on security threats for cloud computing

Law, Security

(Course No.)

(City & State)

INTRODUCTION

Cloud computing has presented new challenges and opportunities to industry IT. Cloud computing can be defined as a set of resources and services offered through the internet. The cloud services are provided from data centers located all over the world. Cloud service providers facilitate its consumers by providing virtual resources via the internet. An example of such a service is Google Apps provided by Google and Microsoft SharePoint. Cloud computing has been termed as a game-changer in scientific and industrial communities. It is increasingly infiltrating into industrial systems, businesses, government organizations, private entities and learning institutions. It is a result of evolution and combination of different technologies. Cloud computing presents many benefits to the industrial and business computing. It can be used for sharing business information resources to improve the capacity of information processing. However, the technology has presented new challenges. Cloud computing security has become the leading source of impediment to development. This paper explores the most vulnerable security challenges in the clouds, which will enable both cloud service providers and consumers to realize the key security threats associated with cloud computing. Thesis statement: In spite of the unparalleled benefits in the clouds, security threats and vulnerabilities have proved to be a constant impediment to its universal adoption and use.

Benefits of Cloud Computing

Cloud is defined by five essential features, four deployment models and three service models. Clod computing provides many benefits, among them include measured service, elasticity, on-demand service, broad network access, pooling of resources.

Security threats

The clouds provide three fundamental service models; SaaS, PaaS, and IaaS. SaaS model is based on a high degree of integrated functionality with minimal customer extensibility and control. IaaS, on the other hand, provide greater customer control over security due to lower degree of abstraction. The security issues can be analyzed basing on these service models.

SaaS service model security issues

With this model, the main issue and concern is the management of access to applications. With this model, there is the possibility of multi-tenancy. This enables the applications to be shared by many users on the cloud. This ability to share the application brings on many issues to the cloud users. This calls for cloud computing vendors to look into ways of offering data protection to the users of the clou8d. One security issue that arises with the SaaS service model is that of segregation and encryption. For a long time, the concern for many cloud computing vendors has been the many people who access the data application that has been installed in the cloud. The concern here has been the loss of control to the data. The multi-tenancy capability raises issues of identity management. How can the data of one company be identified by the cloud vendor? The issues that arise with the

use of the SaaS service model is that of the storage location of the data, operations of the system, and the flow of data transmission between the cloud and the organization. There is a need to ensure that there are strong encryption methods in order to have the security of the data to be assured. The transmission of the data to and from the cloud should be segregated to ensure security is achieved.

Data security in the clouds is not guaranteed. In SaaS, organizational data is processed in plain-text format and stored in the clouds. SaaS provider is mandated with the security of data during processing and storage. Third-party service providers contracted to provide backup services raises concerns together with disparate compliance and regulation issues arising from privacy, segregation and data security in their datacenters.

Accessibility of applications and data in the cloud is made easier via public computers and mobile devices but comes with an additional security tag arising from mobile malware, insecure Wi-Fi networks and proximity-based hacking.

PaaS service model

PaaS facilitates cloud-based application deployment without the need for hardware and software layers. Security issues include those associated with the platform itself and those of customer applications on PaaS. PaaS models inherit security vulnerabilities associated with third-party service components such as mashups in addition to web-hosted development tools and services.

With this model, the cloud computing vendor provides the platform and

environment where the developers can deploy their code. This means that the client can just connect to the PaaS cloud provider and start developing the applications that are used by users. One security issue with this setup is that of shared access and authentication of the environment. There are issues that come with this shared environment. With this environment, there are issues of authentication, access control, and authorization. There should be mechanisms that will ensure that the customers are completely kept separate from one another in the course of operations.

IaaS service model

There are security concerns that are experienced with this cloud computing model. One of the security issues with this model is that there are security concerns that are sourced from the host. The threats that are got from the host are as a result of the communication, monitoring, or the process of modifying the virtual machine. The monitoring process of the virtual machine from the host is considered to be an important process with the use of this service model. The control action includes shut down, pause, restart of the virtual machine, and the modification of the resources used by the virtual machine. With this cloud computing model, most of the security concerns rest with the IaaS provider. The networking is undertaken by the provider, the infrastructure, controlling the access to the network are all the functions that will be controlled by the IaaS provider. The process of designing, implementing, and inspecting the access control of the data will also be the mandate of the provider.

IaaS has the pool of resources such as servers, networks, storage, and

virtualized systems. Security is improved except in the management of the virtual machine monitor. Noted security issues include the extra layer created by virtualization may introduce a new attack platform. The compromise of one virtual machine leads to subsequent compromise of others. Shared resources between VMs decrease their security. Virtual machine rollbacks introduce security. Vulnerabilities and previously disabled accounts which is a security risk. The offline life cycle of the virtual machine presents vulnerabilities for malicious code and malwares. Virtual machine networks links (routed and bridged) presents window of attacks such as sniffing and virtual network spoofing.

Analysis

Cloud computing has been the spotlight of developments in technology. With this new technology, there are security concerns that come up with its adoption. One of the top security issues that come with cloud technology is data breaches. This is illustrated by how the virtual cloud can use side-channel timing so as to access private keys that are used for cryptographic functions. If the design of the multi-tenant applications is not done well, the flaws of one application that is used by one user will affect the other users of the application. The problem that is faced when trying to curb the issues of one application is that when trying to mitigate one security threat can exacerbate one application. This is because of the sharing process that is seen in the cloud computing technology. An organization can encrypt their data to reduce the breach that is caused by the security threats. If the encryption key is lost, there will be data loss.

There is the also the issue of data loss as a security threat. The data can be lost to a careless cloud provider because of the lack of good security infrastructure provided by the security provider. The encryption of the data so that the data loss is mitigated will backfire if the key is lost.

Another security threat that is common with cloud computing is that of account/service traffic hijacking. This is possible if the credentials that are used to gain access to the cloud is stolen by the attacker. The problem with this is that the activities that are undertaken at the organization will be monitored by the attacker by way of eavesdropping. With this information, the attacker can give information which is not true, can redirect the clients to other sites, and can also manipulate the data.

In spite of the numerous benefits it accords the users, its adoption is subject to some significant barriers. Some of the notable barriers are security, compliance, privacy and legal issues in that order. According to Morsy, (2010), cloud computing is a combination of disparate technologies each with their original security issues all of which are carried forward to the clouds. Traditional security mechanisms such as authentication, authorization and identity are insufficient to handle the heterogeneous, completely distributed and virtualized cloud environment. Therefore, the new paradigm represented by cloud computing poses a great uncertainty in the handling of security at all levels i. e. networks, host, application, and data.

It is, thus, clear that the security issues associated with the clouds surpasses the aforementioned benefits. This explains why most organizations have not been in the rush to adopt the cloud movement. The aforementioned security issues on each of the service delivery models can be summed up into two

main groups: Loss of control over data, and dependence on the cloud computing provider

These two issues have the potential of translating into legal and security concerns related to regulatory and legislative compliance, identity management. Others include access control, infrastructure, integrity control, access control and cloud computing provider dependent risks.

Lorna et al posit that client’s data stored by the Cloud Computing Provider can be compromised. This is because the data is out of the owners control and there is lack of transparency on how, when, why, and when their data is processed . Cloud service as stated earlier is a remote accessed service. The connection between the cloud service provider and the customer is not guaranteed of protection, and as such, security risks such as eavesdropping, DNS spoofing and Denial-of-Service is possible.

It can be argued that risk management approaches cannot be attained in the clouds. Irrespective of control of data and software hosted in the clouds, risk management and compliance issues are split between the client, internet provider and the cloud service provider. Since cloud data centers are geographically dispersed, regulatory and legislative compliance presents a problem since it is inadequately defined. Data protection and privacy legislation is different in many countries all over the world. Since Cloud Computing is a global service, problems and risks arises with data protection rules and privacy regulation in America when Cloud Computing servers are located in non-America locations.

In regards to Cloud Computing Provider dependence, availability issues arises in instances when the provider stopped providing services due to

bankruptcy, mergers or acquisitions.

Just like traditional services and utilities such as telecommunication, banking and gas with functionality controls, pricing, liability of the provider and reliability, Cloud computing standards have not been developed to define these parameters. Some of the widely used cloud computing services such as GoogleDocs do not include any contractual agreement between the provider and the user. Therefore, customers do not have anything to refer to in case of any incident.

Conclusion

Cloud computing is a relatively new paradigm that presents unparalleled benefits to its adopters. However, considerable security issues are raised potentially slowing down its adoption. Since cloud computing leverages many technologies, it inherits the individual security issues and potentially adds other compliance and legal complications pending the development of its universal framework and security standard. This paper has presented the security issues based on the IaaS, PaaS, and SaaS service models. The top most challenges encountered has to do with loss of control over data and Cloud Computing Providers dependence. This can be broken into virtualization, legislations, privacy and data storage among others.

References

Jinjun Chen, L. W., 2012. Special Issue: Cloud Computing 2011. Journal of Computer and System Sciences, Volume 78(Issue 5).

Lorna Uden, F. H. J. B. P., 2012. 7th International Conference on Knowledge Management in Organizations: Service and Cloud Computing. s. l.: Springer.

Morsy MA, G. J. M. I., 2010. An analysis of the Cloud Computing Security problem.. Sydney, APSEC.

Rittinghouse JW, R., 2009. Security in the Cloud. In: Cloud Computing. Implementation, Management, and Security,. s. l.: CRS.

Shaikh, F. H. S., 2011. Internet Technology and Secured Transactions (ICITST), 2011 International Conference for Computing. s. l., s. n.

Wei Wu, J. Z. Y. X. L. X., 2013. How to achieve non-repudiation of origin with privacy protection in cloud computing. Journal of Computer and System Sciences, Volume 79(Issue 8), pp. 1200-1213.

Zhiwei Wang, G. S. D. C., July 2013. A new definition of homomorphic signature for identity management in mobile cloud computing. Journal of Computer and System Sciences, pp. 97-103.