National Conference on Communication Technology & Network Security In association with
International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2019 IJSRCSEIT | Volume 4 | Issue 7 | ISSN : 2456-3307

Review on Cloud Security and Its Risk Over E-Commerce Network

Yamuna P
Assistant Professor, Department of Computer Applications Acharya Institute of Graduate Studies, Soladevanahalli, Karnataka, India

ABSTRACT

Many enterprises and businesses of all sizes take advantage of this subscription-based model in order to reduce IT costs which are often associated with traditional on premise applications. SaaS has been steadily growing over the past decade as many businesses adopt this new model of purchasing IT. The applications are remotely hosted by the service provider and can be accessed on demand by customers over the internet or private networks. This paper mainly focused on the architecture of cloud security; survey of the different security issues that has emanate due to the nature of the service delivery module of cloud system and type of attacks in cloud computing environment.

Keywords : Cloud computing, cloud security, cloud standards, cloud Risk, E-commerce Platform, software as a service (SaaS), platform as a service (PaaS), infrastructure as a service (IaaS).

I. INTRODUCTION

Cloud security, also known as cloud computing security, consists of a set of policies, controls, procedures and technologies that work together to protect cloud-based systems, data and infrastructure. These security measures are configured to protect data, support regulatory compliance and protect customers' privacy as well as setting authentication rules for individual users and devices. From authenticating access to filtering traffic, cloud security can be configured to the exact needs of the business. And because these rules can be configured and managed in one place, administration overheads are reduced and IT teams empowered to focus on other areas of the business.

The way cloud security is delivered will depend on the individual cloud provider or the cloud security solutions in place. However, implementation of cloud security processes should be a joint responsibility between the business owner and solution provider.

For businesses making the transition to the cloud, robust cloud security is imperative. Security threats are constantly evolving and becoming more sophisticated, and cloud computing is no less at risk than an on premise environment. For this reason, it is essential to work with a cloud provider that offers best-in-class security that has been customized for your infrastructure.

II. CLOUD SECURITY BENEFITS

- **Centralized security**: Just as cloud computing centralizes applications and data, cloud security centralizes protection. Cloud-based business networks consist of numerous devices and endpoints. Managing these entities centrally enhances traffic analysis and filtering, streamlines

the monitoring of network events and results in fewer software and policy updates

- **Reduced costs**: One of the benefits of utilizing cloud storage and security is that it eliminates the need to invest in dedicated hardware. Not only does this reduce capital expenditure, but it also reduces administrative overheads
- **Reduced Administration**: When you choose a reputable cloud services provider or cloud security platform, you can kiss goodbye to manual security configurations and almost constant security updates. These tasks can have a massive drain on resources, but when you move them to the cloud, all security administration happens in one place and is fully managed on your behalf.
- **Reliability**: Cloud computing services offer the ultimate in dependability. With the right cloud security measures in place, users can safely access data and applications within the cloud no matter where they are or what device they are using.

The Growth of Cloud-Based Applications

The rapid adoption of cloud computing technology in the form of rendered 'cloud services' makes it one of the hottest topics on the minds of IT and ecommerce leaders today. Cloud computing services are often referred to as a 'game-changer' amongst industry pundits, largely due to the opportunity the technology offers in organization-wide collaboration, enterprise-class scalability, and device agnostic availability while providing exceptional cost reduction advantages through optimized and efficient computing.

It is important to distinguish the three cloud computing classifications often referred to as the 'SPI model' where SPI refers to

- **Software as a Service (SaaS)**: offers users access to application software and databases.
- **Platform as a Service (PaaS)**: offers, beyond computing infrastructure, a development environment for application developers (e.g., operating systems, programming language execution environment, databases, etc.).
- **Infrastructure as a Service (IaaS)**: offers basic computing infrastructure (e.g., physical and virtual machines, location, network, backup, etc.).

All of the above SPI cloud service models can be deployed on one of the following four infrastructure deployment models

- Public cloud: the cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.
- Private cloud: the cloud infrastructure is operated solely for a single organization. It may be managed by the organization itself or by a third party and may be located on- premises or off-premises.
- Hybrid cloud: the cloud infrastructure is a combination of two or more clouds (private, community or public).

III. ADOPTION RATES

According to Gartner, the worldwide public cloud services market is projected to grow by 17.3% in 2019 to total $206.2 billion, up from $175.8 billion in 2018.

The growth projections are unevenly spread across SaaS, PaaS, and IaaS.

Infrastructure as a Service (IaaS) is expected to be the fastest-growing cloud services segment with forecasted growth of 27.6% in 2019 to reach $39.5 billion, up from $31 billion in 2018. Amazon is the leading vendor in the IaaS market, followed by Microsoft, Alibaba, Google, and IBM.

3.2 ADOPTION RATES BY VERTICAL.

Many organizations tend to start out with apps that could be easily migrated over to the cloud, and then transition their larger strategic systems such as their ecommerce platform, ERP and supply chain applications. These projects, tend to be integrated into their digital transformation plans.

A survey conducted by The Economist Intelligence Unit revealed the varying rate of cloud adoption across industries.

The first movers to the cloud appear to be digital "pure play" solutions that stand side-by-side with the legacy industry solutions, such as:

- ✓ Digital banking sprouting out of in-person branch banking.
- ✓ Ecommerce stores competing with brick-and-mortar retailers and shopping centers.

IV.CLOUD SECURITY RISK:

As industry trends show the ever-growing popularity and adoption of cloud technology, some organizations still seem hesitant to take the leap.
A Deloitte survey on cloud adoption showed that among a group of CIOs that have yet to implement cloud computing in their organizations, their main objections were:

- ✓ Risk of losing control and governance of data.
- ✓ Legal issues and open compliance.
- ✓ Risk of their data being exposed.
- ✓ Inadequate data security.

From the sub-group of CIOs yet to have adopted cloud technology, 78% of them, revealed that the major reason for non-adoption was their uncertainty in ecommerce security.

"The 'cloud security', is that if an organization stores their data in a third-party data center, they put themselves and their customers at risk of a data breach that will not only damage their organization's reputation but also have significant financial implications in the form loss of business and ultimately lead to penalties or fines."

V. SECURITY LAYERS IN ENTERPRISE SAAS, IAAS AND CLOUD- BASED APPLICATIONS

Cloud-based applications can be primarily categorized into two key layer:

- ✓ Layer 0, the IaaS (Infrastructure as a service) and PaaS (Platform as a service) cloud where everything else runs; typically, Amazon Web Services, Microsoft Azure, Google Cloud Platform, IBM Cloud, or Alibaba.
- ✓ Layer 1, SaaS and cloud-delivered applications that typically run on Layer 0 IaaS infrastructure.

Each layer has a set of both overlapping and distinct security considerations and standards.

5.1 LAYER 0 IAAS CLOUD SECURITY.

- ✓ The central security principle in all IaaS cloud rendered solutions is the concept of 'shared responsibility', which means two things:

- ✓ IaaS providers are responsible for the security of the cloud (e.g. global infrastructure, storage, databases, networking, and computer).
- ✓ Customers are responsible for security in the cloud (e.g. data, platforms, applications, operating systems, firewalls).

5.2 LAYER 1 SAAS CLOUD SECURITY.

- ✓ Data security should involve the use of strong encryption techniques and fine-grained authorization to control access to data.
- ✓ Achieve regulatory compliance, with the most important being
- ✓ Understand the deployment model of your SaaS vendors (i.e. if they will be using a public cloud vendor or hosting themselves).
- ✓ Availability: around the clock availability of service involves architectural changes at the application and infrastructure levels that add scalability and high availability. A load- balanced farm of application instances, running on a variable number of servers will provide resilience to denial of service attacks as well as hardware and/or software failures.
- ✓ Backups: enterprise data essentially needs to be regularly backed up to facilitate quick recovery in any event of a disaster. Strong encryption schemes need to be applied to all backup data.
- ✓ Credential Synchronization: The SaaS vendor supports replication of user account information and credentials between enterprise and SaaS application. User authentication is carried out by the SaaS vendor end using replicated credentials.

VI. SECURITY COMPLIANCE AUDITING.

Security compliance auditing is an assessment of a cloud services provider (CSP) to security- related requirements. At the very least a CSP should be able to ensure compliance with regulations and standards, as well as deploy their customers' applications and store their data securely. SaaS vendors that provide tenants with credible and trustworthy compliance information at any time hold a significant competitive advantage and are likely more reliable than others in comparison.

6.1 COMPLIANCE STANDARDS IN THE CLOUD.

There are two types of standards when ensuring compliance with different security frameworks in the cloud: vertical and horizontal. The horizontal standards may be applicable to many industries across the board, while the vertical standards are specific to each industry.

VII. BASE LEVEL SECURITY CHECKLIST OF IAAS SECURITY

✓ Asset Protection: Redundancy of IaaS Platforms

IaaS providers should guarantee that the data, and the hardware assets storing or processing it, are protected against physical tampering, loss, damage or seizure.

✓ Physical Security Mechanisms

The IaaS provider should offer an assurance that the data, disk images, and other storage, is appropriately protected – physically, logically or cryptographically. In the event that the organization is not satisfied with the protection provided by the IaaS provider, you should be able to deploy volume encryption of your data stores. Data erasure, sometimes referred to as data clearing or data wiping, allows you to completely destroy all electronic data with a software-based method that uses binary data (ones and zeros) to overwrite the data. You should verify with the IaaS provider where responsibility for erasing data lies

✓ Infrastructure security

Infrastructure security involves firewalls, robust encryption, and user authentication. Some IaaS services may directly expose client infrastructure to

public networks, such as the Internet. To establish infrastructure security, ensure that appropriate firewalls are deployed at both the infrastructure and platform level. Virtual networking can be used to separate management and back-end functionality from interfaces exposed to end-users. In situations where your IaaS provider does not offer granular interface control, virtual network security appliances may be useful. When data is intentionally shared with other users, you should have procedures in place to ensure it does not contain information which could give an attacker access to the service

VIII. CONCULSION

Data and ecommerce security is too important of a responsibility to employ alone. Plus, managing the servers and the teams that protect data can develop into a costly venture for any ecommerce business. Hosted ecommerce platforms are often more secure and don't require a high level of expertise compared to self-hosted software solutions. Each Big Commerce store is protected by multiple layers of security to prevent unauthorized access, including perimeter and server-specific firewalls, file integrity scanners, intrusion detection software, and 24/7 human monitoring. Online store data is also replicated on two data centers at a minimum, with backups hosted at a third site.

All Big Commerce plans offer HTTPS across the entire site. Shoppers can feel comfortable knowing an online store is secure from the first page they visit through the checkout process. Safeguarding data from breaches and managing all aspects of ecommerce security shouldn't strain a business. Big Commerce alleviates the pressure with unmatched security performance

IX. REFERENCES

[1]. Peter Mell and Timothy Grance, "The NIST Definition of Cloud Computing," Special Publication 800-145, September 2011, pages2—3,http://csrc.nist.gov/publications/nistpubs/800-145/SP800- 145.pdf. Short NIST document defining cloud computing models and services.

[2]. NIST Cloud Computing Reference Architecture," Special Publication 500-292, September 2011,pages15-17,http://collaborate.nist.gov/twiki_090611.pdf NIST document describing security expectations in a cloud computing environment. 3 By John Panagulias, "Cloud Computing: Platform as a Service Defined", Wednesday, August 5, 2009, http://cloud.kendallsquare.com/article/cloud-computingplatform-as-a-service-defined

[3]. Ian O'Rourke,"Being Too Glib about Cloud", October, 20012, http://www.elucidateit.net/?p=608

[4]. Defense Engineering, Inc.Partnering Technology with Business Needs, "Cloud Computing, http://www.defenginc.com/solutions/cloud_computing

[5]. Cloud Computing Ireland,"Hybrid Cloud", Nov 2012, http://cloudireland.ie/?page_id=9

[6]. Pradnesh Rane, Persistent System White Paper, "Securing SaaS Applications A cloud security perspective for Application Providers"

[7]. Oracle Wiring through an Enterprise Service Bus, 2009 http://www.oracle.com/technology/tech/soa/masteringsoa-series/part2.html accessed on:19Feb February 2010

[8]. Gajek S, Liao L, Schwenk J. Breaking and fixing the inline approach. In: SWS '07, Proceedings of the ACM workshop on secure web services. New York, NY, USA: ACM; 2007. p. 37-43.

[9]. Descher M, Masser P, Feilhauer T, Tjoa AM, Huemer D. Retaining data control to the client

in infrastructure clouds. In: International conference on avail

Cite this article as :

Yamuna P, "Review on Cloud Security and Its Risk Over E-Commerce Network", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 4 Issue 7, pp. 121-126, September-October 2019.
Journal URL : http://ijsrcseit.com/CSEIT194722