ISSN: 0975-766X
CODEN: IJPTFI
Research Article

Available Online through
www.ijptonline.com

A COMPARATIVESTUDY ON THE ECURITYMECHANISMSINCORPORATEDBY THE LEADING CLOUDSERVICE PROVIDERS

Sathiyamoorthy.E
School of Information Technology & Engineering, VIT University, Vellore-632 014.
Email:esathiyamoorthy@vit.ac.in

Received on: 15.10.2016 *Accepted on: 12.11.2016*

Abstract

Cloud Computing offers centralized, virtualized and scalable computing resources like applications, storage, network and server on demand basis as required by its customers. It creates a one-stop platform for the provision of variety of services and products inclusive of both hardware and software. The third parties who maintain and manage this massive storage environment are collectively called as Cloud Service Providers (CSP).It is the responsibility of the CSP to protect the data from various threats, attacks and vulnerabilities which stay as the hurdles in securing and preserving the privacy of the customer's data stored in the cloud. This work presents the survey of the various security mechanisms and principles followed by the leading CSP's and the unique features of their security policies to register themselves unique among their competitors. Also, this paper provides a comparative analysis based on the security characteristics followed by the CSP.

Keywords: Cloud Computing, Cloud Service Provider, Security Policies.

Introduction

Cloud Computing had created a drastic change in the IT infrastructure by providing the massive environment that acts as a single package in offering various resources and products needed by the customer to carry out their IT-based tasks without much difficulty. It also reduces the management overhead sets the customer free in deciding upon the services they need from the cloud and thus cloud is popularly called as the "pay as you use" service. Because of its openness and distributed architecture cloud faces many crises in the form of intruders, malicious attacks which makes it insecure. Customer faces problems due to this and loses their trust and confidence to migrate their data to cloud. CSP's main goal is to provide the services as requested by its clients in the most secure way possible so as to establish their supremacy in the cloud environment. Also, the Cloud Service Providers tries their best by adopting the most standard security procedures and frameworks and conduct periodic reviews and audit to check the compliance. Majority of the CSP adopts latest techniques and procedures to provide better security experience to its customers. The customer will not be aware of the processes used by the CSP, so to enhance the element of trustworthiness and belief in CSP, this paper keenly observes the security approaches followed by the leading CSP such as Amazon, Microsoft Azure and Google. This paper also presents the research oriented survey comparing the security methods used by three of the above mentioned companies so that it will be easy for the customer to be aware of their CSP's effort in securing their data and keep it highly confidential away from hackers.

Discussions

Amazon Web Services

AWS (Amazon Web Services) provides a scalable and reliable cloud computing platform for its customers so that they can run different varieties of applications. It is highly important and desirable that AWS provides its features in a secure fashion to withhold the confidence and trust of its customers. It follows a unique way of securing the services called shared security responsibility model which involves both the customer and the Cloud Service Provider (CSP) to take part in managing the resources in cloud. The CSP has to protect the underlying cloud infrastructure and the customer is responsible for the content that has been migrated to the cloud platform. This way of sharing the security responsibilities between the CSP and customer reduces the management and operation overhead at the customer side and gain authority over their account.

We shall start with discussing about the AWS security responsibilities followed by the individual customer responsibilities. Amazon Web Services provides security in two tiers based on the products and services called Global Infrastructure and Managed Services. Apart from these tiers, it also provides service-specific security configuration.AWS is responsible for securing the global infrastructure which runs all the services given by the Amazon Cloud. This global infrastructure consists of hardware, software and networking facilities which run the AWS services. As a customer, one cannot directly visit the cloud data center and check how his/her data is being secured by the Cloud Service Provider. So AWS periodically provides the security reports from the third-party auditors who confirms and verifies the security model's compliance with the standard security rules and regulations. Inaddition to this, AWS provides security features to its products called managed services. For instance, these services may include Amazon Dynamo DB, Amazon RDS, Amazon Red shift, Amazon Map Reduce and Amazon Workspaces. These services are named managed services since they are not only flexible and scalable but they also can be easily managed. It manages the basic security configuration like Guest Operating system, Disaster Recovery and Database Patching for the services opted by its customers. The customer's only task in securing these managed services is to maintain their account credentials safely and configure proper access control policies in order to keep their data safe in the cloud environment.

The following are the responsibilities of the customer in securing his/her data which has been moved to the cloud. Using AWS, the clients can avail the resources very quickly since it provides wide range of tools and analytics in a single package. Depending upon the type of services, the customer is choosing and how sensitive the data, the security configuration process varies for each client. The products can be classified into many categories such as Infrastructure as a Service (IaaS), managed services. Amazon EC2, Amazon VPC and Amazon S3 come under the IaaS category. For these products, the customer has to perform all the security and management tasks and is solely responsible for maintaining the tasks irrespective of the place where the servers are located. On the contrary, for managed services like Amazon RDS, Amazon Redshift, etc. the customer is not involved in maintaining the security and configuration tasks. Those works are carried out by the CSP itself. But the customers are expected to handle their user credentials properly by using the Amazon Identity and Access Management (IAM).

The next section talks about the Amazon Global Infrastructure Security. This provides a set of network, hardware and software facilities to manage the data installed upon the cloud. This infrastructure security follows the security policies, frameworks and compliance standards. Let us take a look at it.

The AWS compliance program consists of various standards and security frameworks that is aligned with the cloud infrastructure to provide the most feasible and trust-worthy security model to its customers. Some of the IT standards are SOC1, SOC2, SOC3, FISMA, ISO 9001/ISO 27001, etc. In addition to this, they are concerned about meeting some of the industry-specific standards such as CSA, HIPAA, FERPA, etc. It is equally important to secure both data stored in the cloud as well as the medium and environment in which it has been stored. The workstations where the cloud resources are stored are called Data centers. Amazon follows the best securitymechanism in protecting the data centers from intruders, hackers and other physical and environmental hazards. Each physical access is monitored thoroughly via video surveillance and intrusion detection system. The authorized individuals have to undergo a two-factor authentication to gain access to the data center floors. The persons other than staffs for instance visitors are identified and monitored continuously by the professional staff. For the employees, the access privileges are given based on their job positions. Fire detection and suppression is carried out by using automatic fire detection systems that has smoke-sensors installed in almost all of the rooms to provide alert in advance in case of any unexpected fire at the datacenters. The datacenters are fully equipped with power supply options 24*7 and also has backup-facility like UPS in case power shortage or electrical failure to ensure continued delivery of service to the customers. It is essentially important to keep the servers and other hardware devices at the datacenters to be at proper temperature and climatic conditions so that overheating can be reduced and outages can be avoided. All electrical, mechanical and other IT-oriented devices are maintained optimally and discrepancies in working in any of these devices shall be corrected as early as possible. When the storage devices had attained their fullest capacity of storage, it should be properly decommissioned so that the data is not fall into the hands of the intruders. The next section deals about the network security principles followed by the AWS. The customers are scattered across the globe and so the datacenters. Hence AWS follows world-class network security infrastructure that covers all the datacenters. The secure network architecture consists of enforcing ACL (Access Control List) to network and boundary devices like firewalls. These ACL's are approved by the Amazon Information Security section of AWS. To access the computing and analytics tools stored in the cloud, AWS provides secure HTTP (HTTPS) based access points. These access points allow customers to make communication in a secure fashion and retrieve the needed resources from the cloud. These customer-centric access points are called API endpoints. In order to connect to the AWS access points through HTTP/HTTPS, we can use a secure transmission protocol called SSL (Security Socket Layer) which protects the data in cloud from various malicious attacks such as eavesdropping, tampering and message forgery. There may be customers who need additional level of security.AWS provides a solution for these types of requests too by providing a private subnet called VPC (Virtual Private Cloud).It works by establishing the secure tunnel between the cloud data center and the Amazon VPC. The network segregation devices are usedto separate the Amazon corporate network from the Amazon production network. The people at the production side such as Developers and Administrated has to gain access to use the resources via AWS ticketing system. AWS has deployed fault-tolerant network architectures to satisfy the customer's need in spite of network traffic and server load. This is achieved by clubbing the data centers to form clusters. In case of failure of any data center, the task of that datacenter will be redirected to the nearby datacenter thereby balancing the server load.

Microsoft Windows Azure

Windows Azure is the cloud platform that provides application and web hosting services through MS data centers. When we take a look at the security mechanisms followed by Azure to meet the diverse and challenging needs of its customers, we shall find the two-way view of security. One is customer view followed by the Windows Azure view. Azure is basically built upon the infrastructure that consists of servers, applications, hardware and other relevant software needed for the computing environment. It supplies two basic elements namely compute and storage which keeps the customers to use the resources to build their applications. These are managed via a scheme called "Subscription" through which the clients are allowed to create valid credentials by using subscription portal. Once the account credentials have been created, the access is monitored by Windows LiveID which acts the authenticator. The subscription may include one or more hosted services or storage services as discussed earlier. The hosted service consists of deployments which is further categorized consists of roles and each role may consists of one or many instances. Coming to storage services, it consists of queues, tables and blobs. For all these elements, the authentication and authorization is done by the subscription.

Clients upload their applications in the cloud which could be further managed and accessed via the Windows Azure Portal directly or through SMAPI (Service Management API), a programmatic interface. This SMAPI provides authentication to the users based on cryptographic keys or self-signed certificate. The keys are either public or private generated by the users. The certificate is used to assess the sub sequential access to the SMAPI. To provide unique security mechanism for the storage services and accounts owned by the individual users, Azure supplies Storage Account Key (SAK).It can be modified by using the Azure portal or SMAPI.

Till now, we have seen an overview of the customer-centric security processes held at Azure and in this section we will get to know the detailed descriptionsabout the inner workings of the Azure through Azure view. It consists of the single element called fabric which encapsulates the compute and storage components of the infrastructure. For each role instances, it creates separate virtual machines (VM) which executes these roles on it. These VM's in turn run on the hypervisors. Now, it's time to take a look at the security design followed by the Windows Azure. It can be said that security can be described by using three classic dimensions such as Confidentiality, Integrity and Availability. Azure too does this job in a well-versed manner by promising all these components when a customer moves his/her data to the cloud. Apart from these three elements, it also serves another key element called Accountability. In other words, we can say that it provides transparency in viewing the happenings at cloud infrastructure so that the customers can able to manage and monitor their data storage. Let us discuss how it satisfies the three basic dimensions in cloud security. Confidentiality plays an important role in maintaining the trust of the customers. A proper security mechanism should only allow the authenticated and valid and access the resource from cloud. This is achieved in Azure by adopting the procedures such as IAM (Identity and Access Management), Isolation (logically or physically separating the confidential information) and Encryption (optional and it is used if rigorously needed by the customers).

The following are the steps followed by the IAM in maintaining the confidentiality of the information. SMAPI (Service Management API) is one of the key services of IAM which follows the REST (Representational State Transfer) protocol running over SSL (Secure Socket Layer). It is secured by a private key generated by the clients and a self-signed certificate which has a fingerprint authentication engraved within it. So as long as the key and certificate is maintained properly by the customer, it provides a higher level of abstraction and assurance to allow only the authenticated individuals. The next step is Least Privilege Customer Software which restricts the customers to own the administrative privileges in running the Virtual Machines. This preserves the resources from malicious attacks.SSL Mutual Authentication for Internal Control Traffic allows every transaction within the Azure environment to be protected by the SSL signed certificate.

The final step is the adoption of access control policies. After subscription through the Windows Azure portal, the users can create one or more storage accounts. Each and Every account has a secret key which opens door to access the resources contained within that account. The main functions that support the access control are divided into two namely Publicly readableand Shared Access signature. The former allows accessing only the non-sensitive content such as web images etc. The latter describes the work done by the storage servers in authentication. The IAM is followed by isolation and encryption. It is better to segregate the data and keep it under thorough surveillance rather than managing it as bulk content. This type of isolation reduces the management overhead and single point of access and protection. This is achieved at multiple levels starting from the hypervisor, root-OS and guest virtual machines level. In the next level, the fabric controllers are isolated followed by the isolation of the VLAN and then the customer access. The last one in achieving confidentiality is encryption. It has been a practice from ancient times to use cryptographic techniques to provide security the sensitive information and to restrict the illegal access from the intruders and hackers. Azure too employs encryption by integrating the .NET Cryptographic Service Providers (CSP) within it.

The second pillar of data security is integrity which means to protect the content from being altered by the unauthorized hands. Here, the design for integrity starts with the architecture of the fabric virtual machines. To explain more precisely, each VM is integrated along with three of the virtual hard drives (VHD) namely Drive C, Drive E and Drive D. The Information related to the Guest OS is contained in the Drive D. The Fabric Controller based images are stored in the Drive E. The configuration related content and other storage specific data are stored in the Drive C. Apart from this the simple access control model which has been described earlier is also used to provide two-level security to the data.

The key task of every CSP is to deliver the resources as per the demand and request of the customer 24*7.In short it has to provide continual delivery of services without any outages. To achieve this, it has to maintain the third pillar of security called Availability. Like every other CSP, Azure too follows the concept of replicating the servers (redundancy) by involving the virtualization technology. In case of any hardware malfunctioning, the data is diverted to the three nodes present in the fabric controller. There is an option for the customer to create second storage account and also develop customized roles to acquire the data from the storage and avail the backup facilities. On every VM, there is a monitor called Guest Agent which tracks and reports the status and working of the machine. If it fails to report, the Fabric Controller will restart the VM and check for consistencies. In case of any hardware fault, the FC develops new hardware node for replacing the old corrupted one to ensure the continuity of service.

Google

Google provides wide range of applications in the market of IT industry that covers maximumpopulation. We will cover in this section what are the security guidelines followed by it and how it is achieving the security configuration despite of its enormous audience. There are few security components listed by the Google which we will discuss one by one. Google corporate policies are nothing but security framework which encapsulates all the policies and guidelines that should be enacted by all the employees. These policy statements are audited and reviewed on a timely basis and it is updated as well to incorporate latest security elements. Periodic training will be given to the employees in handling the devices carefully without any security leakage, accompanying the data transfer among the nodes carefully and how to handle the sensitive data. Google's organizational security management team is fragmented into divisions to cover different aspects like information security, physical (hardware) security, global security followed by auditing and compliance procedures.

The information security team takes care of framing the rules and regulations and reviews its compliance to the security standards. It also does the job of collaborating all the third party vendors, auditors and public in constructing the policies and procedures. The Audit and Compliance team manages to check the adherence of those policies and procedures with the top security standards such as Payment Card Industry standards (PCI).The physical security team monitors the infrastructure of the data center and other workstations and reports if there is any malfunctioning. Maintaining the customer data securely is most important role of the CSP and Google handles this through Data Asset Management scheme. In this scheme, it follows the unique method of storing the customer's data. Instead of keeping all the data stored under one roof, it will segregate and store in a distributed environment.

There is an advanced fie system adopted by Google to store the structured and unstructured data called Google File System (GFS). For E.g.: Google BigTable. There should be proper mechanism to destroy the used data or unwanted information. Google follows separate policy for media disposal by involving the inspection of the customer to approve and verify the data destruction process. It also follows standard access control mechanisms to restrict the unauthorized access to the cloud environment. It adopts for modules in providing access control. In Authentication Control, it follows two-step authentication process which uses certificates and OTP (One Time Password).Coming to the Authorization controls, it defines access privileges for each employee based on his/her job position in the organization hierarchy. Even though the employees are allowed to access some default functions internally, they are restricted to access the high level secured applications.

Every access to the Google's resources is monitored by the specific staffs who log all those access entry through the process called Accounting. Google is maintaining the Employee Hand Book which contains all the basic information about each of the employee and Google is fully authorized to perform security and background checks upon employee orientation. It is essentially important to keep the place and theenvironment where the cloud data is stored safe and secure away from physical and environmental hazards and disasters. Google adopts the camera surveillance systems, security guards monitoring and fire alarm systems for immediate and quick tracking of the any unwanted and unexpected events which cause data loss.

Table 1. Comparison of Security Mechanisms.

S.NO	CHARACTERISTICS	AMAZON	MICROSOFT	GOOGLE
1.	Shared Security Responsibility (CSP + Customer)	✓		
2.	Physical and Environmental Security	✓	✓	✓
3.	Confidentiality, Availability, Integrity		✓	
4.	Access Control policies	✓	✓	✓
5.	Employee Training(Handbook)			✓
6.	Subscription based Network Security		✓	

7.	Service-specific Security	✓		
8.	Identity and Access Management	✓	✓	
9.	Media Disposal	✓	✓	✓
10.	Accountability		✓	

Conclusion

In spite of its advantages provided by the cloud computing, security threat acts as the hurdle in its path to attain customer trust. To avoid this, each and every CSP continues to strive towards self-sufficiency and adopts standards and techniques to retain the power among its sole competitors. This paper summarizes the principles used by the three of the leading CSP along with its comparison thus enabling its customers to analyze and guide them in decision making process.

References

1. https://d0.awsstatic.com/whitepapers/aws-security-whitepaper.pdf
2. http://www.smartbygep.com/pdf/Microsoft-Windows-Azure-Security-Overview.pdf
3. https://static.googleusercontent.com/media/www.google.co.in/en/IN/work/pdf/whygoogle/google-common-security-whitepaper.pdf
4. Acklyn Murray, et. al., Cloud Service Security & Application Vulnerability, Proceedings of the IEEE Southeast Conference- 2015.
5. Temesgen Kitaw Damenu and Chitra Balakrishna, Cloud Security Risk Management, 9th International Conference on Next Generation Mobile Applications, Services and Technologies - 2015.
6. Muthu Ramachandran and Victor Chang, Recommendations and Best Practices for Cloud Enterprise Security, IEEE 6th International Conference on Cloud Computing Technology and Science- 2014.
7. Tien-Cheu Kao, et. al., Cloud SSDLC: Cloud Security Governance Deployment Framework in Secure System Development Life Cycle, IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications -2012.
8. AkhilBehl, Emerging Security Challenges in Cloud Computing, World Congress on Information and Communication Technologies - 2011.