Microsoft and Amazon: A Comparison of Approaches to Cloud Security

Muthu Dayalan
Senior Software Developer,Chennai, India

Abstract—**Cloud security is an evolving technological paradigm that has several tremendous momenta in the technological and cloud data worlds. The importance of cloud computing security has been identified mainly as protection of data security of an organization. The architecture of cloud computing which involves the IaaS, PaaS, and SaaS whose cloud security architecture differ for the three-cloud computing architecture. Amazon utilizes the AWS while Microsoft utilizes Azure cloud computing approach. In this paper, an analysis on how the different features of the two cloud computing technologies for the two giants. Differences and similarities in computing, network, and storage features are provided. The strengths of Microsoft Azure in relation to AWS are also heighted. The paper concludes with a summary of the potential security threats in cloud security.**

Keywords— **cloud computing, data integrity, web services, NoSQL, servers, encryption, virtual machines, AWS, Azure, Cloud security.**

I. INTRODUCTION

Cloud computing security simply known as cloud security is a system that comprises of a set of policies, controls, procedures and technologies integrated with an objective of protecting the cloud-based systems, data and infrastructure of an organization. Cloud security has largely revolved and is being an essential part of the cloud data applications safety standards [1]. The security measures are configured to protect data, support regulatory compliance and protect consumers privacy. More so, the security system also is set as a system of authenticating rules for users and devices [2]. Cloud security is therefore, sorted through configuration to meet the exact needs of the business. With many organizations relying on cloud data, enhancing their security has led to huge investments in the cloud computing security technology and thorough training of users on how to maximize security of organizational data. Cloud security allows data to be managed in one place thus the overheads are reduced and IT teams empowered to focus on other areas of business [1].

For proper governance of cloud services, specific technologies are required for cloud security to be effectively established. Companies use these technologies to monitor and set granular policies based on employee access to and usage of the common cloud computing software, that is, SaaS, PaaS, and IaaS [3]. Through cloud computing security, companies can also control what ca be used and done with approved cloud services and report on utilization of activities involving identity and access management.

Microsoft and Amazon, multinational corporations who rely immensely on consumers data are examples of organizations with a well-established cloud computing security. For the two organizations, they have adopted cloud security for several reasons. One, cloud security provides a simple, and scalable approach that aims at reducing application-layer risk across web, mobile, and third-party applications. Other cloud security applications include: Static analysis, software composition analysis, dynamic analysis, and providing cloud data developers with real-time feedback and other security recommendations [4]. The cloud security approach used by an organization is tailored to meet the users needs and the type of data requiring protection against potential risks. In this paper, the cloud security

approaches used by Microsoft ad Amazon Corporations are analyzed and will be compared.

II. DATA SECURITY THREATS

With the increasing quantities of data, research shows that data security has become a major concern among organizations. Cloud computing, for instance, is challenged by issues of security of data. Storage of data in many instances is prone to breach of data confidentiality, integrity, and availability. Microsoft, as a software and PC applications manufacturers, has been keen on the issues of data security. As a result, the organization introduced Azure, a cloud security system [5]. Azure utilizes virtual private storage techniques based on the Searchable Encryption. Similarly, Amazon Incorporation, the leading online business of this era, depends on large data of consumers statistics, consumers information, supplier's data, and other key stakeholders. With similar cloud computing threats, the organization established the Amazon Web Services (AWS) that provides critical security. AWS is formulated to primarily focus on the confidentiality, integrity, and availability of data [5].

III. ARCHITECTURE OF CLOUD SECURITY

Cloud security starts with the protection of the three-cloud core components of cloud computing architecture. The protection of IaaS, PaaS, and SaaS, which form the cloud architecture is considered the most critical starting point of building a cloud computing security architecture. With the three types of cloud computing architecture, the cloud computing security architectures also vary from one another depending on the type of infrastructure is being shielded [4]. In a summary, the SaaS cloud computing security architecture focus on security issues such as logging, IP restrictions, and API gateways. IaaS cloud computing security architecture requires additional features such as virtual web application firewalls, virtual network-based firewalls, virtual routers, intrusion detection systems and Intrusion Prevention Systems, and Network Segmentation. Lastly, the PaaS architecture for cloud computing security includes features such as logging, IP restrictions, and API gateways.

IV. MICROSOFT CLOUD SECURITY APPROACH

Microsoft Corporation is the leading company in the development of personal computer software and applications. The book also is engaged in the publication of books and printing services for books. With its headquarters in Redmond, Washington, U.S., the corporation services are found across the globe in all the continents. With a large number of consumers to serve, the corporation relies on the use of cloud commuting to store and protect sensitive organizational and stakeholders' data. With the technological evolution and the era of modernization, the workplace at Microsoft among other companies has influenced the employees by empowering them to create a more secure and productive workplace [6]. One of the priorities set by the management of Microsoft is providing a productivity solution by having a clear cloud security approach to ensure effective communication starting with the internal parties to the external parties.

V. AMAZON CLOUD SECURITY APPROACH

Amazon utilizes the AWS cloud security which is customer-focused and aims at protecting consumers information. After launching AWS in 2006, the cloud security system has been providing an array of cloud computing services aimed at helping companies gain from on-demand computing platforms [7]. The main services AWS Amazon offers include database analytics, networking, computations, application services protection, developer tools for the Internet of Things among other services.

VI. COMPARISON OF MICROSOFT'S AZURE AND AMAZON'S AWS

For a comprehensive comparison of the two-cloud computing security systems by the two global giants, several factors will be considered [7]. Whereas Azure thrives in Windows features, Azure is applied in the Linux environment. The features and services of the two giants in cloud computing will be completed using the following aspects:

VII. COMPUTING FEATURES

Starting with AWS, for computing, AWS renders an Elastic Compute Cloud (EC2) that s based on IaaS architecture. The EC2 provides scalable computing on-demand. Also, AWS offers Elastic Beanstalk, a PaaS service that deploys apps. Other services offered by AWS are EC2 Container service, AWS Lambda, and Autoscaling [8].

Azure, on the other hand, utilizes virtual machines to pivot the cloud security computing features. Azure like AWS mainly focus on IaaS and PaaS to offer a highly-available, infinitely-scalable applications and APIs.

VIII. NETWORKING

Both Azure and AWS are considered as excellent choices for their networking capabilities. Amazon's Virtual Private Clouds (VPCs) and the Azure's Virtual Network (VNET) have the capabilities of allowing users to group VMs into isolated networks in the cloud [9]. Furthermore, a user of either of the two can define a network topology, create subnets, route tables, private IP address ranges, and network gateways.

With Azure, Microsoft enables users to connect to VNETs to on-premises data centers via site-to-site VPN networks or Azure ExpressRoute. However, Azure is considered to have a hybrid system that has overcome the existing Cloud Wars competitors including Amazon, IBM, Salesforce, SAP, Oracle, and Google [10].

IX. STORAGE FEATURES

Amazon's AWS storage is an inextricable part of cloud services by offering Simple Storage Service (S3) as a storage feature. AWS is much better than Azure storage services since it portrays to have an extensive documentation including webinars, tons of sample code and libraries, articles, and tutorials [9]. The discussion forums at AWS are also considered to be more active since users rely on the feedback they get from Amazon's developers on a daily basis. To boost the storage services of AWS cloud security, other services offered include Elastic Block Storage (EBS), Elastic File System (EFS), Import/Export large volume data transfer service, Glacier archive backup and Storage Gateway, which integrates with on-premise environments [11].

Azure's File Storage on the other hand is reliable as it provides a continuous availability storage option. Azure has features that allows users to share file storage among multiple VMs such that there is no hassle in running critical cloud applications. Azure also allows sharing of data between local and local cloud servers [12]. The Figure below summarizes on how the storage features for Microsoft and Azure.

Storage Options	Azure Storage (Blobs, Tables, Queues Files)	Amazon Simple Storage (S3)
Block Storage	Azure Blob Storage	Amazon Elastic Block Storage (EBS)
Hybrid Cloud Storage	StorSimple	AWS Storage Gateway
Backup Options	Azure Backup	Amazon Glacier
Storage Services	Azure Import Export Azure File Storage Azure Site Recovery	Amazon Import/Export AWS Storage Gateway

Source: eventech.com

X. DATABASES

In relation to databases, both AWS and Azure support relational and NoSQL databases. Some of the managed databases for AWS include the SQL server, MySQL, ProgreSQL, Oracle and MariaDB found within the Relational Database Service (RDS) and Redshift. To ensure security in databases, AWS also has Database Migration Service that provides customers with on-premise relational data to the cloud [12].

Azure, on the other hand, has a SQL database that supports relational database based on SQL server. To migrate data to on-premise SQL servers, there are changes required first. The changes are put into place as an encryption of ensuring maximum data security. Azure has more additional Elastic database pools that allows customers to save costs by running multiple databases against the same set of resources. This makes Azure to be more alike with the AWS. However, Azure utilizes a higher version of NoSQL that has the highest performance and is also highly available document database. As a result the database protection by Microsoft is considered to be superior than that of Amazon [13].

XI. COMPARIOSN OF THE CLOUD SECURITY

AWS security follows the Identity and Access Management protocol to maximize security of organization's data. The security of "least privilege" that initially grants no access permissions until customer administrators to explicitly grant all additional user permissions is the cloud security approach used by Amazon [12]. There is also virtualization management platforms that are established in the AWS and uses the multifactor authentication from AWS staff, and customers managing Virtual Machines and host-based security (firewalls, IDS etc.). Amazon offers customers the CITRIX NetScaler (VPX) virtual web application firewall that aims at enhancing application security [13]. However, the implementation of such a firewall has led to slower or dropped application traffic thus still requires thorough testing before implementing on production cloud applications. Lastly, unlike Microsoft, Amazon has a simplified way of performing external penetration tests and vulnerability scans. With less Denial of Service (DoS) tools among other scanning or testing tools being used, Amazon has explicit terms of service to ensure there are no outages or excessive resource consumption [14].

Microsoft Azure security offers a wide range o services with its Windows Azure platform and Office application suite. The architecture of Azure nodes and the authentication mechanisms are highly polished such as Windows Live ID and the Azure Service Management API (SMAPI). Unlike AWS which supports customer-created networks, Azure does not support these customer-created network access controls to allow and deny specific traffic. However, Microsoft is anticipating to launch this type of service soon. Microsoft's customers, can however, have custom configuration files that provide connectivity [15]. Logging and monitoring data is also provided to customers to ensure there is effective analysis and review.

Summary of the Security Issues at Microsoft and Amazon

Security Issues	Amazon AWS components	Microsoft Azure components
Confidentiality	IAM MFA Key rotation	Identity and access management Isolation encryption
Integrity	S3 server side encryption (SSE), HMAC	Cryptographic storage server
Availability	23.5 mins per month	43 mins per month

Source: Tajadod et al. 2012

XII. CONCLUSION

In the world of cloud computing, the two leading providers of cloud security in the global platform are

Microsoft's Azure, and Amazon's AWS. The features of Azure have a higher rate of protection as compared to AWS. This is because Microsoft has employed the best technical and engineering team to ensure that data confidentiality, availability and integrity is maintained. Another factor making Azure stronger is because there are no direct customer-access interferences but rather has security encryptions. Breaching the security codes is almost impossible. AWS has a strength of providing customers with accessibility to data from the cloud. However, the process is protected by the AWS staff who closely monitor the progress and security issues of the company.

REFERENCES

[1] P. Mell and T. Grance, "The NIST Definition of Cloud Computing," September 2011, National Institute of Standard and Technology (NIST), p.7

[2] Juels A, Oprea A. New approaches to security and availability for cloud data. Commun. ACM. 2013 Feb 1;56(2):64-73.

[3] Krutz, R.L. and Vines, R.D., 2010. Cloud security: A comprehensive guide to secure cloud computing. Wiley Publishing.

[4] Okuhara, M., Shiozaki, T., & Suzuki, T. (2010). Security architecture for cloud computing. *Fujitsu Sci. Tech. J*, *46*(4), 397-402.

[5] G. Tajadod, L. Batten, K. Govinda. "Microsoft and Amazon: A comparison of approaches to cloud security." 4th IEEE International Conference on Cloud Computing Technology and Science Proceedings (2012): pp. 539-544.

[6] T. Redkar and T. Guidici, Windows Azure Platform, 2011, Second edition, The Expert's Voice in .NET, US.

[7] J. Varia, "Architecting for the Cloud: Best Practices," January 2011Amazon Web Services

[8] D. Chappell, "Introducing the Windows Azure platform," October 2010, David Chappell and Associate, Sponsored by Microsoft Corporation.

[9] Amazon Simple Storage Service (Amazon S3), Retrieved July 2012http://aws.amazon.com/s3/#protecting.

[10] C. Wang, Q. Wang, K. Ren and W. Lou, "Ensuring Data Storage Security in Cloud Computing," in Proceedings of IWQoS'09, July 2009, pp. 1-9.

[11] Ponemon institute, "Security of Cloud Computing Providers Study," Sponsored by CA Technologies, April 2010, retrieved March 2012, http://www.ca.com/~/media/Files/IndustryResearch/security-ofcloud-computing- providers-final-april-2011.pdf.

[12] B. Calder and M. Atkinson, "Windows Azure Blob Storage vs. Amazon S3," Retrived 27th July 2012, http://gladinet.blogspot.com.au/2009/12/ windows-azure-blobstorage-vs-amazon-s3.html.

[13] Amazon AWS, "AWS Security Best Practices, "January 2011, Retrieved April 2012, http://d36cz9buwru1tt.cloudfront.net/Whitepaper-Security- Best-P ractices-2010.pdf.

[14] K, Anbarasan, "Brief Comparison between Windows Azure and Amazon Web Service," February 2012, Retrieved April 2012, http://f5debug.net/2012/02/06/brief-comparison-between-windowsazure-and-amazon-web-service/

[15] C. Kaufman and R. Venkatapathy, "Windows Azure Security Overview," August 2010, v1.01, pp. 5-12.