# Essential Cloud Security Features in Windows Azure

**Ramya Dharam**[1], **and Sajjan G. Shiva**[2]
[1]Department of Computer Science, University of Memphis, Memphis, TN, USA
[2]Department of Computer Science, University of Memphis, Memphis, TN, USA

**Abstract -** *Cloud computing technology is recently gaining widespread popularity among business owners and consumers/users for hosting and delivering services over the Internet. This technology offers users on-demand access to shared resources, services, and applications with the Internet access by eliminating the need for tedious installation procedures. Security and privacy issues in cloud computing is one of the major barriers for the wide adoption of this emerging technology. In this paper, we first discuss the security and privacy guidelines pertinent to the public cloud computing environment as described by NIST. We then investigate different security features of the Microsoft Azure cloud computing platform and analyze how the security and privacy guidelines described by NIST are implemented in this cloud platform.*

**Keywords:** Cloud Computing; NIST; Cloud Security; Privacy Issues; Microsoft Azure Cloud Platform; Public Cloud.

## 1 Introduction

Over the last few years, cloud computing technology has become an evolving paradigm with lots of benefits to its users and providers. Cloud computing is an integration of different traditional computing technologies and network technologies such as distributed computing, parallel computing, grid computing, virtualization, etc.

Various definitions exist explaining the concept of cloud computing, but the most widely accepted comprehensive definition about cloud computing was made by National Institute of Standards and Technology (NSIT) [1] and in this paper we adopt the same. It describes cloud computing as a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

The essential characteristics provided by cloud computing makes it different from traditional service computing. Following are the five essential characteristics of cloud computing as discussed in [1] that has currently made an impact on the Information Technology industry:

1) On-demand self-service: Services such as applications, storage, etc., can be provisioned by users based on their demand.

2) Broad network access: A variety of cloud services is available over the network and heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations) can be used to gain access to them.

3) Resource pooling: Computing resources such as storage, processing, memory, and network bandwidth are pooled to serve multiple consumers according to consumer demand.

4) Rapid elasticity: Capabilities can be elastically provisioned and released to meet the rapidly increasing demand of users.

5) Measured service: Metering capabilities are employed to automatically control and optimize resource usage and to charge the users accordingly. Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

Service driven business models are employed by cloud computing. In this model software, platform, and hardware level resources are provided as services to users/consumers from the cloud service providers. Three major cloud computing models as discussed in [1] have evolved, which include: 1) Software as a Service (SaaS), which provides consumers the capability to use provider's applications running on cloud infrastructure. 2) Platform as a Service (PaaS), which provides consumers the capability to deploy the application developed by them onto the cloud infrastructure. 3) Infrastructure as a Service (IaaS), which provides consumers the capability to provision processing, storage, networks, and other computing resources.

Private, Public, Community, and Hybrid clouds are the four cloud deployment models currently available. Private cloud is used by a single organization. Community cloud is provisioned for use by a specific community of users from different organizations that have shared concerns. Public cloud can be used by any general public. Hybrid cloud is formed by the combination of two or more distinct cloud infrastructures (private, public, or community).

With cloud computing becoming more and more popular because of its many benefits and characteristics it possesses as discussed above, security and privacy issues in cloud computing have also raised major concerns due to the unique architectural features and characteristics of the cloud. Hence security and privacy issues existing in cloud computing need to be addressed for this technology to be more widely adopted.

In this paper, we first discuss the different security and privacy issues that exist in the cloud computing technology and also the NIST guidelines to achieve security and privacy in public cloud computing. We then study in detail security features of one of the most popular cloud platforms i.e. the Microsoft Windows Azure, and analyze how the NIST guidelines on security and privacy in public cloud computing are accomplished in this platform.

The rest of the paper is organized as follows. In Section 2, we discuss the common security issues in cloud computing. In Section 3, we discuss the NIST guidelines to accomplish security and privacy in public cloud computing. Section 4 discusses about the features of Microsoft Windows Azure cloud platform and Section 5 discusses security features established in the Microsoft Windows Azure platform. Section 6 provides an analysis by helping us understand how the security and privacy guidelines mentioned by NIST are implemented in the Microsoft Windows Azure platform, and Section 7 concludes the paper.

# 2 Security Issues in Cloud Computing

In cloud computing, security is one of the prominent concerns. Security issues in cloud computing hinder the process of it being widely adopted. So in this section, we discuss in detail the different security issues that exist at different levels in this technology, which includes cloud data, cloud access, and cloud platform.

## 2.1 Security Issues related to Cloud Data

Data stored in cloud belongs to different users, enterprises, etc., and is an important asset. Maintaining the confidentiality, integrity, and availability of cloud data is currently the foremost concern to be addressed for this new technology. The inherent nature of cloud computing architecture itself raises several questions about the security of the data stored in the cloud. Some of the issues as discussed in [3] include the following: 1) What ensures integrity and prevents loss of data in cloud? 2) How is the confidentiality of the data maintained? 3) Is the data available to users in case the cloud services are down? 4) Will the data be completely deleted from the cloud storage if the user decides to withdraw the services from the cloud? 5) How do we know that the updates to the data are done periodically and the user gets access to the most updated version? Addressing these issues about cloud data is essential.

## 2.2 Security Issues related to Cloud Access

User authentication, authorization, and access control (AAA) is one of the important security concern related to cloud access. Multitenancy is one of the major features of the cloud computing where a single instance of software running on a server is utilized to serve multiple clients. This feature is known to cause interoperability, authentication, and identification problems because of the usage of distinct negotiation protocols by different clients. A management interface is essential so that the cloud services can be accessed by users. The probability that unauthorized access to this management interface could occur is much higher than for traditional systems where the management functionality is accessible only to a few administrators as discussed in [4].

Some of the issues related to cloud access as discussed in [3] consist of the following: 1) Different users access their data stored in the cloud and in such situations, how can it be ensured that authentication is provided at different levels to access cloud services? 2) How does one ensure that there is no unauthorized access to the cloud by an employee who has left the organization?

## 2.3 Security Issues related to Cloud Platform

This comprises of the security issues related to the cloud platform which include virtualization, networking, etc. Virtualization is the key technology for the success of cloud computing. It results in the creation of multiple VMs out a single physical layer. Each VM is itself a virtual server compromising a guest OS, middleware, application, and data. A Hypervisor/Virtual Machine Manager is a piece of software that allows multiple OSs to share a single hardware host and a computer on which a hypervisor is running one or more virtual machines is defined as a host machine. Each virtual machine is called a guest machine and the hypervisor presents the guest OSs with a virtual operating platform and manages the execution of the guest operating systems. Some of the virtualization induced cloud security issues as discussed in [5] consist of the following: 1) VM hijacking: In case of multitenancy, a single server would host several VMs on it and thus would have respective configuration files of all VMs stored on the host. Since each VM is separated by a virtual boundary, an attacker gaining access to one such files could be able to predict the actual hardware configuration of another VM residing on the same host. The primary configuration files contain all necessary information of a VM. Gaining access to these files and breaking into a VM is termed as "VM hijacking." A malicious user having control of a VM can try to gain control over the other VMs' resources or utilize all system resources leading to denial of service (DoS) attack over other VM users. A malicious user can also try to steal the data of other users located on the same server. 2) VM hopping: This is the process of hopping from one VM to another VM. An attacker on one VM can gain access over the other VM. This can be achieved if both the VMs are running

on the same host. Because there are several VMs running on the same machine, there would be several victims of the VM hopping attack. An attacker can falsify the SaaS user's data once he gains access to a target VM by VM hopping, endangering the confidentiality and integrity of SaaS. 3) VM mobility: This enables the moving or copying of VMs from one host to another over the network or by using portable storage devices without physically stealing or snatching a hard drive. Although this makes the process of deployment easier, it could lead to security problems such as spread of vulnerable configurations. The severity of the attack ranges from leaking sensitive information to completely compromising the OS. 4) VM escape: This means gaining access over the hypervisor and attacking the rest of the VMs. If an attacker gains access to the host running multiple VMs, the attacker can access to the resources shared by the other VMs. The host can monitor the memory being allocated and the CPU utilization. If necessary, an attacker can bring down these resources and turn off the hypervisor. If the hypervisor fails, all the other VMs turn off eventually.

Some of the issues related to the cloud platform as discussed in [4] consist of the following: 1) Are the cloud data centers physically secured against security breaches? 2) How are the applications secured in a shared virtualized infrastructure against malicious attacks? Can the APIs and interfaces provided by cloud services be trusted?

# 3 NIST Guidelines on Security and Privacy in public cloud computing

In this section, we discuss in detail the guidelines described by NIST in [2] to achieve security and privacy in cloud computing.

1) Governance: It involves controlling and monitoring deployed applications over standards, procedures, and policies. It also involves the implementation, testing, design, and monitoring of deployed cloud services. Cloud computing services are widely used among employees and lack of control over the employees' access to the cloud services by the organization can cause problems.

Roles and responsibilities involved in accessing the cloud services need attention to ensure systems are secure and risks are managed. To determine how data is stored, protected, and used, to verify policy enforcement, and to validate services, audit mechanism and tools should be in place. Risks in cloud computing are continuously evolving and to deal with them a risk management program should be in place.

2) Compliance: Conformance with an established standard, specification, law, or regulation is involved. Compliance becomes a complicated issue due to the existence of different types of security laws at the national, state, and local levels within different countries. Any data that is processed or stored outside the bounded spaces of an organization inherently brings a level of risk and it is important to carefully address this issue. Data location is one of the most common compliance issues faced by any organization.

Any organization will structure its computing environment according to their needs and will know in detail where the data is stored, what measures they have taken to protect unauthorized access to the data, and if they use an in-house computing/storage center. But, in case of the usage of cloud computing technology this detailed information about the exact location of an organization's data is not known, then this lack of detailed information leads to a situation and makes it difficult to ascertain whether the specified compliance requirements are met. Usage of external audits and security certification could to some extent help in handling this issue.

3) Trust: In cloud computing an organization places an unprecedented level of trust in the cloud provider by giving away the direct control of many security aspects involved in the cloud. To enable a basis of trust the ownership rights of the organization over the data must be firmly established in the service contract.

It is challenging to assess and manage risk in systems that use cloud services. It is important for organizations to ensure that security controls are implemented and operated correctly as intended to manage risks. Based on the degree of control an organization is able to achieve on the provider, to provision the security controls which are necessary to secure the organization's data and gain assurance that those controls have been placed, it is possible to establish a level of trust in a cloud service. The organization must reject the service or be ready to take a greater degree of risk, if the level of trust provided by the service is below the specified and negotiated expectations and is unable to employ other suitable controls.

4) Architecture: The hardware and software residing in the cloud comprises the architecture used to deliver cloud services. The implementation, scalability logic of the framework, and the physical location of the infrastructure is determined by the cloud provider. Virtual machines are loosely coupled with cloud storage and is the basic unit of deployment in cloud computing. Cloud components communicating with each other using application programming interfaces are typically used to build applications. Underneath the complexity that affects security, many of the simplified interfaces and service abstractions are involved.

5) Identity and Access Management: Unauthorized access to data in the cloud is a major concern and the issues related to data security and privacy are widely discussed for the wide usage of cloud. The existing identification and authentication framework used by organizations may not naturally extend into the cloud and it will be difficult to modify the existing framework to support cloud services.

One possible solution could be to employ authentication systems, one for the internal organizational systems and another for external cloud-based systems.

To administer and authenticate the users so that they can access applications and data, cloud providers support the standard named Security Assertion Markup Language (SAML) which is used to provide cloud based identity and access management services. This alone is not sufficient to maintain identity services, but the capability to adapt cloud to the subscriber privileges and maintain control over access to resources is also needed.

6) Software Isolation: High degrees of multi-tenancy over large numbers of platforms are needed for cloud computing to achieve the envisioned flexibility of on-demand provisioning of reliable services and the cost benefits and efficiencies due to economies of scale. To reach the high scales of consumption desired, cloud providers have to ensure dynamic flexible delivery of service and isolation of subscriber resources.

7) Data Protection: Since the cloud environment is shared, the data stored in cloud co-exists with other customers' data. Before moving the data to the cloud it is very important that organizations reassure the means and control measures that have been established to keep the data secure and to establish the controlled access to the data.

8) Availability: The extent to which an organization's computational resources are accessible and usable is termed as availability. Different threats to availability consist of denial of service attacks, natural disasters, etc. Availability can be affected either temporarily or permanently, and a loss can be partial or complete and can impact the mission of the organization.

9) Incident Response: The security of a computer system is compromised by attacks and incident response, which is an organized method and is essential to deal with attack consequences. Incident verification, attack analysis, problem remediation, service restoration, etc., are some of the incident response activities cloud providers need to perform.

# 4 Overview of Microsoft Windows Azure Architecture

As defined in [6], Windows Azure is a cloud services operating system that serves as the development, service hosting and service management for the Windows Azure platform. This platform helps developers to host and manage web application through Microsoft datacenters with on-demand compute and storage options.

This section discusses the Microsoft Windows Azure architecture and each of its components as described in [7]. This Windows Azure architecture mainly consists of four components: 1) Windows Azure 2) SQL Azure 3) Windows Azure AppFabric and 4) Windows Azure Marketplace.

1) Windows Azure: This is a Windows environment for running applications and storing data on computers in Microsoft data centers. It consists of five components namely: a) Compute – Applications that are built using C#, Visual Basic, C++, Java can be executed using the Compute service on a Windows Server Foundation. b) Storage – Binary large objects (blobs) can be stored using this service and also provides tables with a query language. c) Fabric Controller – It is responsible for creating VMs and starting the applications that run on them. d) Content Delivery Network – It stores the copies of the data that are frequently accessed by the users closer to them which helps in speeding up access to the data. e) Connect – This service helps the Windows Azure applications to access database that is on the premise of the organization.

2) SQL Azure: This can be used for storing data in the cloud and is built on Microsoft SQL Server. It includes the following three components: a) SQL Azure Database - It is a cloud-based database management system (DBMS) and it allows both the on-premise and cloud applications to store data on Microsoft servers. b) SQL Azure Reporting - is used with SQL Azure database and it is responsible for creating SQL Server Reporting Services (SSRS) reports on the cloud data. c) SQL Azure Data Sync - is used to synchronize data between SQL Azure Database and on-premise SQL Server databases. Different SQL Azure databases present in different Microsoft data centers can be synchronized using Azure Data Sync.

3) Windows Azure AppFabric: This provides infrastructure for applications. It consists of the following three components: a) Service Bus - it exposes applications endpoints in the cloud so that other applications in the cloud or on-premise can access them. b) Access Control - used to define rules that help to control what services each user will be able to access. c) Caching - it is used to cache frequently accessed data by users so that performance is increased and reduces the need to query the database by the application every time to retrieve the data.

4) Windows Azure Marketplace: It lets the customers find as well as buy cloud applications and cloud-accessible data. It consists of the following two components: a) DataMarket – datasets are made available to content providers with the help of this component. b) AppMarket – cloud applications developed are exposed using this component so that other customers can buy them.

# 5 Security Features in Microsoft Windows Azure

Data and programs belonging to customers are hosted in the cloud by Microsoft using the Windows Azure. So it is essential to maintain the security and privacy of the data and applications residing in the cloud. In this section, we discuss in detail about the different features implemented by Microsoft in the Windows Azure cloud platform to accomplish the security of user's data as described in [6].

1) Identity and Access Management: This feature ensures that only authorized and authenticated users are allowed to access the required cloud services. Following are the different mechanisms used to accomplish the Identity and Access Management security feature of the cloud: a) SMAPI Authentication – The Service Management API provides web services via the Representational State Transfer (REST) protocol. High degree of assurance is accomplished with this mechanism and that only the authorized representatives of the customer can access the service. b) Least Privilege Customer Software – This is a security best practice that is widely used in which applications are executed with least privileges. Also, customers are not granted administrative access to their VMs. This helps in reducing the potential impact and protects from attacks as an elevation in privileges is required to perform attacks. c) SSL Mutual Authentication for Internal Control Traffic – SSL is used to communicate between the internal components of Windows Azure.

2) Isolation: This involves keeping different data segregated from one another. Isolation can be accomplished at different levels in the Windows Azure using the following: a) Isolation of Hypervisor, Root OS and Guest VMs – The root OS and the hypervisor manages the root VM and the guest VMs and so isolation of the root VM from the guest VMs helps to accomplish security to a certain extent. b) VLAN Isolation – Fabric Controllers and other devices are isolated using VLANs. A network is partitioned using VLANs and without passing through a router no communication is possible. This prevents a compromised node from faking traffic outside its VLAN, and also it cannot eavesdrop on traffic that is not to or from its VLANs. c) Isolation of Customer Access – Customer access environments are separated from customer applications and storage.

3) Encryption: Data in storage and in transit is encrypted to accomplish data protection of user's data. .NET libraries in Windows Azure SDK are extended with .NET Cryptographic Service Providers (CSPs) so that developers can implement encryption, hashing and key management functionalities for their data either in storage or in transit. Encryption algorithms like AES, cryptographic hash functionality like MD5 and SHA-2, etc. can be easily accessed by Windows Azure developers.

4) Availability: Data is replicated to three separate nodes within the Fabric in Windows Azure to minimize the impact of hardware failures. Different levels of redundancy are provided to accomplish greater availability of customer's data.

# 6 Mapping of Microsoft Windows Azure Security Features to NIST Security & Privacy Guidelines

In this section, we map the different areas related to security and privacy as discussed by NIST in [2] to the security features implemented in Microsoft Windows Azure Platform as described in [6].

| NIST Areas | Microsoft Windows Azure Security Features |
|---|---|
| Governance | * Multiple levels of monitoring, logging, and reporting are implemented.<br>* The monitoring and diagnostic log information are gathered by the Monitoring Agent (MA) from many places including the FC (Fabric Controller) and the root OS and are written into the log files.<br>* Various monitoring and diagnostic log data are read and summarized by the Monitoring Data analysis Service. |
| Compliance | * It is certified by one of the premier international information security management standards i.e. ISO27001. |
| Trust | * Customer's data are made unavailable once the delete operations are called by the Windows Azure's Storage subsystem.<br>* Execution of delete operation removes all references to the associated data item and it cannot be accessed via the storage APIs. All copies of the deleted data item are then garbage collected.<br>* When the associated storage block is reused for storing other data the physical bits are overwritten. |
| Architecture | * Windows Azure fully integrates Microsoft's Security Development Lifecycle (SDL) guidelines to provide security assurance within Windows Azure's development processes.<br>* Microsoft scrutinizes places where data from a less-trusted component is parsed by a more trusted component like when Windows Azure portal and SMAPI processes requests coming over the network from sources controlled by customers. |

| | |
|---|---|
| Identity and Access Management | * Customers access the Windows Azure Portal through a web browser or access SMAPI through standalone command line tools, either programmatically or using Visual Studio.<br>* Customers upload developed applications and manage their Hosted Services and Storage Accounts through the Windows Azure Portal web site or programmatically through the Service Management API (SMAPI).<br>* Customers can monitor and manage their applications via the portal or programmatically through SMAPI using the same authentication mechanism.<br>* SMAPI authentication is based on a user-generated public/private key pair and self-signed certificate registered through the Windows Azure Portal. The certificate is then used to authenticate subsequent access to SMAPI.<br>* Access to Windows Azure storage is governed by a storage account key (SAK) that is associated with each Storage Account. Storage account keys can be reset via the Windows Azure Portal or SMAPI. |
| Software Isolation | * Microsoft's Hyper-V is used to provide strong isolation of guest VMs.<br>* The hypervisor and the root OS provide network packet filters that assure that the untrusted VMs cannot generate spoofed traffic, cannot receive traffic not addressed to them, cannot direct traffic to protected infrastructure endpoints, and cannot send or receive inappropriate broadcast traffic.<br>* VLANs are used to isolate the FCs and other devices. |
| Data Protection | * Critical internal communications are protected using SSL encryption.<br>* Windows Azure SDK extends the core .NET libraries to allow developers to integrate the .NET Cryptographic Service Providers (CSPs) within Windows Azure.<br>* Developers familiar with .NET CSPs can easily implement encryption, hashing, and key management functionality for stored or transmitted data. |
| Availability | * Customers can create a second Storage Account to provide hot-failover capability.<br>* Customers can create custom roles to replicate and synchronize data between Microsoft facilities.<br>* Customers can also write customized roles to extract data from storage for offsite private backups.<br>* Data is replicated within Windows Azure to three separate nodes within the Fabric to minimize the impact of hardware failures.<br>* Each datacenter facility has a minimum of two sources of electrical power, including a power generation capability for extended off-grid operation. |
| Incident Response | * Microsoft security vulnerabilities can be reported to the Microsoft Security Response Center or via email to secure@microsoft.com.<br>* Microsoft follows a consistent process to assess and respond to vulnerabilities and incidents reported via the standard facilities. |

# 7 Conclusion

Cloud computing technology is in constant development and has recently emerged as a paradigm for delivering and managing services over the Internet. With the wider adoption of this technology, cloud security issues have also emerged. In this paper, we first analyze the guidelines provided by NIST to address security and privacy issues in public cloud computing. Then we provide analysis of the Microsoft Windows Azure cloud platform describing how the NIST guidelines have been implemented in this platform.

The data and programs belonging to customers are hosted by Microsoft using Windows Azure. It provides different security features, controls and mechanisms for customers to choose so that they can achieve their required level of security. The analysis performed in this paper will provide customers a good understanding of how the privacy and security-related issues that are considered to have long-term significance on the cloud computing technology have been addressed by Microsoft Windows Azure, making it one of the most popular cloud computing platforms to provide a better level of data security.

# 8 References

[1] P. Mell and T. Grance, The NIST Definition of Cloud Computing, National Institute of Standards and Technology, Spetember 2011.

[2] W. Jansen and T. Grance, NIST Guidelines on Security and Privacy in Public Cloud Computing, January 2011.

[3] S. Sengupta, V. Kaulgud, and V. S. Sharma, Cloud Computing Security – Trends and Research Directions, IEEE World Congress on Services, 2011.

[4] B. Grobauer, T. Walloschek, and E. Stocker, Understanding Cloud Computing Vulnerabilities, IEEE Security & Privacy, April 2011.

[5] Cloud Enterprise Architecture, Pethuru Raj, CRC Taylor and Francis, 2012.

[6] C. Kaufman and R. Venkatapathy, Windows Azure Security Overivew, Microsoft, August 2010.

[7] D. Chappell, Introducing the Windows Azure Platform, David Chappel and Associates, Sponsored by Microsoft Corporation, Oct 2010.

[8] Q. Zhang, L. Cheng and R. Boutaba, Cloud computing: state-of-the-art and research challenges, Journal of Internet Services and Applications, May 2010, Volume 1, Issue 1, pp 7-18.

[9] G. Tajadod, L. Batten and K. Govinda, Microsoft and Amazon A comparison of approaches to cloud security, Fourth International Conference on Cloud Computing Technology and Science, 2012.

[10] X. Jing and Z. Jian-jun, A Brief Survey on the Security Model of Cloud Computing, Ninth International Symposium on Distributed Computing and Applications to Business, Engineering and Science, 2010.

[11] Z. Wang, Security and privacy issues within the Cloud Computing, International Conference on Computational and Information Science, 2011.

[12] T. Yu and Y. Zhu, Research On Cloud Computing And Security, Eleventh International Symposium on Distributed Computing and Applications to Business, Engineering & Sciences, 2012.

[13] X. Ma, Security Concerns in Cloud Computing, Fourth International Conference on Computational and Information Science, 2012.