IJITKM Volume 8 • Number 1 June-Dec 2014 pp. 75-79 (ISSN 0973-4414)

Cloud Computing Security Challenges & Offerings with Window AZURE Plate Form

Rini Mahajan[1], Dheerendra Singh[2], Dr. Manish Mahajan[3]
[1]PhD Scholar PTU, 2Shaheed Udham Singh College of Engg, Tangori,Mohali, Punjab, India.
[2]Professor, Department of Computer Science & Engineering, SUSCET, Tangori, Mohali
[3]Associate Professor (Department of Computer Science) Chandigarh Engineering College, Landran, Mohali, India
rinimahajan@gmail.com, professordsingh@gmail.com, manishmahajan4u@gmail.con

Abstract: This paper Now a day's cloud computing is very popular Technology. Many large & medium size organizations are using cloud services like Iaas saas or paas. The access to these Services are based on standard Internet Protocols like HTTP, SOAP, REST, XML and Cloud computing is emerging field because of its performance, high availability, least cost. There are so many platforms to implement & to provide cloud computing services. Microsoft Window Azure is one of the platforms. As the interest of large & medium size organizations is getting increased, security concern is also getting increased. This paper presents the overview of Window azure platform to provide cloud computing services, its security issues & offerings.
Keywords: Cloud Computing, Window Azure, Security, Vulnerabilities, Threats, Risks, Counter measures.

1. Introduction

Cloud Computing is scalable Internet-based IT-services and resources. One feature is common to all such new technologies - a shift in the geography of computation. [1] it is Internet-based computing, whereby shared resources, software and information, are provided to computers and devices on-demand, like the electricity grid. It is the combination of technology, platform, hosting storage, and application hosted as a service [2].The reason of success of cloud computing is its feature to handle different workloads according to need of the users. It also allows workloads to recover from many unavoidable hardware/software failures and manages resource usage in real time to enable scalability & elasticity of allocations when needed [3].cloud computing is based on pay per use i.e. an organization need to pay only for what it uses, depending on the organization's needs change.

There are so many platforms to implement & support cloud computing like google App Engine, Amazon EC2, window Azure e.t.c. Every platform is having its own framework & language. This paper concentrates on Window Azure Platform advantages & challenges.

First subsection discusses about the architecture of window azure then further subsections focus on what are security issues for window azure platform & how it is handled.

2. Window Azure Architecture

Microsoft Windows Azure platform is a collection of cloud technologies; each of them provides a specific set of services to cloud application developers. This platform is very easy to use & it provides a familiar and flexible environment to support specific needs and services of the development team, customers and users. Windows Azure platform consists of the following:

Windows Azure
Microsoft SQL Azure
Windows Azure Platform Application Fabric
Window Azure Market Place [4, 5]

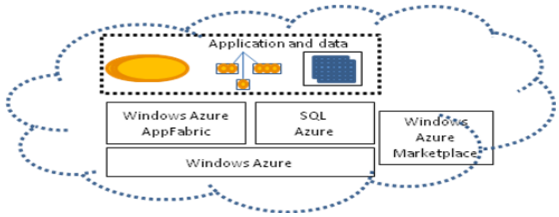

Fig.1 Windows Azure platform

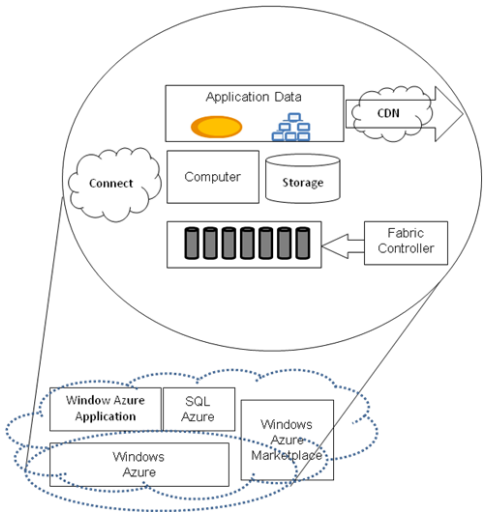

Fig.2 Windows Azure services

Win Azure- It is a platform to run Windows applications and to store data in the cloud. It has three main parts: the Compute service, the Storage service, and the Fabric.
The Compute service is used to run various applications. It runs the application on window server which has been created on .Net Platform. Storage service is used to stores data. It provides storage for large binary objects which work as Back end for window applications. The fabric controller unites the machines into a cohesive whole. The Win Azure Fabric facilitates a common way to manage and monitor applications that use win azure cloud platform.
Content delivery network supports data caching of to speed up & to improve the performance.
Connect services makes interaction with cloud applications easy for organizations as it seems to be they inside the own firewall of the organization. SOAP, REST and XML protocols are used to offer Azure's services. These services are independent OS i.e. can be supported by any operating system thus using them will not be a problem [5].

SQL Azure- Whenever we develop any application, we need a front end & a backend. SQL Azure offers cloud-based backend services. The components of SQL Azure are as follows:
SQL Azure Database is a cloud-based database management system (DBMS). SQL Azure facilitates customers to store on-premises and cloud applications data on Microsoft servers that are located in Microsoft data centers.
SQL Azure Reporting is a reporting tool that runs in the cloud. It is a version of SQL Server Reporting Services (SSRS). It is primarily used with SQL Azure Databases to create and publish standard reports on cloud data which are stored on Microsoft servers.
SQL Azure Data Sync synchronizes data between SQL Azure Database and on-premises SQL Server databases. It can also be used for the synchronization of data of different SQL Azure databases in different Microsoft data centers. SQL Azure is built on Microsoft SQL Server. It used in the same way as SQL Server. Application developers can create indexes and views, create & use stored procedures, can define trigger etc. Applications can access SQL Azure data using Entity Framework, ADO.NET, and other Windows data access interfaces [5]

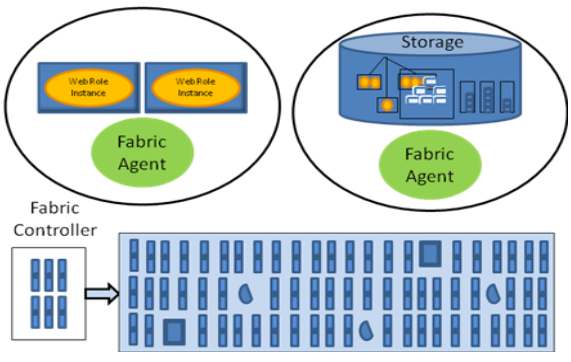

Fig.3 Window Azure App Fabric

Window Azure App Fabric- It is comprised of a large group of machines which is managed by software called fabric controller. This software is repeated across a group of 5 to 7 machines. Fabric controller owns all of the resources in the fabric i.e. computers, switches etc. because it communicate with fabric agent on every computer. It monitors & manages all running applications, operating systems. It also takes care of things like patching the version of Windows Server 2008 that runs in Windows Azure VMs. Decision regarding where new applications should run, choosing physical servers to optimize hardware utilization is also taken by it.

3. Advantages of Window Azure Platform

1. With Windows Azure, you can scale up or down on-demand resources according to need of business. Business
2. The Windows Azure Management Portal gives you the power to produce a web application within minutes. So to launch any website through this platform is very easy and fast.
3. Any site managed within Windows Azure can be managed directly in Visual Studio, while providing live data streams and site logs.
4. Azure is Window based , so we can write applications in the same programming languages that we have used for Windows apps It allows to produce applications using many other languages like ASP, ASP.net, PHP, Python, or Node.js. Azure environment is very similar to the standard Windows environment so it is easier to create a cloud based version of an existing Windows application.
5. Windows Azure uses Blobs which are one of the easiest ways to store unstructured text and binary data like images, video, and audio.
6. With Azure, we don't have to worry about the H/w, just need to focus on code
7. With Azure you can you can develop and debug an application locally and then move it to the cloud.
8. Azure Storage offers scalable, secure, performance-efficient storage services in the cloud. After creating a Web application, we can specify the number of processors for the application to use and we can also change the number of processors on the basis of current need.
9. SQL Azure provides organizations with high availability and reliability of Data. It manages redundant copies of organization's data and automatic failover. There is no need to worry about backing up data ourselves.
10. With Azure, we can develop hybrid applications that allow your on-premises applications to use cloud services. These services can be cloud database, storage services & much more. Communications services work between on-premises applications and the cloud, as well as mobile devices.
11. Security is one of the biggest concerns for companies while considering a move to the cloud. Azure provides very good level of security. Access Control Service provides a way to incorporate identities, and Security

Assertion Markup Language (SAML) tokens are used by applications to determine whether a user is allowed access.10, 11]

12. The Windows Azure Platform allows ISV's (Independent Software Vendors) to run their applications and store their data in Microsoft Datacenters rather than in their customer's premises, their own datacenter or in a hosted facility. This brings with it many benefits. [12]

13. Lower application lifecycle costs. [9]

4. Window Azure risks & Challenges

Since the data is in the hand of 3rd party so there is Potential loss of account control to that party. So one of the major issues is Security which must be considered before moving applications & data on to Cloud [9].If the data security is not provided properly by cloud provider then anyone from 3rd party can misuse the data or can insert malicious data into the database.

5. Cloud Security

There is a critical need to securely data hosted by cloud service provider. Since many applications are critical in nature it is important that clouds be secure. The major security challenge with clouds is that the owner of the data may not have control of where the data is placed. There are numerous security issues for cloud computing as it encompasses many technologies including networks, databases, operating systems, virtualization, resource scheduling, transaction management, load balancing, concurrency control and memory management. Therefore, security issues for many of these systems and technologies are applicable to cloud computing [6].One way to make security actionable and prescriptive is to focus on threats, attacks, vulnerabilities and countermeasures [6, 7, 8].

Threats, Attacks, Vulnerabilities, and Countermeasures these are defined as follows:

Asset- it can be any data which is stored on cloud such as the data in a database, data on the file system etc.

Threat- it is a malicious event A that can harm an asset.

Vulnerability- It is typically a loophole that makes a threat possible.

Attack.- it is an action taken to take advantage of vulnerability and realize a threat.

Countermeasures- there are the methods to mitigate risk.

It means that by surveying about threats & building a knowledgebase of threats, attacks, vulnerabilities, and Countermeasures, we can considerably improve security know [1, 6, 8]

Window azure considers all these things & provides various points to be considered while moving to cloud to maintain security.

6. Windows Identity Framework Impact

Windows Identity Framework impacts security design a lot, so following points must be considered.

Claims –we can use claims for identity management and for access control. Claims support well with cloud applications because they allow to factor out identity management logic from application and integrate with identity providers such as an on-premise Active Directory via Active Directory Federation Services.

VM model and trust -- The Windows Azure security model is centered on strict control over VMs imposed by two Windows Azure specific trust policies which are defined as full and partial trust. These policies limit access to system resources to prohibit common attacks like elevation of privilege. A working knowledge of what level of permissions are available is required to know which pieces of an existing application can be migrated and which must be adjusted to work under more restrictive permissions. Azure Storage and SQL Azure -- Some of the things to think about in Windows Azure regarding data include deciding where to host your data, what will be used to host the data, and what the means of access to that data will be. You can use on-premise data and expose it as a service to your Windows Azure application. Data hosting in the cloud can be done primarily through Windows Azure Storage or SQL Azure. Data exposed to other applications or services should be exposed as a service (Data as a Service), but data consumed only by your application has the option of being accessed without a service interface.

Deployment -- Deploying the Windows Azure can potentially mean deploying across multiple data centers that are physically separate. This will influence application design patterns, deployment, as well as communication between application pieces. Be aware of your application boundaries, and use resources within the same data center when possible, and communication options such as internal endpoints when applicable.

7. Win Azure Cloud Security Design

In the actual realm of security, Windows Azure Platform provides several security mechanisms to keep data protected. Customers must authenticate with their Windows Live Identifier so as to correctly identify themselves as an authorized client to help prevent unauthorized access to backend systems. Data stored on the platform is encrypted within Windows Azure, so even a breach of their security systems does not make data stored by your application available. Each customer's data is logically separated onto a different (virtual) volume so it is difficult to access another customer's data. As with Google Apps, data can be replicated at several locations so catastrophic failure does not imply data loss [6].

To maintain security any cloud computing plate form must provide confidentiality, integrity, availability of customer data and accountability. Confidentiality is one of the important factors from security point of view which ensures that a customer's data is only accessible by authorized entities.

Windows Azure provides confidentiality via:-

Identity and Access Management - Ensures that only properly authenticated entities are allowed access.

The Service Management API (SMAPI)-provides web services via the Representational State Transfer (REST) protocol. The protocol runs over SSL and is authenticated with a certificate and private key generated by the customer.

As long as the customer maintains control of the private key and the Live ID used to create the account, this mechanism provides a high degree of assurance that only the customers' authorized representatives can access specific aspects of the service.

Isolation - Minimizes interaction with data by keeping appropriate containers logically or physically separate.

Encryption - Used internally within Windows Azure for protecting control channels and is provided optionally for customers who need rigorous data protection capabilities [8].

Example Application Scenario and Solution: as shown in Figure 4 it is a scenario of interaction with cloud based application. During interaction data send & retrieval mat be performed which is required security so that no intruder can hack data from inbetween or cannot insert malicious data.

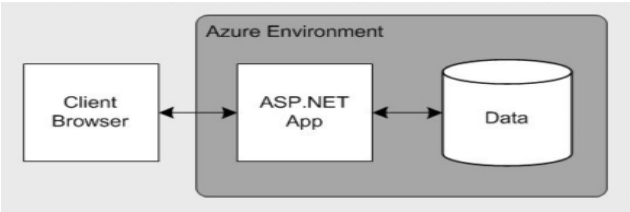

Fig.4 Example Scenario

As shown in Figure 5 window azure provides solution for this. It performs Authentication, Authorization & maintain security while communication.

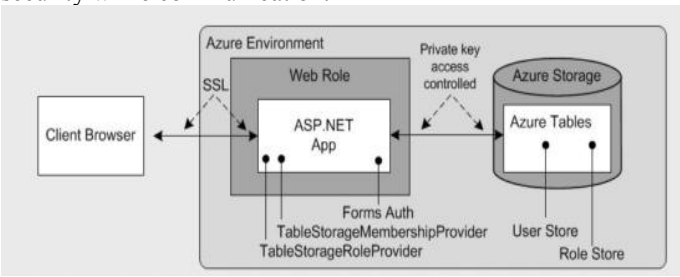

Fig.5 Solution

Although it provides various securities measures for communication but still it cannot be fool proof. So there is much more to do in security area to promote cloud computing amongst various organizations.

8. Conclusions

Cloud computing has brought revolution especially for large scale industries however cloud computing environment forces to face issues directly to developer. Window Azure supports SQL Server and Active Directory providers for authenticating the user to maintain the confidentiality. However there are several other security challenges including security aspects of virtualization. it is very difficult to get point to point security. So the challenge for developer is to ensure more secure operations even if some failure occurs. To build trust applications from un trusted components will be a major aspect with respect to cloud security. There is much more to do in security sector in cloud computing to promote it amongst various organizations.

References

[1] H. Erdogmus. Cloud computing: Does Nirvana hide behind the Nebula? IEEE Software, 26(2):4–6, 2009.

[2] B. C. Kaufman and R. Venkatapathy, "Windows Azure TM Security Overview."

[3] www.ibm.com/developerworks/websphere/zones/hipods/

[4] D. Chappell, "Introducing the azure services platform an early look at windows azure, . net services ," October, 2008.

[5] R. Jain, "A Survey of Cloud Security Issues and Offerings," pp. 1–14.

[6] K. Hamlen, M. Kantarcioglu, L. Khan, and B. Thuraisingham, "Security Issues for Cloud Computing," Int. J. Inf. Secur. Priv., vol. 4, no. 2, pp. 36–48, 2010.

[7] HighTech_Whitepaper_Windows_Azure_09_2011 by TCS

[8] P. Enfield, "Azure Security Notes."

[9] http://readwrite.com/2010/07/12/ray-wang-of-the-altimeter

[10] http://www.techrepublic.com/blog/10-things/10-reasons-to-use-azure-for-your-cloud-apps/

[11] http://vorsite.com/blog/2014/01/10-benefits-features-windows-azure/

[12] http://www.sysfore.com/Assets/PDF/Advantages_Of_Moving_An_Application_To_The_Azure_Cloud.pdf