A Detailed Study of Security Aspects in Cloud Computing

NagaRaju Pamarth
Department of CSE, GMR Institute of Technology, Rajam, AndhraPradesh, India.

Nagamalleswara Rao N
Department of CSE, RVR&JC College of Engineering, Guntur, AndhraPradesh, India.

Abstract-Cloud computing has become a buzz word in present era of technology. Cloud is nothing but an internet. It provides organizations and individuals with a cost-effective utility, empowering businesses by delivering software and services over the Internet to a large number of users. But, on the other hand security in cloud computing is still a biggest problem. This paper discuss about the various security issues confined to cloud computing, some the security implemented mechanisms, techniques to deal with risks and threats, case study of windows azure.

Index Terms - Cloud computing, Security, Security mechanisms, risks, windows azure.

1. INTRODUCTION

Cloud computing has no particular definition. But in summarized it provides various services such as SaaS, PaaS, IaaS to the users over the internet. The European Network and Information Security Agency (ENISA) defined cloud computing as: "On- demand service model

For IT provision often based on virtualization and distributed computing technologies"[2]. Cloud Computing provides the facility to store the data on the cloud which can be available anytime and anywhere. So many organizations are using the cloud storage which reduces the cost of disk storage. But users raised some security concerns that whether their data are accessed by unauthorized persons since there are many users sharing the resources over the cloud.

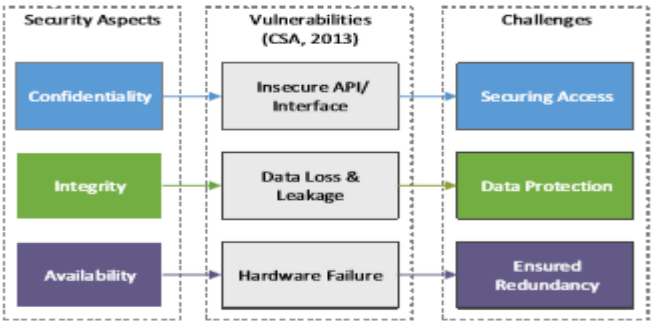

Fig.1 Cloud Storage Security Aspects, Vulnerabilities & Challenges

This has also been supported by Cloud Security Alliance (CSA) in their statistical overview of vulnerabilities. It has been reported by CSA that major security issues are confidentiality, integrity and availability [1].

The cloud storage architecture consists of three components: Front End, Storage Controller, and Back-End Storage.

2. SECURITY ISSUES

Some of the key security challenges in cloud computing are:

A. Data Protection

Generally, users store their data in the cloud, but they are not aware of where the data has been stored. They can't have control over the physical access mechanisms to that data. As the cloud providers have datacenters distributed over different countries globally, users can't know the exact location where their data is being stored.

B. Unwanted Access

Cloud computing may actually increase the risk of access to confidential information. In some Foreign countries, the government can have legal rights to view the data under certain circumstances. There is also no need for them to notify the users. There is also a risk of unauthorized access if the security mechanisms being implemented are inadequate.

C. Data Segregation

Since, multiple users store the data in the same cloud, encryption can't be assumed as a solution for data segregation problems. In some cases, users don't want to

Encrypt their data because sometimes encryption accident may destroy the data.

D. Vendor Lock-In

So far, cloud computing lacks interoperability between different service providers. This makes it difficult to establish security frameworks for heterogeneous environments. It also becomes difficult for migrating the data between one cloud providers to another or bringing back data and processing it in-house.

E. Data Remanence

Another question arises to the users mind that how to be sure whether the data to be deleted are really deleted and are not recoverable the service provider. The risks of data exposure may vary according to the service model.

F. Data Reliability Issues

1) Co-residency and Multi-tenancy:

[4] For co-residency, there would be multiple services held in a single server and it is difficult to predict the application performance. The chance of reliability and availability of a service be affected by other "busy" services are higher. For Multi-tenancy, multiple independent instances of an application, such as e-mail or web service, can be consolidated on a single virtualized platform. The instances are then available simultaneously to various user groups. Actually multi-tenancy has the same cost benefits and challenges as co-residency. However the challenges are more difficult because failures of server may affect large population from different aspect.

2) Server Down:

[4] Down time is another important aspect which creates some serious reliability problems. The cloud computing system down time can be in days which create some serious consequences for users. Users suffer further from unplanned downtime. As there are no prior warning, users do not have any preparation for the downtime. For cloud service providers such as Google and Amazon, they suffer from the downtime as their services are bound by tough SLA's (service level agreements). However, under tough SLA's, planned downtime is allowed.

3) Latency Challenges:

[4] In some real time applications such as video conferencing, the requirements on making latency are as short as possible unless it affects the service quality. However, some mechanism such as virtualized configurations, resource contention, real-time notification latency and virtualization overhead add extra latency. This may result in bad user experience.

3. IMPLEMENTED MECHANISMS

Some of the security mechanisms implemented which are most likely interest customers and security professionals will be explained below:

A. Vendor Security Certification

Certification of trustees or identity trust is another aspect where trust is needed in cloud computing. This certification ensures the client that the service provider is the same whom it claims to be. For certifications we can use different mechanisms like PGP or X.509 etc.,

B. External Audits

Many customers may feel that they are given insufficient information or guarantees by service providers such as: what security controls are in place to protect the data? Where the data is physically located? Who has the access to data? Etc., For any deployment involving legally protected data respondents only considered providers that could give the clients clear answers to key audit questions.

C. Identity and Authentication

Generally, for authentication passwords are used for logging in. But the password security heavily depends on how strong the passwords are so that they can't be stolen. So it requires lengthy passwords to provide more security, but lengthy passwords are difficult to be remembered. Authentication can also be done through face recognition, finger print recognition etc.,[5] The following table compares the biometric and non-biometric techniques.

Technique	Advantages	Disadvantages
Fingerprint recognition and image processing [2]. Fingerprint identification and mixed encryption [3].	Fingerprint image used as biometric input for authentication purpose provides more security than non-biometric algorithms.	The fingerprint impressions of user can be obtained from any object which is hold by user in hands.
Generating a distributed authorization token composed of two parts for a single resource access [4].	It is non-biometric authentication and token generated by IDM and cloud both are sent to the user for authentication which is more secure method.	The communication link in the model carries the complete token due to which a hacker is able to acquire the protected resource.
Retina Pattern Recognition Algorithm (RPRA) [5].	Retina image is used which is a unique identity of any person hence it can provide higher security to the mobile cloud.	The number of images matched with dataset is not very high.
RSA and Hash Function [6].	It is a non-biometric method of authentication. It provides encryption and decryption to the messages of users to secure them from unauthorized persons.	It provides security to the messages of user, but it is not applicable at the time of login to the mobile cloud.
Orthogonal Line Ordinals Features (OLOF) extraction [7].	Palmprint image works like fingerprint image and as it is a biometric authentication provides more security than any other authentication methods.	Like fingerprint impression palmprint impressions can be obtained by hackers.
Image-Level	It uses fusion of	It gives better

Fusion Algorithm and Multi-Level Fusion Algorithm [8].	two images which provides better security than a single image used for authentication. No information is lost in this method.	results for the combination of ear and finger knuckle but for other biometrics it is not so good.
Key Generation Algorithms [9].	The key generation algorithm is used for fingerprin authentication. This algorithm may results better for other biometrics also.	Fingerprint authentication is not much secure.

Fig.2 Comparison of biometric and Non-biometric techniques.

Proposed System:

[3]MIST: MIST is an implementation of a secret question and answer system that uses predetermined questions with a number of possible answers for each question. The MIST algorithm had to show the answer that the user setup among a group of fifty other similar answers. For example, if a user set his security answer as "What is birthplace street address?", the MIST application was able to take any custom answers from the user.

The initial question selection was:

1) What is your favorite car brand?

2) Which country would you like to visit one day?

3) What is your lucky number between 1-100?

All the questions will have generic answers. Additionally, for these questions, random lists of possible answers are populated on the answer selection screen.

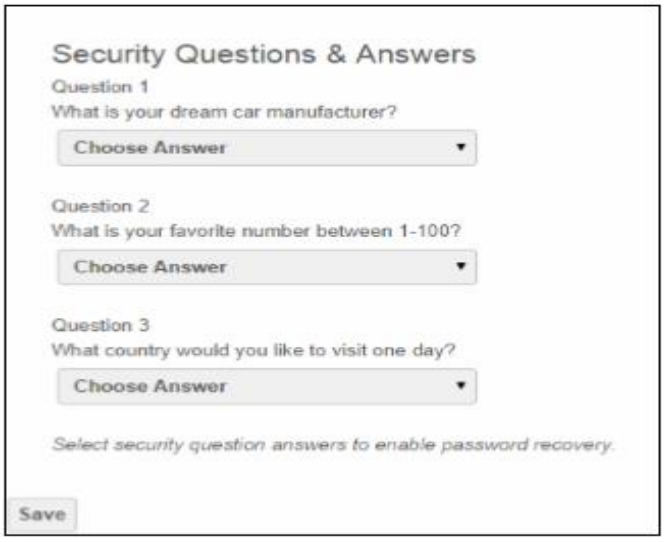

Fig.3 MIST model implementation

To address added another security weakness an additional layer was added to this version of MIST. This security layer will not allow the user to try resetting their password more than five times. There are three questions to answer in a row and they have five chances to get it right. If the user fails to choose the correct answer for any of the security questions, they will be redirected to the home page and they will have to start over again. For each wrong answer they provide for any of those three security questions, they will lose one chance out of five. If they cannot make it through using all of their five attempts, their account will be locked down and they will not be able try to continue with the password reset option. They will have to contact the administrator for getting access to their account again.

D. Data Encryption

To protect the data hosted on the servers in cloud, the information can be encrypted which can only be decrypted at the client level with a key. There are numerous data encryption mechanisms like Truecrypt, BoxCryptor, 7-Zip etc., Generally symmetric encryption algorithms are used.[6]Symmetric encryption algorithms use only single key for encrypting and decrypting the data. For these algorithms, how much longer the key length is that much stronger the encryption will be.

Encryption methods	Approach		Limitation
Symmetric cryptography (Private-key)	Searchable symmetric encryption [15] [14]		The key used to encrypt and decrypt data must remain secure because anyone with access to it can read the coded messages.
Asymmetric cryptography (Public key)	Attribute-based Encryption (ABE)	Attribute-based Encryption (ABE) [16]	Encryption are more complex compared to symmetric encryption and takes longer to encrypt and decrypt. Needs verification of the public key authenticity.
		Searchable ABE [17]	
		Cipher text-policy Attribute-based Encryption (CP-ABE) [18]	
		Hierarchical Identity-Based Encryption and Key-Policy Attribute-Based Encryption [19]	

Fig.4 Review about encryption methods and approaches

For encryption a new proposed architecture was explained called Shamir Secret Sharing Scheme (SSSS)[15]. It consists of three phases:

1) Key generation and Distribution
2) Encryption and Upload
3) Download and Decryption

It also consists of fourth phase which talks about lawful interception.

E. Firewall

Firewall protects the internal network against the Internet; it is used to decrease the attack surface of virtualized servers in cloud computing environments. The client can request from the cloud provider for firewall rules to be opened or closed after viewing them through provider's portal, meaning anything the client needs to block can be blocked.

F. Intrusion detection and prevention systems

[13] Intrusion detection means monitoring of network activity and recording of unusual activity in the system. There are two types of intrusion protection systems being offered. They are:

HIPS: Host based Intrusion Protection System

NIPS: Network based Intrusion Protection System

They include elements like: monitoring system's log files etc.,

G. Antivirus

It is software which protects individual computers against known viruses. Antivirus scanning can be done on the cloud to reduce the risk of malicious activities. Using the power of cloud more anti-virus engines can be employed and used more efficiently. Panda is the famous software company releases the cloud computing based antivirus.

H. Backup and Recovery

[13] If some accident occurs there may be a chance of losing all the data. If such thing occurs then all companies face a lot of problems, so it is essential to have a robust backup routine. Client should have regular checks to see Whether the backup is being done periodically, and his recovery plan is viable or not. The cloud should also provide the facility to recover the data and the infrastructure if the cloud has undergone some unintended attacks which can render the system complete destruction; so the provider should offer facility to completely recover the data even after the destruction of the data.

4. TECHNIQUES TO DEAL WITH THREATS

Though cloud computing faces many issues mentioned in the previous sections. Now we will discuss some techniques to deal with threats:

A. STRIDE MODEL:

[1] STRIDE means Spoofing identity - Tampering with data - Repudiation Information disclosure - Denial of service - Elevation of privilege.

A STRIDE model helps in analyzing a security problem,

Design mitigation strategies; evaluate solutions and the techniques that will be used to deal with the threats.

It contains following steps:

1. Identify attackers, assets, threats and other components that systems must be protected from.

2. Rank the threats to prioritize and address the most significant threats first. These threats present the biggest risk. The rating process weighs the probability of the threat against damage that could result an attack occur. It might tum out that certain threats do not warrant any action when compared to the risk posed by the threat with the resulting mitigation costs.

3. Choose mitigation strategies.

4. Build solutions based on the strategies.

5. WINDOWS AZURE CASE STUDY

[20]To study the security aspects in Windows Azure, PaaS must be divided into several architectural components. Windows Azure offers an insight into its components by grouping its components into distinctive categories based on services it offers rather than security architecture.

Component I: **Developer environment**	**Subscription Web Portal/ SMAPI**
	App Fabric
Component II: **Host/ Compute**	**VMs and Guest OS**
	Hypervisor
Component III: **Storage**	**Tables, Queues, Blobs, Emulator**
	Fabric Controller

Fig.5 Azure components

Developer Environment Security: [20] Windows Azure offers Windows Live ID and a self-signed certificate as authentication mechanisms to provide identity and access management to the cloud service. The cloud service subscription is registered with a Windows Live ID associated to the customer's credit card detail. It is setup with an email address and password used to create a Windows account and is authenticated by a Microsoft authentication server once the credentials are sent via a SSL connection. In Windows Azure, the SMAPI and web portal are built upon the Representational State Transfer (REST) protocol. A secure SSL communication is established using asymmetric cryptography or public key encryption which provides encryption of credentials sent between the customer's web browser and the Microsoft authentication server.

Host/Compute Security: [20] Virtualization security is provided on this component by providing VM security, OS hardening and Hypervisor security. Although users are not given full administrative privileges to their VMs, security can be enhanced as an administrator can create a boundary of IP addresses to restrict unauthorized access to VMs deployed

and running in the PaaS cloud. This is referred to as establishing endpoints or creating subnets. VM isolation or segregation is provided by the hypervisor coupled with the network functionality of the Fe. Isolating VMs on Windows Azure is enhanced by allocating individual fixed private IP addresses to VMs created within a cloud service subscription. This ensures only VMs within that cloud service can communicate with each other, hence a technique in resolving multi-tenancy while access to the internet is provided, using a single public IP address. Closing and opening only specific ports also can be used to secure VM communication.

Storage Component Security: [20] Windows Azure provides data security for the storage emulator and cloud storage services by ensuring that the .NET cryptography techniques such as PKI encryption, decryption and hashing can be implemented to secure data stored and transmitted on the local machine using Virtual Studio Web Express. Therefore customer themselves must provide data storage security using cryptographic techniques they are used to in tradition information systems. Cryptography and hashing mechanisms such as symmetric key encryption (AES), asymmetric PKI infrastructure, SHA-I, SHA-2, and MD5 hashing are all recognizable.

6. CONCLUSION

In this paper, we have discussed about the various security issues present in cloud computing and some of the security mechanisms that are being implemented by various service providers. STRIDE model to deal with threats and finally windows azure case study. So, through this paper we want to make aware that security plays an important role and especially if you are storing your important information on cloud.

REFERENCES

[1] Study of Security Mechanisms Implemented in Cloud Computing by Abobaker Elhouni, ElBahlul EIFgee . IEEE 2014
[2] ENISA. "Benefits, Risks and Recommendations for Information Security". ENISA Quarterly Review.
[3] Comparison of Security Algorithms in Cloud Computing by Dinesh Devkota, Prashant Ghimire, Dr. John Burris, and Dr. Ihssan Alkad. 2013 IEEE
[4] Challenges on Privacy and Reliability in Cloud Computing Security by Daniel W.K. TSE. 2014 IEEE
[5] Comparison of Biometric and Non-Biometric Security Techniques in Mobile Cloud Computing by Nileshree R. Darve, Deepthi P.Theng. 2015 IEEE
[6] R Ranjan, Sanjay Kumar Singh," Improved and Innovative Key Generation Algorithms for Biometric Cryptosystems" 2013 3rd IEEE International Advance Computing Conference (IACC)
[7] Towards Data Confidentiality and Portability in Cloud Storage by Ebtesam Ahmad Alomari and Muhammad Mostafa Monowar. 2013 IEEE
[8] Data Security: challenges of cloud computing by HuShuijing. 2014 IEEE
[9] Analysis of Security Vulnerabilities of Cloud Computing Environment Service Models and Its Main Characteristics . 2015 IEEE
[10] A quantitative analysis of current security concerns and solutions for cloud computing by Nelson Gonzalez, CharlesMiers1,4,FernandoRed´ıgolo1,MarcosSimpl´ıcio1,TerezaCarvalho1, MatsN¨aslund2 . 2012 Springer
[11] CSA(2009)Security Guidance for Critical Areas of Focus in Cloud Computing.Tech.rep., Cloud Security Alliance
[12] An analysis of security issues for cloud computing Keiko Hashizume1, David G Rosado, Eduardo Fernández-Medina and Eduardo B Fernandez. 2013 Springer
[13] Security and Privacy in Cloud Computing: Vision, Trends, and Challenges by Zahir Tari, Xun Yi, Uthpala S. Premarathne, Peter Bertok, and Ibrahim Khalil, RMIT University
[14] A survey on security issues and solutions at different layers of Cloud computing by Chirag Modi·Dhiren Patel·Bhavesh Borisaniya· Avi Patel·Muttukrishnan Rajarajan . 2012 Springer
[15] New Secure Storage Architecture for Cloud Computing by Sameera Abdulrahman Almulla and Chan Yeob Yeun
[16] Protecting Data Privacy and Security for Cloud Computing Based on Secret Sharing. 2013 IEEE
[17] Risk perception and risk management in cloud computing : results from case study of Swiss companies. 2013 Elsevier
[18] Towards Robust, Scalable and Secure Network Storage in Cloud Computing . 2013 IEEE
[19] Security Challenges in Cloud Storage by F. Yahya[1], V. Chang[2], R.J. Walters[1], and G.B. Wills[1] . 2013 IEEE
[20] Evaluating Security Mechanisms Implemented on Public Platform-as-a-Service Cloud Environments Case Study: Windows Azure by A. Akinbi, E. Pereira, C. Beaumont. 2013 IEEE