UACEE International Journal of Advances in Computer Networks and its Security – IJCNS
Volume 3 : Issue 2 [ISSN 2250 – 3757]
Publication Date : 05 June 2013

SECURE ZONE IN CLOUD

Ms.R.S.M.Lakshmi Patibandla
Vignan University
India
patibandla.lakshmi@gmail.com

Dr.Ande Prasad
V.S.University
India
prasadjkc@yahoo.co.in

Mr.Y.R.P.Shankar
Vignan University
India
radhashankar77@gmail.com

ABSTRACT:
In a fast-moving and volatile market, the ability to remain competitive is more important than ever in IT. Today Cloud computing was playing a most prominent role in improving the value of IT. Adopting cloud technology can be an affordable way to get access to a dynamically scalable, virtualized computing environment. While cloud computing models are attractive because of their flexibility and cost effectiveness, certain challenges must be addressed in order to provide a viable option to traditional data services. First and foremost is the issue of security. Each type of cloud computing model public, private or hybrid faces different levels of IT risk. In the private cloud delivery model, the cloud owner does not share resources with any other company. Private clouds are owned and operated by a single organization, delivering IT services within the constraints of their own network perimeter .In the public cloud computing model, IT activities and functions are provided as a service that can be billed on a pay-per-use or subscription basis via the Internet from external suppliers, using resources not owned by the consumer. The sharing of IT resources in a public, multitenant environment can help improve utilization rates and can reduce costs significantly while maintaining access to high quality technology. In a public cloud, an organization rents IT resources instead of having to invest in their own physical IT infrastructure or maintain under-utilized equipment to service peak loads. Instead, they can scale usage up or down, according to need, with costs directly proportional to need. This paper mainly concentrates on discussion on security, authentication to the data (storage) by encrypting using best encrypting algorithms.

Keywords: Volatile market, Affordable, Virtualization, Scalable, Multitenant, Encryption and Authentication.

INTRODUCTION:

If we start to define the meaning of cloud computing it should be incredible and if we want to find its origin it should be obscure. But what all of us do is to draw few designed clouds of network and communication. But it is said that the underlying concept of cloud computing had laid its foundation early in 1950's. Cloud computing will allow its users to make use of any software even without having a deep knowledge on every software. When it came to say generally we can say that there are 2 sun's behind the cloud.

1) **Virtualization:** we can say virtualization as "The ability to run multiple operating systems on a single physical system and share the underlying hardware resources.*"*
2) **Autonomic computing:** Autonomic computing is just like human nervous system which can respond even without any inputs. The goal of autonomic computing is to create systems that run themselves, capable of high-level functioning while keeping the system's complexity invisible to the user.

Depending upon the several fundamental models, cloud providers offer their services in different variants. They are

a) IaaS(Infrastructure as a service):
b) PaaS(Platform as a service):
c) SaaS(Software as a service):
d) NaaS(Network as a service):

As there are different types of services are provided, there also different types of clouds available. They are

a) Public cloud:-

A public cloud can be accessed by any subscriber with an internet connection and access to the cloud space.

b) Private cloud :-

A private cloud is established for a specific group or organization and limits access to just that group.

c) Community cloud :-

A community cloud is shared among two or more organizations that have similar cloud requirements.

d) Hybrid cloud :-

A hybrid cloud is essentially a combination of at least two clouds, where the clouds included are a mixture of public, private, or community.

GOING IN DEEP:

Cloud computing has become a source of boom to the IT. By the usage of cloud computing most of the companies can be able to save a lot of operational charges. We already know that cloud is a on-demand, pay-per-use environment so it is also a beneficial to the users also. As there are such benefits available here in the cloud that's why many unauthorized person are having a look on cloud, which leads to lack of security. We have keep one word in mind that hackers not the only threats. The possible security conflicts in cloud computing are also known as notorious nine that means there are 9 top threats according to latest survey , they are :

1. Data Breaches
2. Data Loss
3. Account Hijacking
4. Insecure APIs
5. Denial of Service
6. Malicious Insiders
7. Abuse of Cloud Services
8. Insufficient Due Diligence
9. Shared Technology Issues

DATA BREACHES:

In general we define data breach as the acquirement of unencrypted personal information

by an unauthorized person. Lost laptop, hard drive, thumb drive, mobile device, or misdirected information also lead to data breach. Malicious or criminal attacks such as phishing, malware, economic espionage, advanced persistent threats, political hacking. Third party flub -- service provider suffers a data breach.

DATA LOSS:

Data loss is a very serious problem in Cloud computing. If the vendor closes due to financial or legal problems there will be a loss of data for the customers. The customers won't be able to access those data's because data is no more available for the customer as the Vendor shut down.

ACCOUNT HIJACKING:

Account hijacking is the fast growing form of the identity theft; it can show the most devastating effect on the users. Accounting hijacking occurs when an unauthorized person obtains your personal information and uses it to take over the confidential data like bank accounts. When this had done it would take much more time to discover. This can be done by phishing or by spyware.

INSECURE API'S:

Many supposedly secure devices have some kind of application programming interface, or API, that untrustworthy people and processes can call in order to get some task performed.

DENIAL OF SERVICE:

Denial of service (DoS) usually refers to an attack that attempts to make a computer resource unavailable to its intended users by flooding a network or server with requests and data. It can also simply refer to a resource, such as e-mail or a Web site that is not functioning as usual. Often, the denial is accidental rather than a planned attack, resulting from too many legitimate requests. However, malicious DoS attacks are still

prevalent against network devices, and a newer breed of DoS attack targeted specifically at applications is becoming more and more common.

MALICIOUS INSIDERS:

Malicious insiders, who have legitimate access to an organization's network, pose a serious threat to an organization. Malicious insider behavior, unlike that of external foes, cannot be detected using traditional intrusion detection methods and can have serious consequences.

ABUSE OF CLOUD SERVICES:

Any technology will be having both good things and bad things also. The providers will not manufacture anything for the sake of bad but few people going to use those things in bad. This is called abuse of cloud services.

INSUFFICIENT DUE DILIGENCE:

Cloud computing has brought with it a gold rush of sorts, with many organizations rushing into the promise of cost reductions, operational efficiencies and improved security. While these can be realistic goals for organizations that have the resources to adopt cloud technologies properly, too many enterprises jump into the cloud without understanding the full scope of the undertaking.

HOW TO SECURE THE CLOUD:

As we already discussed the different threats in the cloud computing, these may become a big disaster for the famous and big companies. One of the ideal way to solve this problem is ENCRYPTION of data. But many of the cloud customers were not using this encrypted data. For this data encryption we are using best encryption algorithms such as TWO FISH, RC5-32, triple BLOW FISH.., are under this category. Let us have a look on the TWO FISH ALGORITHM i.e. how it works and implemented.

TWO FISH ALGORITHM:

TWO FISH is a 128- bit symmetric block cipher and can accept a variable length key upto 256 bits. The cipher is based on a Feistel network that has 16 rounds, a bijective *F* function made up of four key dependent 8-by-8-bit S-boxes, a fixes 4-by-4 maximum distance.

The performance analysis of this algorithm is

- Key lengths: 128 bits, 192 bits, and 256 bits.
- A 128-bit symmetric block cipher.
- No weak keys.
- Flexible design:
  - ✓ Accept additional key lengths.
  - ✓ Suitable for a stream cipher, hash functions, and MAC.
  - ✓ Implementable on a wide variety of platforms and applications.
- Simple design: ease of analysis and ease of implementation.
- Accepts any key length upto 256 bits.
- Encrypts the data in less than 500 clock cycles per block.
- Be implementable on a 8-bit microprocessor with only 64 bytes of RAM.
- Not includes any elements that make it inefficient in hardware.

Two fish builds four objective key – independent 8x8-bit S-boxes using a key/permutation called "sandwich".

So(x)=q1[q0[q0[x]^k0]^k1]

S1(x)=q0[q0[q1[x]^k2]^k3]

S2(x)=q1[q1[q0[x]^k4]^k5]

S3(x)=q0[q1[q1[x]^k6]^k7]

Where q0, q1 are two fixed 8-bit permutations.

Fixed S-boxes may provide a gate for attackers to study the S-boxes and they may find the weak points. But with key–dependent S-boxes, those attackers don't know what the s-boxes are. This

will barricade from "unknown attacks". But the length of key will judge the complexity of keyed S-box.

Feistel networks:

Simply saying a feistel network is a general method of transforming a function into a permutation. As the function was named after its discoverer horst feistel. This function widely known to world after its use in DES. From then this was used in many block ciphers. This Feistel network is based on Feistel function (F function)which is a key dependent function that maps and input string into a output string. The F is always non – linear and can be non – surjective:

F={0,1}^n/2 X {0,1}N → {0,1}n/2

Where

n-the block size of the feistel network.

F- is a key dependent function which takes n/2 bits of the block and N bits of a key as input and produces an output of length n/2 bits.

For each consecutive round, the "source block", which is the input to F, and the output of F is XORed with the "target block". Then the two blocks swap places for the next round. The purpose of the XOR and swap operations is to use a F function, which can even be a weak encryption algorithm, and iterate it repeatedly to create a strong encryption algorithm. Two rounds in a Feistel network are called a "cycle". After a cycle every bit of the text block has been modified once. The number of rounds of a Feistel network in an encryption algorithm is usually directly proportional to the strength of the algorithm. More rounds mean a stronger encryption algorithm. Two fish is a 16- round feistel network and uses a bijective F function.

AUTHENTICATION:

There is also a little problem faced in case of authentication. The major problem is that whether the message is received from the authorized person or not. If this was abused then some untrusted user will send as a trusted one. For authentication purpose we are also having many algorithms but we can overcome this problem only by using the best algorithms such as SHA-1, MAC…, etc.

MAC (Message Authentication Code):

Message authentication code is a piece of information used to authenticate a message and to provide integrity and authenticity assurances on the message. Integrity assurances detect accidental and intentional message changes, while authenticity assurances affirm the message's origin. While MAC functions are similar to cryptographic hash functions, they possess different security requirements. To be considered secure, a MAC function must resist existential forgery under chosen-plaintext attacks. This means that even if an attacker has access to a database which possesses the secret key and generates MACs for messages of the attacker's choosing, the attacker cannot guess the MAC for other messages (which were not used to query the database) without performing infeasible amounts of computation. MACs differ from digital signatures as MAC values are both generated and verified using the same secret key. This implies that the sender and receiver of a message must agree on the same key before initiating communications, as is the case with symmetric encryption. For the same reason, MACs do not provide the property of non-repudiation offered by signatures specifically in the case of a network-wide shared secret key: any user who can verify a MAC is also capable of generating MACs for other messages. In contrast, a digital signature is generated using the private key of a key pair, which is asymmetric encryption. Since this private key is only accessible to its holder, a digital signature proves that a document was signed by none other than that holder. Thus, digital

signatures do offer non-repudiation. However, non-repudiation can be provided by systems that securely bind key usage information to the MAC key; the same key is in possession of two people, but one has a copy of the key that can be used for MAC generation while the other has a copy of the key in a hardware security module that only permits MAC verification.

Universal hashing and in particular pairwise independent hash functions provide a message authentication code as long as the key is used at most once (or less than k -times for k -wise independent hash functions. This can be seen as of the one-time pad for authentication.

The simplest such pairwise independent hash function is defined by the random key $key = (a, b)$ and the mac tag for a message m is computed as $tag := (a * m + b) \mod p$, where p is a prime.

CONCLUSION:

Cloud computing is the scope of large scale and complex computing in the feature. So an user must be free to interact with cloud but not fear to store the sensitive data in it. In this paper we discussed about the cloud computing boom in market, types of providers, types of clouds, latest surveyed threats in cloud computing and at last we provided some data about securing data by encryption and proper authentication and authorization. Among these cloud computing issues are most important challenge to users and vendors. So by using the cloud by using as much as safety measures we can achieve the purity of cloud.

REFERENCES:

1. Fei Hu, Meikang Qiu – a review on architecture and security of cloud.
2. Cloud Security Alliance – top threats working group.
3. Security Guidance for Critical Areas of focus in Cloud Computing [online]. Availabe: http://www.cloudsecurityalliance.org/guidance/csaguide.pdf.
4. http://www.infoworld.com/d/cloud-computing /what-cloud-computing-means-031.
5. N.Santos, K.P.Gummadi, R.Rodrigues, To-wards Trusted Cloud Computing.
6. Security and high availability in cloud computing environments- **IBM Global Technology Services** Technical White Paper June, 2011.