ISSN : 2394-2975 (Online)
ISSN : 2394-6814 (Print)
Vol. 3, Issue 1 (Jan. - Mar. 2016)
International Journal of Advanced Research in Education & Technology (IJARET)

Network Security in Cloud Computing

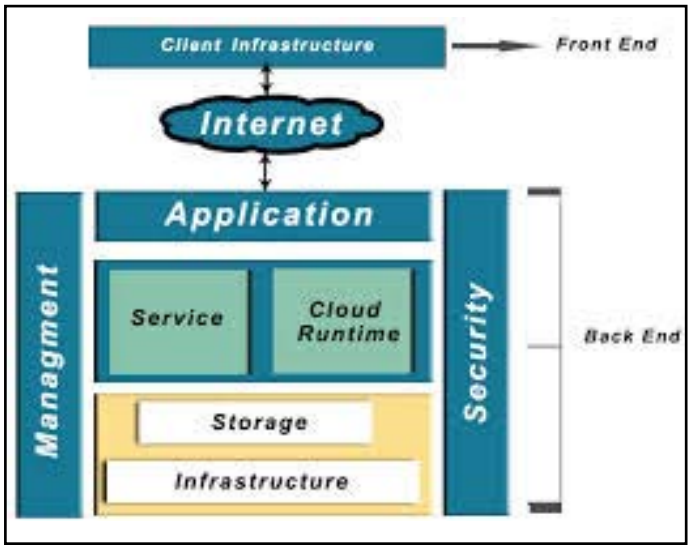
Sheenu
Dept. of Computer Science, Student, Patiala Institution of Engg. and Tehnology, Nandpur Keso, Patiala, Punjab

Network security refers to any activities designed to protect your network. Specifically, these activities protect the usability, reliability, integrity, and safety of your network and data. Effective network security targets a variety of threats and stops them from entering or spreading on your network. Many network security threats today are spread over the Internet. Network security consists of the policies adopted to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Network security involves the authorization of access to data in a network, which is controlled by the network administrator

The most common include:

- Viruses, worms, and Trojan horses
- Spyware and adware
- Zero-day attacks, also called zero-hour attacks
- Hacker attacks
- Denial of service attacks
- Data interception and theft
- Identity theft

A spec111`ialized field in computer networking that involves securing a computer network infrastructure. *Network security* is typically handled by a network.



A. Security management

Security management for networks is different for all kinds of situations. A home or small office may only require basic security while large businesses may require high-maintenance and advanced software and hardware to prevent malicious attacks from hacking and spamming.

B. Types of Attacks

Networks are subject to attacks from malicious sources. Attacks can be from two categories: "Passive" when a network intruder intercepts data traveling through the network, and "Active" in which an intruder initiates commands to disrupt the network's normal operation.

Types of attacks include:

Passive Attack:

1. Network
2. Wiretapping
3. Port scanner
4. Idle scan

Active

- Denial-of-service attack
- DNS spoofing
- Man in the middle
- ARP poisoning
- VLAN hopping
- Smurf attack
- Buffer overflow
- Heap overflow
- Format string attack
- SQL injection
- Phishing
- Cross-site scripting
- CSRF
- Cyber-attack

C. Cloud Computing Security

Cloud computing security or, more simply, cloud security is an evolving sub-domain of computer security, network security, and, more broadly, information security. It refers to a broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing

D. 2.4 Security issues associates with cloud

Cloud computing and storage solutions provide users and enterprises with various capabilities to store and process their data in third-party data centres. Organizations use the Cloud in a variety of different service models (SaaS, PaaS, and IaaS) and deployment models (Private, Public, Hybrid, and Community).[2] There are a number of security issues/concerns associated with cloud computing but these issues fall into two broad categories: security issues faced by cloud providers (organizations providing software-,platform-, or infrastructure-as-a-service via the cloud) and security issues faced by their customers (companies or organizations who host applications or store data on the cloud). The responsibility goes both ways, however: the provider must ensure that their infrastructure is secure and that their clients' data and applications are protected while the user must take measures to fortify their application and use strong passwords and authentication measures.

When an organization elects to store data or host applications on the public cloud, it loses its ability to have physical access to the servers hosting its information. As a result, potentially business

ISSN : 2394-2975 (Online)
ISSN : 2394-6814 (Print)

sensitive and confidential data is at risk from insider attacks. According to a recent Cloud Security Alliance Report, insider attacks are the third biggest threat in cloud computing. Therefore, Cloud Service providers must ensure that thorough background checks are conducted for employees who have physical access to the servers in the data centre. Additionally, data centres must be frequently monitored for suspicious activity.

In order to conserve resources, cut costs, and maintain efficiency, Cloud Service Providers often store more than one customer's data on the same server. As a result, there is a chance that one user's private data can be viewed by other users (possibly even competitors). To handle such sensitive situations, cloud service providers should ensure proper data and logical storage segregation.

The extensive use of virtualization in implementing cloud infrastructure brings unique security concerns for customers or tenants of a public cloud service. Virtualization alters the relationship between the OS and underlying hardware - be it computing, storage or even networking. This introduces an additional layer - virtualization - that itself must be properly configured, managed and secured. Specific concerns include the potential to compromise the virtualization software, or "hypervisor". While these concerns are largely theoretical, they do exist. For example, a breach in the administrator workstation with the management software of the virtualization software can cause the whole datacentre to go down or be reconfigured to an attacker's liking.

D. Cloud security controls

Cloud security architecture is effective only if the correct defensive implementations are in place. An efficient cloud security architecture should recognize the issues that will arise with security management.The security management addresses these issues with security controls. These controls are put in place to safeguard any weaknesses in the system and reduce the effect of an attack. While there are many types of controls behind a cloud security architecture, they can usually be found in one of the following categories:

1. Deterrent controls

These controls are intended to reduce attacks on a cloud system. Much like a warning sign on a fence or a property, deterrent controls typically reduce the threat level by informing potential attackers that there will be adverse consequences for them if they proceed. (Some consider them a subset of preventive controls.)

2. Preventive controls

Preventive controls strengthen the system against incidents, generally by reducing if not actually eliminating vulnerabilities. Strong authentication of cloud users, for instance, makes it less likely that unauthorized users can access cloud systems, and more likely that cloud users are positively identified.

3. Detective controls

Detective controls are intended to detect and react appropriately to any incidents that occur. In the event of an attack, a detective control will signal the preventative or corrective controls to address the issue.[8] System and network security monitoring, including intrusion detection and prevention arrangements, are typically employed to detect attacks on cloud systems and the supporting communications infrastructure.

4. Corrective controls

Corrective controls reduce the consequences of an incident, normally by limiting the damage. They come into effect during or after an incident. Restoring system backups in order to rebuild a compromised system is an example of a corrective control.

E. Dimensions Of Cloud Security

It is generally recommended that information security controls be selected and implemented according and in proportion to the risks, typically by assessing the threats, vulnerabilities and impacts. Cloud security concerns can be grouped in various ways; Gartner named sevenwhile the Cloud Security Alliance identified fourteen areas of concern. Cloud Application Security Brokers (CASB) are used to add additional security to cloud services.

F. Security And Privacy

1. Identity management

Every enterprise will have its own identity management system to control access to information and computing resources. Cloud providers either integrate the customer's identity management system into their own infrastructure, using federation or SSO technology, or a biometric-based identification system,[1] or provide an identity management solution of their own.[13] CloudID,[1] for instance, provides a privacy-preserving cloud-based and cross-enterprise biometric identification solutions for this problem. It links the confidential information of the users to their biometrics and stores it in an encrypted fashion. Making use of a searchable encryption technique, biometric identification is performed in encrypted domain to make sure that the cloud provider or potential attackers do not gain access to any sensitive data or even the contents of the individual queries.[1]

2. Physical security

Cloud service providers physically secure the IT hardware (servers, routers, cables etc.) against unauthorized access, interference, theft, fires, floods etc. and ensure that essential supplies (such as electricity) are sufficiently robust to minimize the possibility of disruption. This is normally achieved by serving cloud applications from 'world-class' (i.e. professionally specified, designed, constructed, managed, monitored and maintained) data centers.

3. Personnel security

Various information security concerns relating to the IT and other professionals associated with cloud services are typically handled through pre-, para- and post-employment activities such as security screening potential recruits, security awareness and training programs, proactive security monitoring and supervision, disciplinary procedures and contractual obligations embedded in employment contracts, service level agreements, codes of conduct, policies etc.

4. Availability

Cloud providers help ensure that customers can rely on access to their data and applications, at least in part (failures at any point - not just within the cloud service providers' domains - may disrupt the communications chains between users and applications).

5. Application security

Cloud providers ensure that applications available as a service via the cloud (SaaS) are secure by specifying, designing, implementing,

testing and maintaining appropriate application measures in the production environment. Note that - as with any commercial software - the controls they implement may not necessarily fully mitigate all the risks they have identified, and that they may not necessarily have identified all the risks that are of concern to customers. Consequently, customers may also need to assure themselves that cloud applications are adequately secured for their specific purposes, including their compliance obligations.

6. Privacy

Providers ensure that all critical data (credit card numbers, for example) are masked or encrypted and that only authorized users have access to data in its entirety. Moreover, digital identities and credentials must be protected as should any data that the provider collects or produces about customer activity in the cloud.

Effective Encryption

Some advanced encryption algorithms which have been applied into the cloud computing increase the protection of privacy.

Attribute-Based Encryption Algorithm

Cipher text-policy ABE (CP-ABE)

In the CP-ABE, the encryptor controls access strategy, as the strategy gets more complex, the design of system public key becomes more complex, and the security of the system is proved to be more difficult. The main research work of CP-ABE is focused on the design of the access structure.

Key-policy ABE (KP-ABE)

In the KP-ABE, attribute sets are used to explain the encrypted texts and the private keys with the specified encrypted texts that users will have the right to decrypt.[15]

Fully homomorphic encryption (FHE)

Fully Homomorphic encryption allows straightforward computations on encrypted information, and also allows computing sum and product for the encrypted data without decryption

Compliances

Numerous laws and regulations pertain to the storage and use of data. In the US these include privacy or data protection laws, Payment Card Industry - Data Security Standard(PCI DSS), the Health Insurance Portability and Accountability Act (HIPAA), the Sarbanes-Oxley Act, the Federal Information Security Management Act of 2002 (FISMA), and Children's Online Privacy Protection Act of 1998, among others.

Similar laws may apply in different legal jurisdictions and may differ quite markedly from those enforced in the US. Cloud service users may often need to be aware of the legal and regulatory differences between the jurisdictions. For example, data stored by a Cloud Service Provider may be located in, say, Singapore and mirrored in the US.[17]

Many of these regulations mandate particular controls (such as strong access controls and audit trails) and require regular reporting. Cloud customers must ensure that their cloud providers adequately fulfil such requirements as appropriate, enabling them to comply with their obligations since, to a large extent, they remain accountable.

Business continuity and data recovery

Cloud providers have business continuity and data recovery plans in place to ensure that service can be maintained in case of a disaster or an emergency and that any data loss will be recovered.[18] These plans may be shared with and reviewed by their customers, ideally dovetailing with the customers' own continuity arrangements. Joint continuity exercises may be appropriate, simulating a major Internet or electricity supply failure for instance.

Logs and audit trails

In addition to producing logs and audit trails, cloud providers work with their customers to ensure that these logs and audit trails are properly secured, maintained for as long as the customer requires, and are accessible for the purposes of forensic investigation (e.g., eDiscovery).

Unique compliance requirements

In addition to the requirements to which customers are subject, the data centers used by cloud providers may also be subject to compliance requirements. Using a cloud service provider (CSP) can lead to additional security concerns around data jurisdiction since customer or tenant data may not remain on the same system, or in the same data center or even within the same provider's cloud.

Legal And Contractual Issues

Aside from the security and compliance issues enumerated above, cloud providers and their customers will negotiate terms around liability (stipulating how incidents involving data loss or compromise will be resolved, for example), intellectual property, and end-of-service (when data and applications are ultimately returned to the customer). In addition, there are considerations for acquiring data from the cloud that may be involved in litigation.[20] These issues are discussed in Service-Level Agreements (SLA).

Public Issues

Legal issues may also include records-keeping requirements in the public sector, where many agencies are required by law to retain and make available electronic records in a specific fashion. This may be determined by legislation, or law may require agencies to conform to the rules and practices set by a records-keeping agency. Public agencies using cloud computing and storage must take these concerns into account.

Potential privacy risks

while there are benefits, there are privacy and security concerns too. Data is travelling over the Internet and is stored in remote locations. In addition, cloud providers often serve multiple customers simultaneously. All of this may raise the scale of exposure to possible breaches, both accidental and deliberate. Concerns have been raised by many that cloud computing may lead to "function creep" — uses of data by cloud providers that were not anticipated when the information was originally collected and for which consent has typically not been obtained. Given how inexpensive it is to keep data, there is little incentive to remove the information from the cloud and more reasons to find other things to do with it.

How Does Network Security Work?

To understand What is network security?, it helps to understand that no single solution protects you from a variety of threats. You need multiple layers of security. If one fails, others still stand.

Network security is accomplished through hardware and software. The software must be constantly updated and managed to protect you from emerging threats.

A network security system usually consists of many components.

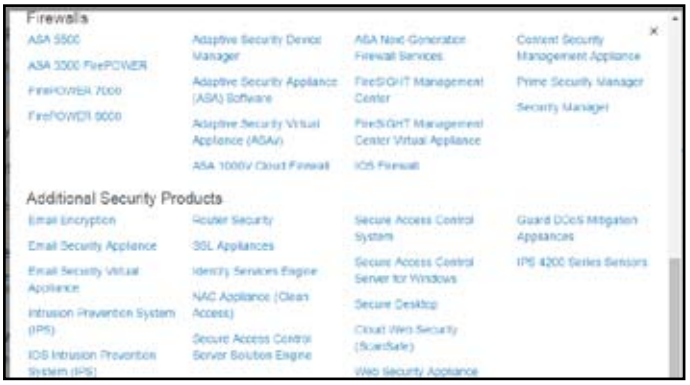
ISSN : 2394-2975 (Online)
ISSN : 2394-6814 (Print)

Ideally, all components work together, which minimizes maintenance and improves security.
Network security components often include:

- Anti-virus and anti-spyware
- Firewall, to block unauthorized access to your network
- Intrusion prevention systems (IPS), to identify fast-spreading threats, such as zero-day or zero-hour attacks
- Virtual Private Networks (VPNs), to provide secure remote access

What are the Business Benefits of Network Security?

With network security in place, your company will experience many business benefits. Your company is protected against business disruption, which helps keep employees productive. Network security helps your company meet mandatory regulatory compliance. Because network security helps protect your customers' data, it reduces the risk of legal action from data theft.
Ultimately, network security helps protect a business's reputation, which is one of its most important assets.
These are some security services those are provided to client according to his requirement..it include web service security as well home security and also for mobile like smart phones, android etc . There are too many companies those are provided security (cisco, quick heal,Canadian Police Association ,etc.)



Refrences

[1] *Abbadi, I.M. and Martin, A. (2013). Trust in the Cloud. Information Security Technical Report*
[2] *Agarwal, A. and Agarwal, A. (2014). The Security Risks Associated with Cloud Computing. International Journal of Computer Applications in Engineering Sciences, 1 (Special Issue on CNS), 257-259.*
[3] *Arshad, J, Townsend, P. and Xu, J. (2013).A novel intrusion severity analysis approach for Clouds. Future Generation Computer Systems, 29, 41*
[4] *Wikipedia.com/cloud computing*