Journal of Data Acquisition and Processing
ISSN: 1004-9037
https://sjcjycl.cn/
DOI: 10.5281/zenodo.9854905

NETWORK SECURITY AND ISSUES IN PRIVATE CLOUD

Dr.N.Prakash
Assistant Professor, Department of computer science, Gobi arts & science college.
Gobichettipalayam, Tamil Nadu India

Dr.S.Annapoorani
Assistant Professor, Department of computer science, Gobi arts & science college
Gobichettipalayam, Tamil Nadu

India Network security has grown in significance users of personal computers, businesses, and the armed forces. Security became a serious worry with the introduction of the internet, and the development of security technologies can be better understood by looking at security history. As private clouds have grown in popularity, more businesses are concentrating on how to safeguard their network security. Information security must be included into the infrastructure itself as part of the security system. This paper focuses on a variety of security issues related to cloud computing, examines some of the major research challenges in cloud security, offers solutions for securing the dynamic cloud environment, and provides a practical solution to avoid the challenges that cloud suppliers and buyers encounter.

The fundamental network security scenario, big data security, and the private cloud network security situation are also discussed in this article. It also analyses the pertinent assessment indexes and goes into more detail regarding the private cloud network. With the advent of the internet, security became a major concern. The internet structure itself allowed for many security threats to occur. Network security is becoming of great importance because of intellectual property that can be easily acquired through the internet.

KEYWORDS: *Network security, Access control, Cloud security, Cyber security*

1. INTRODUCTION

Network Security management is different for all kinds of situations and is necessary as the growing use of internet. 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. There are currently two fundamentally different networks, data networks and synchronous network comprised of switches. The internet is considered a data network. Since the current data network consists of computer-based routers, information can be obtained by special programs, such as “Trojan horses,” planted in the routers.

The synchronous network that consists of switches does not buffer data and therefore are not threatened by attackers. Then, in addition to systems administration vulnerabilities, cloud applications must also handle possible risks from cloud users, such as unidentified. Normal cloud risks include information abuse, malicious insiders, shaky interfaces and APIs, frequent innovation problems, information leakage or misery, account or administrative commandeering, and hazard profiles that are hidden. A legal and accurate understanding of

cloud security is a crucial need for the success of cloud sending. This paper's main focus is on understanding common perceptions on cloud security.

The target of this work is to give researchers and experts with an information platform about later. The fundamental commitments of this study are triple:

(1) This work features fundamental vulnerabilities of cloud security and spreads key issues in the field

(2) We orchestrate trademark answers for each kind of dangers in cloud security.

1.1 Network security

A crucial piece of technology for many different applications is system and network technology. For networks and applications, security is essential2. Although network security is a vital necessity in developing networks, there are very few security measures that can be quickly put into place. There is a "communication gap" between network and security technology developers. The Open Systems Interface (OSI) concept serves as the foundation for the well-developed process of network design. When developing networks, there are various benefits to using the OSI model. It offers modularity, flexibility, usability, and protocol standardization. It is simple to mix the protocols from several levels to build stacks that enable modular development. Individual layer implementation can be altered later without requiring other changes, providing flexibility.

When developing a secure network, the following need to be considered:

1. Access – authorized users are provided the means to communicate to and from a particular network.
2. Confidentiality – Information in the network remains private.
3. Authentication – Ensure the users of the network are who they say they are
4. Integrity – Ensure the message has not been modified in transit
5. Non-repudiation – Ensure the user does not refute that he used the network

These tools are encryption, authentication mechanisms, intrusion-detection, security management and firewalls. Network intrusions consist of packets that are introduced to cause problems for the following reasons:

• To consume resources uselessly
• To interfere with any system resource’s intended function
• To gain system knowledge that can be exploited in later attacks

2. DATA SECURITY

Cryptographic methods have to continue to advance due to the advancement of the hackers as well. When transferring cipher text over a network, it is helpful to have a secure network. This will allow for the cipher text to be protected, so that it is less likely for many people to even attempt to break the code. A secure network will also prevent someone from inserting unauthorized messages into the network. Therefore, hard ciphers are needed as well as attack-hard networks. It can be seen that the cryptography occurs at the application layer; therefore, the application writers are aware of its existence. The user can possibly choose different methods of data security.

2.1 Security Issues in Cloud

Data Hijacking

A vengeful performer will appear if Cloud seller assurance or programming interface credentials are lost. The cloud state might be blamed on someone outside of an association.

Information Breaches

Poor access the executives of object stockpiling pails and information stores cause touchy data to be made open, which has been one of the significant reasons for information breaks on the cloud.

Misuse and Nefarious utilization of cloud assets

Record seizing of a cloud record can result in the malevolent client to utilize the undermined assets to dispatch DDOS, spam and phishing crusades leaving the association inclined to lawful obligation.

Advanced threats(AT)

Once within a system, malware and advanced persistent threats adapt to the security measures, over time they build up a solid foundation and disperse horizontally, and when they reach their intended target, they exfiltrate sensitive data. These risks are challenging to identify and address.

Vulnerabilities

With Cloud administrations being multitenant, vulnerabilities that incorporate benefit acceleration and VM limit bouncing can cause information breaks and leave the applications and remaining burdens defenseless.

3. NETWORK SECURITY

3.1 Network Security Situational Awareness

Network security circumstance is a far reaching research point. It predominantly contains three levels. To start with, manage the gigantic network data, show network security circumstance with designs. Besides, the data are quantitative investigation, the qualities are disconnected, and the history and current circumstance of network security are assessed.

3.2 The Key Technology of Network Security Situational Mindfulness

One of the key advancements of network security circumstance is the data combination innovation, a bound together of various security equipments are gathered and changed into a standard data position which screens the security log or cautioning data. The Network security situational mindfulness depends on logical, the chronicled security events and network security status are analyzed and compared, and the network security status later on is anticipated.

The data that is stored on the network is done so with an ever-increasing degree of openness and ease, while at the same time with less and less security and secrecy. Data is easily stolen while being sent and stored by the organisation. Particularly, it is worried about data encryption.

3.3 The Security of Virtual Cloud Data

Big data and cloud computing are advancing thanks to the development of new network innovation. Organise security may be improved in the age of big data from a variety of angles, including physical security, host security, data content security, data transmission security, etc. Investigating enormous amounts of data, preventing hacker intrusions and assaults, and strengthening network security defences via the use of more dynamic and potent network

security measures are all extremely difficult tasks in the age of big data. It is helpful to know how to store and use data in the era of big data.

3.4 The Key Technologies of Private Cloud Network Security

The company will develop a number of network security technologies in the storage zone and transport layer to ensure the privacy of private clouds. The transferred data is encrypted at the transport layer. The recipients decipher the encrypted material once it has been encoded using technologies for transmission of important data. How to keep these data safely is important after data exchange security. The majority of the time, data security includes things like data border security for networks, data mutual isolation, data disaster recovery, etc.

The most comprehensive innovation is the new intelligent firewall. Intelligent firewall innovation is a different type of firewall innovation from traditional firewall innovation. It uses artificial intelligence and a fuzzy recovery database to effectively recognise the data. By preventing programmers from filtering network traffic, intelligent firewall innovation can maintain the private cloud's data security. The intelligent firewall has three different protection settings: intrusion avoidance, cheat prevention, and anti scanning.

4. KEY TECHNOLOGIES IN NETWORK SECURITY

Private cloud organize security can be comprised of five levels: gadget security layer, system security layer, network security layer, application security layer and data security layer. By breaking down the danger of each layer and receiving suitable safety efforts, the security objective can be accomplished: confidentiality, integrity, accessibility, controllability and non repudiation.

4.1 Network Security Situational Awareness of Private

In the age of big data, it is possible to collect many types of data designs, such as hardware logs, security logs, hardware logs, and data in private clouds that were used in administrative frameworks. Thus, we are better knowledgeable about the state of network security. The rapid processing of massive amounts of data is another benefit of big data. People are able to thoroughly study the parameters of network data and traffic. High insight model techniques have strict requirements for computational resources.

First, data base can be built up by contemplating network attack cases, including standard, attributes, environment, the most well-known equipments and techniques.

Second, environment vulnerability data base can be built up by analyzing the limitations of private cloud design framework vulnerabilities and storage devices.

Third, environment threat data base can be built up by dissecting the design topology and hardware of private cloud.

Finally, by dissecting and looking at the three sorts of data base horizontally, individuals can affirm the adequacy of security incidents.

4.2 The Assessment Index of Network Security Situational Mindfulness on Private Cloud

We should compile a thorough report from five perspectives, including physical security, host security, network security, data security, and content security, in order to evaluate the security situation of private clouds. The investigation may include a look at the storage disk's security as well as the security of the data framework, the security of the data itself, the security of data

transmission, and the security of the usage of private cloud data. The network security Index is among them the best indicator of the network security situation.

Three categories make up a private cloud architecture: reliability, susceptibility, and network risk. The security of the hardware and programming, which is based on the network's continuous and consistent activity throughout a certain duration, both indicate the network's stability. The network is vulnerable in terms of its capacity for prevention and disaster resilience.

4.3 The Security Situation Warning of Private Cloud Network

Network security is currently at the highest level of the security guard structure. Therefore, the private cloud will use sophisticated analysis technology to analyse the dubious data in the network for a considerable amount of time; the logical principle will be provided in the network security scenario. It's crucial to develop a long-term monitoring approach in order to create an optimal network security circumstance gauge pattern map and increase the use of security circumstance expectation. As a result of the network's rapid development, the assaults force is becoming more and more well-rounded, the danger is also rising, and the network security situation is becoming more unpredictable.

5. AN INTERNET ARCHITECTURE AND SECURITY ASPECTS

The security architecture of the internet protocol, known as IP Security, is a standardization of internet security. IP security, IPsec, covers the new generation of IP (IPv6) as well as the current version (IPv4). Although new techniques, such as IPsec, have been developed to overcome internet's best-known deficiencies, they seem to be insufficient. IPSec is a point-to-point protocol, one side encrypts, the other decrypts and both sides share key or keys. IPSec can be used in two modes, namely transport mode and tunnel modes.

5.1 IPv4 Architecture

The protocol contains a couple aspects which caused problems with its use. These problems do not all relate to security.

The causes of problems with the protocol are:

1. Address Space
2. Routing
3. Configuration
4. Security
5. Quality of Service

The IPv4 architecture has an address that is 32 bits wide. This limits the maximum number of computers that can be connected to the internet. The 32-bit address provides for a maximum of two billions computers to be connected to the internet. The problem of exceeding that number was not foreseen when the protocol was created. The small address space of the IPv4 facilitates malicious code distribution.

5.2 IPv6 Architecture

When IPv6 was being developed, emphasis was placed on aspects of the IPv4 protocol that needed to be improved. The development efforts were placed in the following areas:

1. Routing and addressing
2. Multi-protocol architecture
3. Security architecture

4. Traffic control

The IPv6 protocol's address space was extended by supporting 128 bit addresses. With 128 bit addresses, the protocol can support up to 3.4*(10)^38 machines. The address bits are used less efficiently in this protocol because it simplifies addressing configuration.7 The IPv6 routing system is more efficient and enables smaller global routing tables. The host configuration is also simplified. Hosts can automatically configure themselves.

5.3 Common internet attack methods

Some attacks gain system knowledge or personal information, such as eavesdropping and phishing. Attacks can also interfere with the system's intended function, such as viruses, worms and Trojans.

5.3.1 Eavesdropping

Eavesdropping is the term used to describe the unauthorised interception of conversations. The term "passive eavesdropping" refers to when someone merely listens covertly to networked messages. Active eavesdropping, on the other hand, involves the intrusive party listening and adding something to the communication stream. This can cause the messages to be twisted. This method allows for the theft of sensitive data.

5.3.2 Viruses

Viruses are self-replicating programmes that spread through the usage of files. The virus will begin to operate on the system as soon as a file is opened.

5.3.3 Worms

A worm and a virus are similar in that they both have the ability to replicate themselves, however a worm does not need a file to spread. Mass-mailing worms and network-aware worms are the two primary categories of worms. Email is a method used by mass mailing worms to infect other computers. Worms that are network-aware pose a serious threat to the Internet. Once the network-aware worm has gained access to the target host, it can infect it via a Trojan or another method.

5.3.4 Trojans

Trojans appear to be benign programs to the user, but will actually have some malicious purpose. Trojans usually carry some payload such as a virus.

6 TECHNOLOGIES FOR INTERNET SECURITY

Internet threats will continue to be a major issue in the global world as long as information is accessible and transferred across the Internet. Different defense and detection mechanisms were developed to deal with these attacks.

6.1 Cryptographic systems

Today, a helpful and popular technique in security engineering is cryptography. It entailed converting information into incomprehensible data by using cyphers and codes.

6.2 Firewall

A firewall is a common perimeter defence or border control device. A firewall's main function is to prevent traffic from the outside, but it may also be used to stop internal communication. The first line of defence against invaders is a firewall. It is a mechanism made to stop unauthorised users from accessing or leaving a private network. Firewalls can be set up as either hardware, software, or a hybrid of the two.

6.3 Intrusion Detection System

An Intrusion Detection System (IDS) is an additional protection measure that helps ward off computer intrusions. IDS systems can be software and hardware devices used to detect an attack. IDS products are used to monitor connection in determining whether attacks are been launched. Some IDS systems just monitor and alert of an attack, whereas others try to block the attack.

6.4 Anti Malware Software and scanners

Viruses, worms and Trojan horses are all examples of malicious software, or Malware for short. Special so-called anti-Malware tools are used to detect them and cure an infected system.

7 CONCLUSION

Network Security is the most vital component in information security because it is responsible for securing all information passed through networked computers. This article conducted a survey to examine all significant security aspects of cloud computing. The convergence covered network security, computer security, and protection of data. The literature study examined all of the significant risks and weaknesses associated with cloud computing, as well as their remedies.

Artificial Intelligence provides new possibilities for solving the problem of network security In the future, based on artificial intelligence and powerful data analysis ability, people can anticipate the danger ahead and greatly enhance the ability of network security defense. In the future, more consideration will be given to the use of artificial intelligence to solve the security problem of any organization's private cloud.

REFERENCES

[1] FireEye. Cybersecurity's Maginot Line: A Realworld Assessment of the Defense-in-Depth Model [R]. FireEye, 2015.

[2] Sun F. X. Artificial immune danger based model for network security evaluation. Journal of Networks.2011,6(2) :255-262.

[3] Zhang J. F. Research on key technologies of network security assessment [D]. Changsha: National University of Defense Technology,2013.

[4] K. Gai, M. Qiu, H. Zhao, L. Tao, and Z. Zong. Dynamic energy-aware cloudlet-based mobile cloud computing model for green computing. Journal of Network and Computer Applications, 59:46–54, 2015.

[5] Simmonds, A; Sandilands, P; Van Ekert, L (2004) Ontology for Network Security Attacks". Lecture Notes in Computer Science. Lecture Notes in Computer Science 3285, pp. 317–323.

[6] Elkamchouchi, H. M; Emarah, A. A. M; Hagras, E. A. A, A New Secure Hash Dynamic Structure Algorithm (SHDSA) for Public Key Digital Signature Schemes‖, the 23rd National Radio Science Conference (NRSC 2006).

[7] Predictions and Trends for Information, Computer and Network Security http://www.sans.edu/research/security-laboratory/article/2140 [9] Cloud Security Alliance Big Data Analytics for Security Intelligence, https://downloads.cloudsecurityalliance.org/initiatives/bdwg/Big_Data_ Analytics_for_Security_Intelligence.pdf