A Review of Security Issues in Cloud Computing

Ogala Justin Onyarin & Mughele Sophia Ese (Ph.D)
Department Computer Science
University of Delta
Agbor, Delta State, Nigeria
Email: Justin.ogala@unidel.edu.ng, prettysophy99@gmail.com
Tel: +2347063649842; +2348035859666

Abstract

Cloud computing is one of the most popular terms in the computer industry right now. Virtualization enables resource sharing, which includes software, platform, and infrastructure. The underlying technology underpinning cloud resource sharing is virtualization. This environment aspires to be dynamic, dependable, and configurable, with a high level of service assurance. Security is just as important in the cloud as it is everywhere else. Various people have different perspectives on cloud computing. Some people feel that using the cloud is risky. Cloud providers go to great lengths to assure security. This study looks at a few important security vulnerabilities with cloud computing, as well as available remedies to those security issues in the cloud computing sector.

Keywords —Cloud Computing Security, Distributed Networks Security, Network Security.

Introduction

loud computing is a pay-per-use paradigm for providing on-demand network access to a shared pool of programmable computer resources that can be quickly provided and released with minimum administration effort or service provider contact. [1][4][5]. Software-as-a-service, platform-as-a-service, and infrastructure-as-a-service are the three categories of cloud services that may be provided and consumed. [1][2][3][5]. The three primary categories of cloud computing services are as follows. Software-as-a-Service is the first sort of cloud computing service (SAAS). Subscribers to this service get access to the provider's software applications that are hosted on a cloud infrastructure. The application is managed and controlled by the service providers. Customers do not have to own the program; instead, they simply have to pay to utilize it via a web API [1] [2]. Google Docs, for example, uses JAVA Script, which runs in the browser [3]. Platform-as-a-Service is the second type of cloud service (PaaS). It's a different method of delivering applications. PaaS allows customers to install their apps on the provider's cloud infrastructure using the provider's programming languages and tools.

Citation Ogala, J.O & & Mughele, S.E. (2022). A review of Security Issues in Cloud Computing
SMART-IEEE-ACity-ICTU-CRACC-ICTU-Foundations Series
Book Chapter on Web of Deceit - African Multistakeholders' Perspective on
Online Safety and Associated Correlates Using Multi-Throng Theoretical, Review, Empirical
and Design Approaches. Pp 279 -290. www.isteams.net/bookchapter2022.
DOI https://doi.org/ 10.22624/AIMS/BK2022-P47

The consumer is not responsible for the underlying cloud infrastructure, but he or she does have control over the installed application [1] [2]. The Google App Engine, for example, is a service that allows developers to design apps that operate on Google's infrastructure [3].

Infrastructure-as-a-Service is the third and final form of cloud computing (IaaS). This service essentially provides virtual machine images as a service, with the machine containing anything the developer desire [3]. Customers can acquire these resources as an outsourced service supplied through the network cloud [2] instead of acquiring servers, software, data center resources, network equipment, and the competence to administer them. To meet changes in their requirements, the customer can automatically expand or reduce the number of virtual computers running at any one moment. Host firewalls, for example [1] [2] [3]. There are a variety of cloud deployment models to choose from. We'll go through three different sorts of clouds. The private cloud is the first. An internal cloud is another name for this.

The architecture of Cloud Computing

The front end and the back end are the two halves of a cloud computing system. These two ends are frequently connected via the Internet. The user interface is the front end, while the back end is the system's "cloud" component. The client's PC and the program necessary to access the cloud computing system make up the front end. The numerous computers, servers, and data storage systems that make up the "cloud" of computing services [2][5][6] are represented on the back end of the system in figure 1. The system is managed by a central server, which keeps track of traffic and client needs to ensure that everything operates well. It adheres to a set of rules known as protocols and makes use of a type of software known as middleware [2][5].

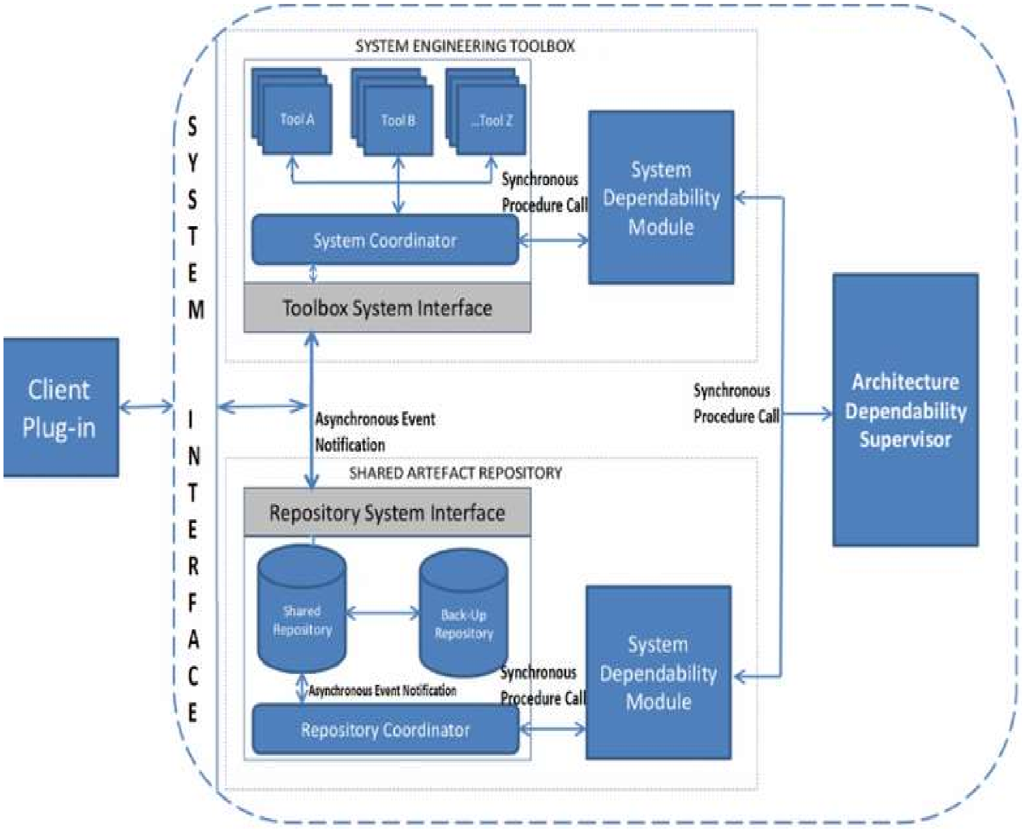

SYSTEM ENGINEERING TOOLBOX
Tool A
Tool B
...Tool Z
Synchronous Procedure Call
System Dependability Module
System Coordinator
Toolbox System Interface
SYSTEM INTERFACE
Client Plug-in
Asynchronous Event Notification
Synchronous Procedure Call
Architecture Dependability Supervisor
SHARED ARTEFACT REPOSITORY
Repository System Interface
Shared Repository
Back-Up Repository
Asynchronous Event Notification
Synchronous Procedure Call
System Dependability Module
Repository Coordinator

Figure 1 . Example of a High-Level Cloud Middleware Architecture

The key system that administers and regulates services is cloud middleware, often known as cloud OS. Networked machines can interact with each other thanks to middleware [6]. Cloud middleware includes Google App Engine and Amazon EC2/S3 [20]. To make applications appropriate for network clouds, an Application Programming Interface (API) for applications, acquisition of resources such as processing power and storage, and machine image management must be offered [2][5][13].

The cloud computing infrastructure is depicted in Figure 2 in a simplified form. First, the client submits service requests. The system's administration then locates the appropriate resources. Following that, system provisioning locates the appropriate resources. Following the discovery of computer resources, the client request is carried out. Finally, the clients receive the outcomes of their service requests [2][6][13].

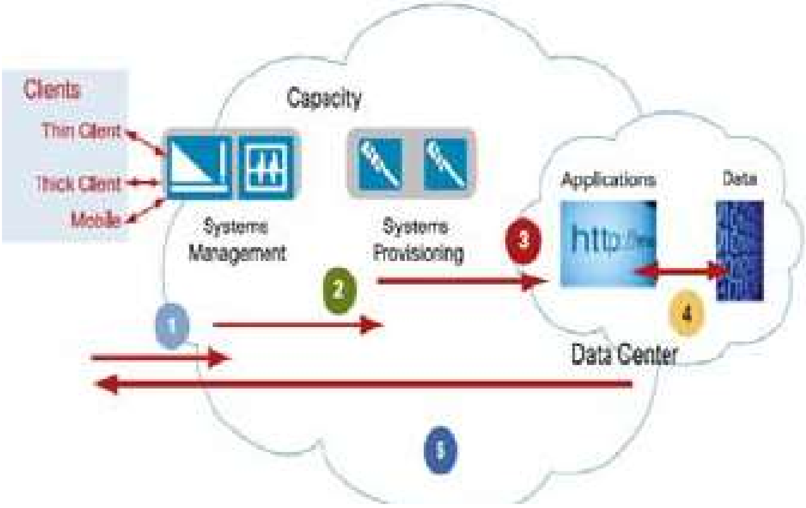


Figure 2. Workflow in Cloud Computing

In the next part, we'll look at some of the various potential applications of cloud computing and how it may benefit businesses of all sizes.

Applications Of Cloud Computing

Cloud computing has nearly endless applicability. A cloud computing system can run all of the apps that a desktop computer can run with the correct middleware. Other usages include:

1) Clients will be able to access their programs and data from any computer connected to the Internet at any time [6].
2) Organizations that rely on computers for their operations have traditionally had to purchase all of the necessary software or software licenses for each employee. These enterprises may use the cloud computing system to acquire access to all of their essential computer software without having to buy them. I, However, the company might pay a per-use fee to a cloud service provider [4] [6].
3) Client hardware expenditures will be reduced by using a cloud computing system. The user will not be required to purchase the computer with the largest RAM, nor will he be required to purchase a huge hard drive to keep his data. This client's needs will be met through the cloud system. Clients just need to purchase a computer terminal with a display and input devices, as well as enough processing power to run the middleware required to connect to the cloud system [4][6][[18].

4) Servers and digital storage devices take up a lot of room in most businesses. Some businesses do not have enough physical space on-site to house their servers and databases, so they rent space. The cloud computing system allows these businesses to store their data on the servers of others (cloud service providers), removing the need for them to have their own physical space on the client-side. [6] and [17].
5) Clients can benefit from the massive processing power of the cloud system. Clients can transmit large complicated calculations to the cloud for processing, similar to grid computing. To speed up the computation, the cloud system will employ the processing power of the appropriate number of available machines on the back end [1][6][8].

Cloud computing provides several advantages over traditional computer systems, but it also has its drawbacks. The primary security concerns in cloud computing systems, as well as known remedies, are discussed in the next section.

Cloud Computing Issues

Cloud computing raises two significant concerns: security and privacy. In the cloud computing world, customers can access computing capabilities that are higher than what is accessible in their physical surroundings. A user must transport data via the cloud to gain access to this virtual environment. As a result, there are various security risks [4] [7] [8] [16]. Some of the issues include:

A. Information Security

It is responsible for the prevention of data's confidentiality, integrity, and availability, independent of the data's format [9]. Various information security risks that may arise in a given setting include::

1) Data control is lost

Outsourcing entails a considerable loss of data control. Large banks do not want to operate cloud-based software that may compromise their data due to contact with another program. [3] [10]. The Amazon Simple Storage Service (S3) APIs enable access restrictions at both the bucket and object level, with defaults allowing only authorized access by the bucket and/or object creator. Unless a customer permits anonymous access to their data, a user must first be authenticated using an HMAC-SHA1 signature of the request using the user's private key before they may access it. [9] [15] [16]. As a result, the client has complete control over who gets access to their information. [13].

2) Data Integrity

The guarantee that data changes solely in response to approved transactions are known as data integrity, and if the client is in charge of creating and verifying database queries, and the server executes them blindly, the intruder will always be able to change the client-side code to do anything he wants with the backend database. In most cases, this indicates the invader has complete control over data [3]. There is currently no uniform standard for ensuring data integrity [8]. Users in this new computer environment are expected to accept the underlying concept of trust. Indeed, some have speculated that cloud computing's primary challenge is trust [7].

3) Seizure Risk

When you use a public cloud, you're sharing computer resources with other businesses. Because another corporation has broken the law, exposing your data in a shared environment might provide the authorities with "reasonable cause" to confiscate your assets. Data may be in danger of seizure just because you share the environment in the cloud [4][8]. The only way to secure users' data from being seized is to encrypt it. The subpoena will compel the cloud provider to provide up the user's data and whatever access it may have to it, but the cloud provider will not have access to or decryption keys for the user's data. As a result, the user will have the same amount of control as he has in his own data center. [4][16].

4) Incompatibility Issue

If you decide to switch cloud vendors, the storage services offered by one may be incompatible with the services provided by another. Vendors are notorious for providing "sticky services," which are services that an end-user may find difficult to move from one cloud provider to another. Amazon's "Simple Storage Service" [S3], for example, is not compatible with IBM's Blue Cloud, Google, or Dell. [4] [8][13]. Both Amazon and Microsoft have declined to join the Open Cloud Manifesto, which was just released. Amazon and Microsoft are both working on interoperability on their grounds [11]. [12][14].

5) Continuous Feature Inclusions

Cloud apps are always evolving, and users must stay current with program updates to ensure their security. The SDLC (Software development life cycle) and security will be affected by the speed at which cloud applications change [4]. [8]. Updates to AWS infrastructure are done in such a manner that in the great majority of situations they do not influence the customer and their Service use [9] [13]. AWS interacts with customers, either through email or through the AWS Service Health Dashboard when there is a potential that their Service use may be affected [9].

6) Failure of the cloud provider's security

The breach of subscriber systems occurs when the cloud provider fails to effectively protect elements of its infrastructure, particularly in the maintenance of physical access control. A cloud can be made up of several entities, and no cloud can be more secure than its weakest connection in this scenario. [3][7]. Customers are supposed to have faith in the provider's security. Small and medium-sized organizations may find that supplier security outweighs client security. Details that assist in guaranteeing that the appropriate things are done are difficult to get by [3][7].

7) Cloud Provider Deteriorates

This scenario can take several forms, including insolvency, a decision to pivot the business or abroad, and a long-term outage. Whatever is going on, subscribers are in danger of losing access to their production system as a result of another company's actions. Subscribers also run the risk of the organization in charge of their data failing to safeguard it according to the service levels to which they may have previously agreed [4]. The sole alternative for users is to choose a second cloud provider and employ automatic, frequent backups, for which several open source and commercial solutions are available, to ensure that any current and historical data may be restored even if the user's cloud provider goes out of business [4].

B. Network Security

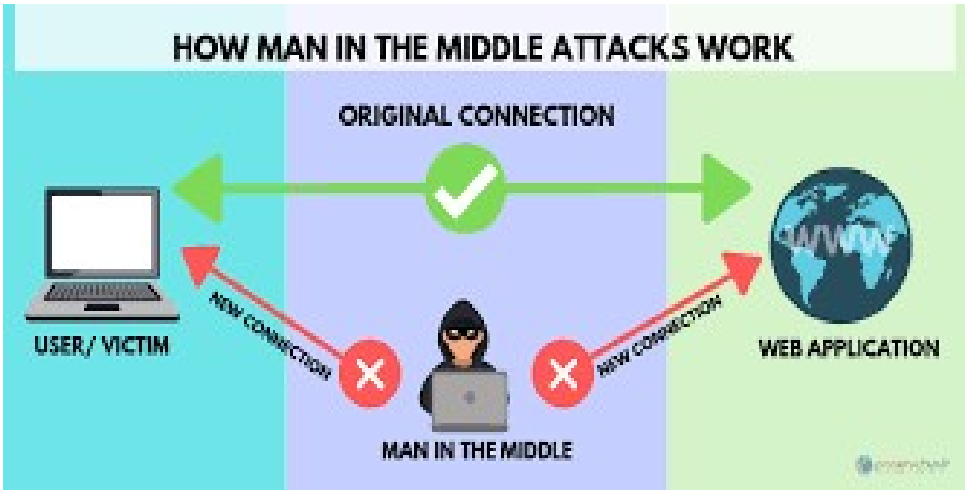
Data must be protected during delivery between the terminal user and the computer, as well as between the computer and the web browser [21][22]. Among the various network security techniques that may be used in this review are:

1) DDOS (Distributed Denial of Service)

A DDOS attack uses a significant amount of network traffic to bring servers and networks down, and consumers are denied access to a certain Internet-based service. In a well-known worst-case scenario, attackers employ botnets to launch DDOS attacks. Subscribers or providers may be subjected to blackmail to prevent hackers from targeting the network [21][14]. The Application Programming Interface (API) endpoints of Amazon Web Service (AWS) are hosted on enormous, Internet-scale, world-class infrastructure that benefits from the same engineering skill that has helped Amazon become the world's largest online retailer. DDOS mitigation solutions that are proprietary are utilized. To provide Internet access variety, Amazon's networks are multi-homed among some providers [9].

2) Man in the Middle Attack

This is a type of active eavesdropping in which the attacker establishes separate connections with the victims and transmits messages between them, giving the impression that they are conversing privately when, in reality, the attacker is controlling the whole discussion [21]. All AWS APIs are accessible over SSL-protected endpoints with server authentication. On the initial boot, Amazon EC2 AMIs creates fresh SSH host certificates and log them to the instance's console. Before login into the instance for the first time, customers may utilize the secure APIs to contact the console and get the host certificates. For the whole of their transactions with AWS, customers are advised to utilize SSL [9].



Source: https://wallstreetinv.com/cyber-security/man-in-the-middle-attack-mitm/

3) IP spoofing

IP spoofing is the production of TCP/IP packets using the IP address of someone else. When an intruder gains unauthorized access to a computer, he sends messages to a computer with an IP address that indicates the communication is from a trustworthy host. [21] [22]. Spoofed network traffic cannot be sent from Amazon EC2 instances. An instance cannot send traffic with a source IP or MAC address other than its own across the Amazon-controlled, host-based firewall architecture [9].

4) Port Scanning

If the Subscriber sets the security group to allow traffic from any source to a certain port, that port becomes exposed to a port scan. Because a port is where data centers and exits a computer, port scanning identifies open gateways to a computer [21]. Because visiting an Internet server exposes a port, which opens a door to your computer, there is no way to prevent someone from port scanning your computer while you are online [8]. The Amazon Elastic Compute Cloud (EC2) Acceptable Use Policy prohibits customers from scanning ports (AUP). Violations of the AUP are handled seriously, and each one that is reported is looked into. Customers have the option to report suspected abuse. It is capped and blocked when port scanning is discovered. Post-scans of Amazon EC2 instances are unsuccessful in most cases since all inbound ports on Amazon EC2 instances are closed by default and must be opened by the customer [9].

5) Packet Sniffing:

Other Guests' Packet Sniffing: Packet sniffing entails listening to the raw network device (through software) for packets of interest. When the program recognizes a packet that meets particular requirements, it records it in a file. Words like "login" or "password" are the most prevalent criterion for an intriguing packet [21][22]. It is not feasible for a promiscuous virtual instance to accept or "sniff" communications destined for another virtual instance.

Customers can enable promiscuous mode on their interfaces, but the hypervisor will not deliver any traffic that is not addressed to them [9]. Despite virtualized instances owned by the same customer and running on the same physical host are unable to eavesdrop on each other's traffic. Attacks like ARP cache poisoning aren't possible with Amazon EC2. While Amazon EC2 provides enough protection against a customer unintentionally or deliberately attempting to access another's data, customers should encrypt important communication as a routine practice [9].

C. Security Issues

There are more challenges in a virtualized environment since security is now divided into two tiers: physical host security and virtual machine security. If the security of the physical host server is breached, all virtual machines on that host server are affected. A hacked virtual computer might potentially cause havoc on the actual host server, affecting all other virtual machines on the same server [23]. Amid the various security issues that may be used in this study are:

1) Isolation of instances:

Systems running on the same physical computer at the same time as each other are called 'Isolation', which means they are operating in isolation from one another. Isolation ensures that various instances running on different machines are not able to interact directly with each other, and can instead operate independently of each other. To achieve cloud virtualization efficiency, virtual computers from several businesses must be co-located on the same physical resources. Physical segregation and hardware-based security cannot guard against assaults across virtual machines on the same server, even if typical data center security still applies in the cloud [18].

Administrative access is provided through the Internet rather than the traditional data center model's limited and restricted direct or on-premises link. Due to the increased danger of exposure, changes in system management and access control restrictions will need to be closely monitored [8]. The Xen hypervisor is used to isolate instances operating on the same physical system. Amazon engages in the Xen community, ensuring that it is up to date on the newest advances. AWS firewalls are also located within the hypervisor layer, between the actual network interface and the virtual interface of the instance. Because all packets must transit via this layer, the neighbors of an instance have no more access to it than any other host on the Internet and may be regarded as if they were on different physical hosts. Similar approaches are used to isolate the physical RAM [9]

2) Host Operating System:

To acquire access to purpose-built administration hosts, administrators with a business requirement to access management plans must use multi-factor authentication. These administrative hosts are systems that have been conceived, constructed, configured, and hardened particularly to safeguard the cloud administration layer. This type of access is tracked and inspected. The credentials and access to such hosts and corresponding systems are terminated when an employee no longer has a business requirement to access the management plane [18].

3) Guests Operating System

The consumer has total control over virtual instances. Customers have completed administrative or root access to their accounts, services, and applications. AWS has no access to client instances and is unable to get into the guest OS. Customers should stop password-based access to their hosts and use some type of multi-factor authentication to obtain access to their instances, or at the very least certificate-based SSH Version 2 access, as recommended by AWS [9][13][15]. Customers should also utilize a privilege escalation method that includes per-user reporting. If the guest OS is Linux, for example, they should use certificate-based SSHv2 to access their virtual instance, block remote root login, employ command-line logging, and use'sodu' for privilege escalation after hardening their instance. Customers should create their key pairs to ensure that they are unique and are not shared with other customers or AWS [9].

AWS Multi-Factor Authentication (AWS MFA) is a security feature that gives you more control over your AWS account settings. Before access to an AWS account settings is permitted, it requires a valid six-digit, single-use code with an authentication device in your possession in addition to your usual AWS login information. This is known as Multi-Factor Authentication because it requires customers to submit both their Amazon email address and password (the first "factor": something they know) as well as the specific code from their authentication device (the second "factor": something they have).

D. Basic Security Issues

Aside from the aforementioned concerns, there are a few more security issues that are slowing cloud computing adoption and must be addressed. Data Location: When a user utilizes the cloud, he or she is unlikely to know exactly where his or her data is kept, or in which nation [3][4][8]? Amazon does not even provide the locations of its data centers. They merely state that each data center is housed in an unassuming structure with a military-grade security fence. Even if customers are aware that their database server is situated in the USA-east-1a availability zone, they are unaware of the location of the data center9s0 that supports that availability zone, or which of the three East Coast availability zones us-east-1a represents [4]. Amongst the frequent basic security issues include:

1. Data sanitization

Data sanitization refers to the process of deleting sensitive data from a storage medium. What happens to data saved in a cloud computing environment once it has passed its user's "use by date" [18] is always a problem for cloud computing customers. AWS protocols include a decommissioning process when a storage device reaches the end of its useful life, ensuring that client data is not accessible to unauthorized parties. As part of the decommissioning process, AWS utilizes the DoD 5220.22-M approach as described in the National Industrial Security Program Operating Manual to delete data [9][13]. Whenever item and attribute data are erased from a domain, the mapping is removed from the domain instantly and is usually completed in seconds. There is no remote access to the erased data after the mapping is gone. After that, the storage region is only available for write operations, and the data is overwritten by freshly stored data [9].

2. Job depletion caused by a virus or worm:

This occurs when one job consumes a large number of resources, causing the other jobs to run out of resources. Customers can reserve resources ahead of time. The priority of the impacted tasks/jobs can also be reduced by the customer [16] [18].

Related Working Groups On The Cloud

A working group is a collection of researchers who have come together to work on new research projects that would be challenging for one of them to undertake on their own. Working groups are frequently formed with the goal of producing an informational document, a standard, or finding a solution to a system or network's problems.. Typically, the working group tries to bring together specialists on a certain issue. Task groups and technical advisory groups are other names for working groups. The Open Cloud Consortium (OCC) is divided into many working groups [8]. The OCC's mission is to facilitate the development of cloud computing standards and a framework for interoperability among different clouds [19].

A working group on broad area clouds and the influence of network protocols on clouds is also present. This working group is focused on creating wide-area cloud technologies, as well as providing methodology and benchmarks for assessing wide-area clouds. This working group's mission is to investigate the applicability of TCP variations and the usage of other network protocols in cloud environments. The working group on sharing information, security, and clouds are primarily concerned with standards and standard-based frameworks for cloud data exchange. This is especially true for clouds that belong to multiple organizations and may be subject to different regulations and authorities.

This group is also interested in cloud security architectures. Finally, a working group called the Open Cloud Test-bed oversees and operates the open cloud test-bed [19]. The Distributed Management Task Force (DMTF) [8] is another extremely active group in the realm of cloud computing. The distributed management task force, according to their website, enables more effective administration of millions of IT systems throughout the world by bringing together the IT industry to work on the creation, validation, and promotion of systems management standards [24][25]. With 160 member firms and organizations and over 4,000 active participants from 43 countries, this association represents the whole sector. The DMTF is led by 16 industry-leading technology businesses on its board of directors.

The Virtualization Management Initiative was launched by the DMTF (VMAN). The VMAN brings the power of virtualization to virtual computing environments by establishing widely approved interoperability and portability standards. VMAN allows IT, administrators, to deploy preinstalled, preconfigured solutions across heterogeneous computing networks and manage them during their full life cycle [20][25].

Security Standards For Cloud Computing

The methods, procedures, and practices required to implement a security program are defined by security standards. These standards also apply to cloud-related IT operations, and they contain specific actions to guarantee that a safe environment is maintained in the cloud, ensuring the privacy and security of private information. Security standards are founded on a set of fundamental principles that are meant to safeguard this sort of trusted environment. Layers of protection, often known as defense-in-depth, are a core security philosophy. This entails having many systems that work together to offer security even if one fails.

A firewall in combination with an intrusion detection system is an example (IDS). Because there is no single point of failure and no single entry vector via which an attack may occur, defense in depth ensures security. As a result, a false dichotomy exists between providing network security in the center of a network (i.e., in the cloud) or at the endpoints [8]. Because no one security system can provide a complete solution, it is considered preferable to safeguard all systems. This kind of tiered security is exactly what we're seeing in cloud computing. Security was traditionally implemented at the endpoints, where the user had control over access. An organization had no option but to install firewalls, intrusion detection systems, and antivirus software on its network. Additional security may now be given inside the cloud with the emergence of managed security services supplied by cloud providers [8][9].

Some of the innumerable network security standard for cloud computing include:

1. SAML (Security Assertion Markup Language)

SAML is an XML-based standard for exchanging authentication, authorization, and attribute data between online parties. It enables enterprises to securely convey claims about a principal's identity and entitlements across partner entities. In an XML format, SAML standardizes user authentication, entitlements, and attribute information requests and replies. This format may then be used to ask a SAML authority for security information about a principal. The asserting party, also known as a SMAL authority, is a platform or application that could also communicate intelligence information. A partner site that gets security information is known as the relying party, assertion consumer, or asking party. The authentication status, access authorization, and attribute information of a subject are among the data transferred. A subject is an entity in a certain domain identified by an email address, such as a printer [8]. SAML is based on several existing protocols, including SOAP, HTTP, and XML. SAML mandates the usage of SOAP and uses HTTP as its communication protocol.

2. Open Authentication (OAuth):

OAuth is an open protocol created by Blaine Cook and Chris Messina to offer safe API authorization for a variety of online apps in a simple, standardized manner. OAuth is a technique for communicating with and publishing protected data. OAuth gives users access to their data while keeping account credentials safe for developers. It also allows users to provide access to their data, which is shared with the service provider and consumers, without revealing their entire identity. OAuth is the foundation upon which further extensions and protocols can be constructed. Many requested functionality, such as automatic endpoint discovery, language support, support for XML- RPC and SOAP, the standard definition of resource access, OpenID integration, signature methods, and so on, are by design not accessible in OAuth Core 1.0 [8]. The heart of the protocol is concerned with the establishment of a method for exchanging a user name and password for a token with defined privileges, as well as the provision of tools to safeguard the token. It's important to remember that the protocol doesn't guarantee security or privacy.. In truth, OAuth does not provide any privacy by itself and relies on other protocols such as SSL to do so.

3. OpenID

It is an open, decentralized standard for user authentication and access control. It allows users to log onto many services using the same digital identity. It is a single-sign-on (SSO) method of access control. OpenID replaces the common log-in process, i.e. a log-in name and a password, by allowing users to log in once and gain access to resources across participating systems. An OpenID is in the form of a unique URL and is authenticated by the entity hosting the OpenID URL [9]. The OpenID protocol does not rely on a central authority to authenticate a user's identity. Neither the OpenID protocol nor any websites requiring identification can mandate that a specific type of authentication be used; nonstandard forms of authentication such as smart cards, biometrics, or ordinary password are allowed [8].

4. SSL/TLS: Transport Layer Security (TLS) and its precursor, Secure Sockets

Layer (SSL), are cryptographically secure protocols that offer data integrity and security for TCP/IP connections. At the transport layer, TLS and SSL encrypt the segments of network connections. TLS allows client/server programs to interact across a network in a secure manner that prevents eavesdropping, manipulation, and message forging [21]. TLS uses cryptography to enable endpoint authentication and data secrecy. TLS authentication is one-way: the client already knows the server's identity, hence the server is authenticated. The client is still unauthenticated in this situation [12]. TLS also has a more secure bilateral connection mode, which ensures that both sides of the connection are interacting with the person to whom they believe they are connected. Mutual (assured) authentication is the term for this. There are three basic phases in TLS. The first stage is to negotiate algorithm support among peers.

The client and server negotiate cipher suites at this phase, which define which ciphers are utilized. The next step is to decide on key exchange and authentication. During this step, the key exchange and authentication algorithm to be utilized, as well as the message authentication codes, are decided. Typically, public key algorithms are used for key exchange and authentication. The symmetric cipher encryption and message encryption are the last steps. Cryptographic hash functions are used to create the message authentication codes. Data transmission can commence when these decisions are made [9][12].

Conclusion

The cloud computing phenomenon is getting a lot of interest throughout the world because of its lower total cost of ownership, scalability, competitive differentiation, less complexity for customers, and faster and easier service procurement. While cloud computing has significant advantages, people approach the problem from various perspectives. Some people feel a cloud is a dangerous place. However, few people feel it is safer than their security provider, especially small businesses that lack the resources to maintain the necessary security. Several significant financial institutions and government bodies continue to be cautious.

They say they won't be shifting to the cloud anytime soon since they don't know how to assess their risks. Cloud computing requires some standardization in the security environment, as well as third-party certification to ensure that standards are met, to gain complete acceptance from all potential users, including individuals, small businesses, Fortune 500 companies, and the government We develop a precise characterization of the cloud security challenge and essential elements that any suggested security solution should address based on this study.

References

[1] Csrc.nist.gov. (2021). Cloud Computing | CSRC. [online] Available at: <http://csrc.nist.gov/groups/SNS/cloud-computing/index.html> [Accessed 20 February 2022].

[2] Paper, C. W. (2009) http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/white_paper_c11-532553.html, published 2009, pp. 1-6.

[3] Viega, J. (2009). McAffee, Cloud Computing, and the Common Man," published on the IEEE Journal ON Cloud. Computers & Security, (August), 106–108.

[4] George Reese (2009), "Cloud Application Architectures", First edition, O'Reilly Media, April 2009, ISBN 9780596156367, pp. 2-4, 99-118.

[5] En.wikipedia.org. (2001). Cloud computing security - Wikipedia. [online] Available at: <https://en.wikipedia.org/wiki/Cloud_computing_security> [Accessed 20 February 2022].

[6] Strickland, J., (n.d). How Cloud Computing Works. [online] HowStuffWorks. Available at: <https://computer.howstuffworks.com/cloud-computing/cloud-computing.htm> [Accessed 20 February 2022].

[7] John Harauz, Lori M. Kaufman, Bruce Potter (2009), "Data Security in the World of Cloud Computing," published on the IEEE Journal on Cloud Computing Security, July/August 2009, Vol. 7, No.4, pp. 61-64.

[8] John W. Rittinghouse, James F. Ransome (2009), "Cloud Computing Implementation, Management, and Security", CRC Press, August 17, 2009, ISBN 9781439806807, pp. 147-158, 183-212.

[9] Paper, A.W. http://aws.amazon.com/about-aws/whats-new/2009/06/08/new-aws-security-center-and-security-whitepaper/, published June 2009.

[10] Descher, M., Masser, P., & Feilhauer, T., A Min Tjoa, David Huemer (2009), " Retaining Data Control to the Client Infrastructure Clouds", published on the IEEE, 2009 International Conference on Availability, Reliability, and Security, pp. 9-15.

[11] Bernstein, D., Ludvigson, E., Sankar, K., Diamond, S., & Morrow, M (2009). "Blueprint for the Intercloud – Protocols and Formats for Cloud Computing Interoperability, submitted to IEEE, 2009 Fourth International Conference on Internet and Web Applications and Services, pp. 328-335. https://doi.org/10.1109/ICIW.2009.55

[12] Zhang, L.-J., & Zhou, Q (2009). "CCOA: Cloud Computing Open Architecture", published on IEEE, 2009 IEEE International Conference on Web Services, pp. 607-615.

[13] Paper, A. W. "Introduction to Amazon Virtual Private Cloud", Available: http://aws.amazon.com/about-aws/whats-new/2009/08/26/introducing-amazon-virtual-private-cloud/, published Aug 26, 2009, pp. 6-8.

[14] Rajkumar Buyya, Chee Shin Yeo, Srikumar Venugopal, "Market-Oriented Cloud Computing: Vision, Hype, and Reality for Delivering IT Services as Computing Utilities", grid Computing and Distributed Systems and Software Engineering, The University of Melbourne, Australia. https://doi.org/10.1109/HPCC.2008.172

[15] Varia, J (2008). Amazon Web Services, "Building GrepTheWeb in the Cloud, Part 1: Cloud Architectures", Available: http://developer.amazonwebservices.com/connect, July 2008, pp. 1-7.

[16] Brodkin, J. " Gartner: Seven Cloud-Computing Security Risks", Available: http://www.infoworld.com, published July 2008, pp. 1-3.

[17] IBM CIO White Paper, " Staying aloft in tough times", April 2009, pp. 3-19.

[18] Steve Hanna, Juniper Networks, "Cloud Computing: Finding the Silver Lining", published 2009, pp. 2-30.

[19] Manifesto, "Open Cloud Manifesto, Dedicated to the belief that the cloud should be open", Available: www.opencloudmanifesto.org, published Spring 2009, pp-1-7.

[20] Peter Fingar, " Dot. Cloud: the 21st-century business platform built on cloud computing", First edition, Meghan-Kiffer Press, February 18, 2009, ISBN 9780929652498, pp. 81-99.

[21] William Stallings, "Network Security essentials", Third Edition, Prentice-Hall, July 29, 2006, ISBN 9780132380331, pp-2.

[22] En.wikipedia.org. n.d. Network security - Wikipedia. [online] Available at: <https://en.wikipedia.org/wiki/Network_security> [Accessed 20 February 2022].

[23] Scribd. n.d. Security Challenges in Cloud Computing | PDF | Cloud Computing | Transport Layer Security. [online] Available at: <https://www.scribd.com/document/552039906/Security-Challenges-in-Cloud-Computing-6> [Accessed 20 February 2022].

[24] Douglas K Barry, D., n.d. Project Gutenberg Self-Publishing - eBooks | Read eBooks online | Free eBooks. [online] Self.gutenberg.org. Available at: <http://self.gutenberg.org/articles/Distributed_Management_Task_Force?View=embedded%27%27> [Accessed 20 February 2022].

[25] Itu.int. 2010. [online] Available at: <https://www.itu.int/dms_pub/itu-t/oth/49/01/T49010000020002PDFE.pdf> [Accessed 20 February 2022].