Sri Lanka Institute of Information Technology

Cloud Security

Individual Assignment

IE2022 - Introduction to Cyber Security

Submitted by:

Student register Number	Name
IT21175602	H.A.N.Nilakshana

Table of Contents

Abstract

The world of computation has evolved over the past three decades from centralized (client-server, not web-based) to distributed systems, and we are now returning to the virtualization of centralization (Cloud Computing). In the world of computation, the location of data and processes is crucial. On the one hand, a user has total control over the data and programs running on his or her computer. On the other hand, cloud computing prevents clients or customers from knowing where operations are being carried out or where data is being stored by having service and data maintenance provided by a vendor. Therefore, the client logically has no influence over it. The internet is the communication medium for cloud computing. When it comes to cloud computing data security, the vendor must offer some guarantee through service level agreements (SLA) to persuade the client on security issues.

When using the cloud as a service infrastructure, organizations take a close look at the security and confidentiality concerns for their mission-critical and non-sensitive applications. However, because the "cloud" offers a variety of services, including Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service, ensuring the security of corporate data there is challenging, if not impossible (IaaS). Every service has unique security concerns. To help the client understand the security policies being applied, the SLA must specify several levels of security and their complexity based on the services. Regardless of the suppliers, the SLA preparation process must be uniform. This may encourage some businesses to use cloud services in the future. In this paper, we present a few security-related requirements for SLA.

Introduction

A concept for quick, on-demand network access to a shared network is cloud computing. A pool of reconfigurable computer resources, such as networks, servers, storage, software, and services, is available. It can be simply provided and published with little administration work or service provider participation. There will be a paradigm shift in information technology that many of us will experience. The notion of capital in computing as well as how computation is done may have undergone significant change because of recent advancements in the field. In a cloud computing network, the services are typically in someone else's building or network and are accessible remotely by cloud users [1].

- Transmission of confidential personal data to the cloud server,
- Transmission of data from the cloud server to the computers of the clients
- Storage of personal data of clients on cloud serversthat are remote servers not operated by clients.

Due to the extreme vulnerability of the first two of the three cloud computing phases to security breaches, research and analysis on the security aspects of cloud computing are essential. The fundamental idea behind cloud storage has changed over time, but it has remained the same: customers borrow infrastructure or services that are kept elsewhere and under someone else's ownership for the duration of their use . [1]Confidential data kept on external cloud servers may also need to be taken into account in some situations. Activities involving secure programming have prioritized safety. Given that any unauthorized party is capable of "snaking" on any private device using a variety of "hacking" techniques, the extension of the scope for accessing someone's personal data via cloud storage actually raises more security concerns.

Due to its existence and culture, cloud computing is unlikely to stop this rising breadth. As a result, maintaining stability has never been easy for cloud storage operations. It's crucial to assess and comprehend state-of-the-art cloud computing security as a vital activity because reliable

security and secure computing technology are ongoing endeavors. The private cloud, group cloud, hybrid cloud, and public cloud are the four main categories of cloud. [2].

The discussion in this paper only makes one cloud-type assumption. Given that this assertion matches all the characteristics of another sort of cloud, there is a public cloud. The cloud storage solution is not just another facility but the fifth utility to follow the current water, gas, and telecommunication services because of its diverse capabilities. The research covered in this article is organized with an eye on defining and examining the answer to the issues with cloud storage, security issues, and other issues that must be considered in this study. deployment on a platform powered by the cloud. The discussion of this article considered the significance of security in cloud computing, security concerns, and cloud security threats, including architectural illustration, cloud security attacks, solutions, and critical examination of existing solutions.

Cloud security Evaluation

First generation

The Early Adopters

The infrastructure for cloud computing is driven by APIs. Anyone with programming or application development knowledge can now write the code that processes information requests. You can cycle through the metadata, for instance, to identify the secure and insecure configuration.

Second generation

The Enlightened

Despite the robust network security in the cloud and the implementation of secure configuration at the cloud management layer, some people started to understand that additional analysis was required at the API layer during this time. analyzing API logs while monitoring and reporting cloud activity in little depth. Machine learning-enabled platforms have started warning cloud clients about irregularities in their surroundings. This has assisted cloud clients in realizing the need to prioritize the security of their cloud platforms in addition to the security of their workloads and networks.

The introduction of a new serverless architecture also made a significant difference for people accustomed to ticking antivirus box after antivirus box. IDS, IPS, and common server hardening are all used. This second-generation cloud security platform was developed. because the API was logging even in a serverless context. This indicated that it was utilized in settings that only made use of cloud PaaS services. Activities in the cloud environment could still be recorded and examined.

Third Generation

Cloud Everywhere

Today, in the future... Infrastructure solution management, containers, serverless, infrastructure-as-code, platform-as-a-service, etc. The newest craze, DevSecOps, automates the entire pipeline from development to infrastructure and operations, with security at its center. Today, the operations teams can write infrastructure code to create their virtual private clouds, while the development teams are familiar with building and deploying, and firewall administrators are learning how to manage their conventional appliances within the CI/CD process.

The effectiveness of third-party solutions vs native cloud services is still up for debate despite the discipline of cloud security's increasing maturity. There are now mature and affordable cloud native security services; third-party cloud security platforms with new features and capabilities; and classic security solutions that provide first-class support for the public cloud.

What is the cloud security

From mainframes to servers, clouds, and Internet virtualization, the world of information technology has advanced. Cloud computing is a centralized, on-demand, configurable IT service (e.g., compute, networking, applications, storage, and information) that is metered (on a pay-as-you-go or subscription basis, over a networked system, and multitasking service) basis, requires little maintenance work, focuses on service level agreements between service providers and customers, and is used primarily by service providers and customers. This also manifests itself in the form of web-based applications or tools that users may access and utilize in the same way as software that is locally installed on their computer [3]. Applications (software as a service), hardware (infrastructure as a service), on-demand hardware, licensed software, and tools can all be provided by cloud computing.

Licensed software and tools, on-demand hardware, applications (software as a service), hardware (infrastructure as a service), or technological tools can all be provided through cloud computing (platform-as-a-service). Most of the time, the service level agreement (SLA) between the service provider and the client specifies the type and quality of performance for cloud storage [4].

Cloud role players

In conventional IT environments, applications and other IT resources are handled internally. Applications, IT platforms, storage, and other resources are made available through cloud computing and are in the cloud somewhere on the Internet. A third-party provider offers services while concealing from the end user the complexity of the underlying networks. Hardware and software designs that enable infrastructure virtualization and scalability are the building blocks of cloud computing. Additionally, cloud services (intermediary services) provided by cloud service providers (vendors, third parties, or brokers) to cloud customers (businesses, IT employees, or end users) across networked networks are included in the cloud computing architecture (i.e., virtual private networks or the Internet). These cloud storage services include contractual provisions (SLAs) that outline client requirements and the vendor's duty to meet them. [5]

Architectural Framework

Utilizing a variety of technologies, cloud computing offers customers effective services. This section presents the cloud computing architecture framework, which is displayed in Figure 1. The architecture and fundamental idea of cloud computing must be understood in order to comprehend the security concerns associated with it. In the majority of literary works, authors use the National Institute of Standards and Technology's definition of cloud architecture (NIST). The organization's definition of cloud computing is commonly used to explain cloud computing in detail. These cloud models, according to NIST, include four (4) distribution models, three (3) cloud models,

and five (5) fundamental characteristics.

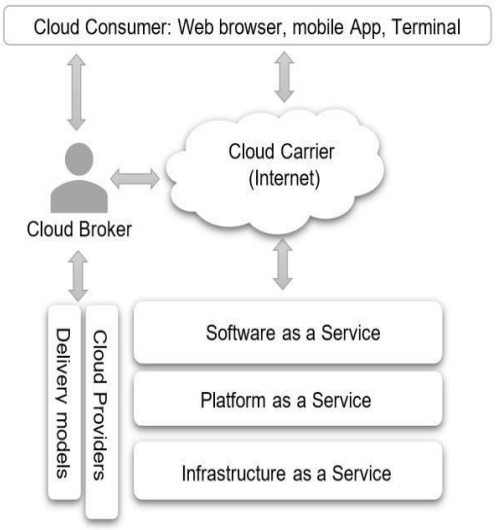


Figure 1 Architectural framework of Cloud Computing (Driesen &Eberlein, 2012)

Essential Characteristics

The five main characteristics of cloud computing provided by NIST includes.

I. On- demand self service

Consumers can directly manage access and services via web services and management interfaces as needed. This is possible without interacting with service providers directly. [6]

II. Broad network access

It is necessary for cloud capabilities, data, and services to be accessible through standard protocols that enable the usage of heterogeneous systems for thin or thick client platforms. Workstations, smartphones, laptops, and other devices all operate using common protocols, and the cloud is designed to support such protocols.

III. Resources Pooling

Large physical and virtual computer resources are offered by cloud service providers, who pool and distribute them across many users. In a multi-tenant context, these resources are typically dynamically assigned based on consumer requests. [6]

IV. Rapid elasticity

The cloud's ability to be elastic allows for the elastic provisioning and release of capabilities, data, and services. These capabilities may be quickly scaled to meet customer requests in any quantity and at any time.

V. Measured service

Utilizing the metering capabilities of the cloud system, services can be automatically optimized and tracked in accordance with client needs. The utilization of resources can then be monitored and reported to the provider and the customer. where the customers are billed on a pay-as-pay-use basis. [6]

Service models

"SPI MODEL" is a commonly accepted framework for defining cloud computing service model. The acronym "SPI" reflects the three cloud-based service models: software-As a Service (SaaS), Platform-as-a-Service (PaaS), and Infrastructure-as-a-Service (IaaS):

I. Softwre as a service(SaaS)

The capacity of a third-party provider to let users use their program to transmit data to distant storage on cloud infrastructure is known as software as a service (SaaS) [7]. Through a thin interface, such as a browser or a programmatic interface, programs can be accessible from a variety of client devices. Customers of SaaS can generally access it whenever they want. Well-known SaaS examples include Google Docs, Salesforce, and Oracle CRM.

II. Platform-as-a-service (PaaS):

platform-oriented model (PaaS) with a more advanced programmable platform [8]. Customers are given the option to create and deploy applications on the cloud infrastructure. The platform offers remote application development tools like libraries, APIs, programming models, and IDEs. Examples of PaaS with an expandable environment include RedHat OpenShift, Windows Azure, and Google App Engine.

III. Infrastructure-as-a-service (IaaS):

IaaS offers users the fundamental computing resources they need to install and operate any software, including operating systems and apps. It provides basic storage, infrastructure that is virtualized, and various abstract hardware and operating systems that may be controlled via a service API. [9] Amazon Web Service, Microsoft System Center, and VMware vCloud Suite are a few examples of IaaS solutions.

Deployment models

There are four main models through which cloud services can be deployed, regardless of the service model chosen.

I. Private cloud

One organization, or external auditing, controls and manages the private cloud internally (TPA). A highly virtualized data center housed inside the clients' firewall makes up the private cloud model. It has special workloads that provide an environment that is well-managed, makes good use of computer resources, is safe, and complies with regulations. [10]

II. Community cloud

Here, several enterprises must work together to share a single cloud infrastructure with a specific group that has a shared interest. Interest could be expressed in terms of needs, services, security measures, or applications.

III. Public cloud

The public can use public clouds for free. It might be a mix of a business, academic, or governmental organization that owns, controls, and runs it. It is located at the location of the cloud provider.

IV. Hybrid cloud

This cloud infrastructure combines two or more different cloud models. Although these infrastructures are still distinctive, they are connected by standardized or proprietary technology that permits the portability of data and applications.

Cloud roles and boundaries

There are many established roles in the cloud. Five primary roles, commonly referred to as actors, are defined by the NIST cloud computing architecture. The processes or activities in the cloud infrastructure are engaged in by these players (entities or organizations). Each actor's roles are described in this section.

I. Cloud provider

A purveyor of cloud resources is another name for a cloud provider. Making and ensuring that cloud services are accessible to consumers is the primary duty of the cloud provider. [11]

II. Cloud consumer

The entity or business known as a "cloud consumer" makes use of and consumes cloud resources made available by cloud providers. [11]

III. Cloud broker

A cloud broker acts as an intermediary between the customer and the cloud provider. As the cloud architecture develops, the integration of resources may become too challenging for a customer to manage alone. The broker can help a customer implement their desired services in place of a cloud provider [11].

IV. Cloud carrier

The cloud carrier serves as a channel for communication and is in charge of transferring data between all parties. In cloud computing, the HTTP protocol is used as the vehicle to send information to and among multiple entities across the internet. [11]

V. Cloud auditor

A cloud auditor is a third-party organization that conducts an impartial assessment of all cloud procedures, safeguards, capabilities, and security risks with the goal of providing feedback. [11]

Cloud Computing Security

Security Issues in cloud computing

Like traditional outsourcing agreements, third party controls and assurance are used in part to achieve cloud security. However, there are extra issues connected to this since there is no global standard for cloud computing security. Cloud services frequently use their own proprietary encryption and communication technology, as well as a variety of security models that must each be evaluated on their own merits. In the manufacturer's cloud paradigm, it is up to the adoption of client organizations to guarantee that cloud security complies with their own security standards by requesting supplier requirements. Risk assessment, due diligence, and assurance procedures. [12]

As a result, the security issues presented by firms looking to use cloud platforms aren't really any different from those faced by those relying on their own internally managed businesses. The same internal and external hazards are present and call for risk management or risk acceptance. The information management concerns that businesses will need to consider are covered in the sections that follow, whether through vendor insurance, public cloud services, or more particularly, the development and implementation of security measures in a privately owned cloud. The following issues are specifically examined:

• Information attribute protection in a cloud computing environment.

• Types of attackers and how they can use the cloud as a target.

• The cloud's vulnerability to threats, as well as any related attack and defense considerations

Security Issues Faced by Cloud Computing

Reaching the beating force of computation is made simple by the cloud. They have a separate physical world. It causes numerous security problems. The cloud service provider promises that the consumer will not experience any problems like data theft or leaks. Emerging technologies and infrastructure, the majority of which have not been thoroughly vetted for security, are used in cloud storage architecture. Numerous users who share the tainted cloud are consequently impacted. Below is a discussion of the security issues that cloud computing is experiencing.

• Data Access Control:

Personal information is frequently obtained incorrectly when safe data access controls are absent. Significant security risks in a cloud-based framework are arising for critical data in a storage environment. [2]

• Integrity of data

This term refers to situations in which human errors occur during data entry. Data transfers from one device to another may encounter errors, or hardware issues like disk crashes may result in errors. [2]

•Data loss:

This is a significant issue with cloud computing. Unknown parties may have access to shared knowledge if corporate transfers, research, and development concepts are all conducted online. [2]

•Administrative Access to Servers:

For cloud service models to work, consumer access to computing resources is essential. In data centers, only on-site connections are allowed to access servers with higher privileges. However, cloud computing makes the infrastructure more vulnerable to attack because access to servers with enhanced privileges is done online. Therefore, it is essential to limit access with elevated privileges and to maintain an access record effectively for tracking system control changes. [2]

• Privacy Issues

For cloud computing, user secrecy is essential. The supplier can ensure that they are effectively shielded from other operations since many servers are external. [2]

•Data Theft:

To operate, cloud storage makes use of an online, scalable, and cost-effective data server. [2]

•User-level Issues:

Users can ensure that other users of the same cloud are not tampering with or missing data because of their ownactions.

• Security issues in Provider level:

The provider may permit a high level of security between the user and the consumer. It should make sure the server is adequately safeguarded against any risks it might encounter.

Cloud Security Threats

Threats in the context of computer security are situations that negatively affect a system's functionality. The top hazards to cloud computing, according to the 2020 cloud security study, are improper configuration of the cloud platform, unauthorized access, and an unsecure interface or API. Other dangers include account theft, disclosure of external data, and malicious insiders. [13]

I. Side Channel attacker

For cloud delivery models that leverage virtualization technology, the potential for side channel attacks, which ultimately leak data across several virtual machines in the same datacenter, is a major concern. As a result, hackers can breach the data of other customers while operating within a shared cloud architecture**.** (Zhang et. Al, 2016) [14]

II. Misconfiguration of cloud platforms

According to the AWS 2020 Cloud Security Report, the biggest hazard to cloud computing and a major contributor to data breaches is incorrect configuration of cloud platforms. Customers use the cloud to outsource their software and data with the knowledge that their assets are secure there. The security of the system can be compromised by a little setup error, leaving the cloud resources open to intrusion. As a result, configurations must be in place and in accordance with security policies. [1]

III. Unauthorized Access

Unauthorized access is a complicated threat that must be managed. An intruder could gain direct access through poor access control or malicious use of staff credentials, possibly without the organization's awareness. Inadequate access control occurs when the right measures are not taken to prevent unwanted access to the cloud infrastructure. Employees log onto the cloud infrastructure from a variety of devices, such as home PCs and mobile phones, and may reuse passwords for both work and personal accounts or share passwords with coworkers to access accounts. This misuse of credentials is caused by employee ignorance. As a result of all this, the device is now exposed to outside dangers. [1]

IV. Insecure interfaces/API

Cloud service providers offer customers a collection of software interfaces and APIs for interacting with and accessing cloud services. These interfaces offer management, monitoring, and provisioning of the cloud services. As a result, the security of these essential services is what determines the availability and security of general cloud services [1] However, these interfaces must be set up to defend against both innocent and intentional attempts to undermine the security of these APIs. Weak interfaces and APIs can put customers at risk of a range of security risks, including the disclosure of confidential information, anonymous access, limited monitoring, changing application configuration settings, etc.

V. Hijacking of Accounts

Utilizing stolen client login information, account or service hijacking is done in order to access cloud services. Phishing or software vulnerability manipulation can be used to carry this out. In some circumstances, the reuse of credentials frequently aids in such assaults. With the stolen login information, the attackers can access private areas of cloud services, jeopardizing their security, integrity, and availability. [4]

VI. External Data-Sharing

The exchange of data is now a crucial process for practically all organizations. The cloud technology was created to greatly simplify data sharing. With the cloud, inviting collaborators is simple via emails or a shared URL that anyone with the URL may use to access and modify the shared resource. Although this convenient data sharing is viewed as a benefit, the link could be leaked, stolen, or just assumed, giving unauthorized users access to the resources. This can compromise the shared resources' integrity and confidentiality [4]Additionally, access to the recipient cannot be reversed once this connection has been shared.

VII. Malicious Insider

This issue raises serious security concerns and is difficult to defend against. It involves an insider who can quickly gain access to a system's crucial resources or have higher-level management over cloud services with little to no chance of being discovered. A malevolent insider's actions have an adverse influence on the availability, confidentiality, and integrity of information as well as on internal operations, brand reputation, and customer trust. [4]

Cloud Security Attacks

I. Denial of service attacks

DoS attacks occur when an attacker makes many requests to use up all the server's resources and render it unavailable. The request packet squanders performance time, capacity, and cryptographic processes. This has an impact on the behavior and availability of clouds [15]. A distributed DoS assault is significantly more difficult to detect and more complicated than a DoS attack.

II. Man-in-the -Middle attacks

A "man in the middle attack" occurs when a malicious actor deceitfully intervenes between two communicating parties to access the information being shared or, conceivably, to change the data being transmitted and received without either party's knowledge [16].This attack is only viable if the communication channels are not protected or if Secure Socket Layer (SSL) security configurations are not present. [16]

III. Phishing Attacks

A social engineering tactic known as phishing uses a disguised email as a weapon. When an attacker uses a link or attachment to pose as a trustworthy entity, it raises suspicion and creates a sense of urgency [2].When a person clicks on the link, they are unknowingly sent to a bogus website and asked for their login information. The attacker can access it when the user submits their credentials.

Existing Security Solution

- **Intrusion Detection and Prevention**

To stop attacks like zero-day attacks, intrusion detection systems (IDS) and intrusion prevention systems (IPS) monitor enterprise applications and operating system vulnerabilities until a patch or upgrade is made available. Cloud servers and virtual machines frequently employ the same system software, application software, and physical infrastructure. However, the installation of software-based IDS and IPS on virtual machines provides security against vulnerabilities [10].

- **Firewall**

In a typical cloud context, a firewall can be used to minimize the attack surface of virtual machines. On VMs, a two-way firewall or bidirectional firewall with integrated firewall policy administration is installed. However, the following templates must be enabled and included in the firewallpolicy:

1.To separate VMs

2. Finer granularity filtering

3. Compatibility with all IP-based protocols and frame types

4. The power to design rules for any network interface

- **Log Inspection**

Log inspection and analysis for security-related events in operating system and application logs Security event detection can be improved by using Log Inspection Rules, which typically find events that are lost in many log entries [10]. Maximum visibility of received events is guaranteed by a Security Information and Event Management (SIEM) system. However, the following is possible using cloud-based log examination software:

1. A list of security-related activities.

2. The discovery of ominous activities

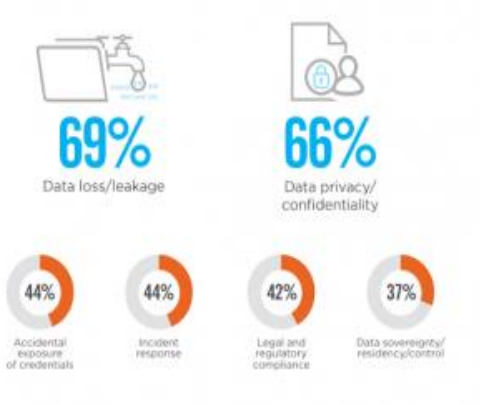
3. A compilation of security-related server farm occurrences

Cloud Security Trends 2022

- **Cloud Security Posture Management (CSPM)**

The highest-ranked cloud dangers, according to research, are misconfiguration, lack of visibility, identification, and illegal access. Cloud Security Position Source. Your cloud platform accounts' configuration is examined by management, or CSPM, who searches for any potential configuration errors that could result in data leaks and breaches. The cloud environment is dramatically growing, making it more challenging to identify misconfiguration. According to Gartner, misconfiguration is the main cause of data breaches. Better functioning would result from reduced or complete eradication. CSPM assists companies in fostering user confidence in terms of safety and security. It automates security and offers cloud-based compliance assurance.

Here is how CSPM proves to be effective for businesses:



- Easy detection and remediation of cloud misconfigurations
- Inventory of best practices of varied cloud configuration

- **Lack of consensus**

Businesses have difficulties as a result of global differences in rules and diversity in approaches to pressing concerns. Users put a lot of effort into making sure they obtain adequate security. Businesses must devote time and effort to ensuring that rigorous compliance with established rules is maintained in light of the rise in cybercrime.

- **A drastic increase in cybercrimes**

With cloud computing, information is always available. However, the risk that results is the responsibility of the users who are connected to the resources. Due to a lack of visibility and control, cloud computing significantly increases the risk of cybercrime. People are not fully aware of the dangers involved.

The three types of data in cloud computing exposed to the risk of cybercrime are:

- Data processed in the cloud
- The idle or resting data
- The data in transit

Companies cannot operate without end-to-end encryption due to the heightened danger of cybercrime. Only one in five businesses periodically evaluates their cloud security posture while being aware of the serious concerns. To prevent serious losses for your company, make sure you don't fall behind in this area.

- **The need for centralized platform**

With cloud computing, information is always available. However, the risk that results is the responsibility of the users who are connected to the resources. Due to a lack of visibility and control, cloud computing significantly increases the risk of cybercrime. Companies cannot operate without end-to-end encryption due to the heightened danger of cybercrime. Only one in five businesses periodically evaluates their cloud security posture while being aware of the serious concerns. To prevent serious losses for your company, make sure you don't fall behind in this area.

- **Summing up**

We are aware that organizations face new, sophisticated cyber threats every day. Following analysis of the tendencies, businesses must be ready for the worst. To preserve their integrity and establish enduring relationships with their clients, it is imperative that they implement robust security measures. To shield your company from serious attacks, continue to monitor and work on security issues.

Future developments in Cloud security

First off, a high level of assurance in ownership and accountability will be restored thanks in large part to blockchain technology. Smart contracts based on the blockchain, for instance, can be used to control your interactions with various cloud service providers. It's written into the smart contract that if there's a problem or a downtime, an SLA exception will automatically credit you. There may be a predetermined commercial relationship. It looks at the fundamental link and the obligations associated with your significant infrastructure, not only for cryptocurrencies. Together, the cloud and blockchain will enable proper cyber security and the return of control to people and organizations who desire it.

The second factor that will be crucial to cloud security is privacy. The EU is leading the world in implementing privacy laws, which ought to be at the forefront of our culture. For every piece of PII or proprietary information, for instance, we must apply encryption properly. For enterprises to adopt encryption and data security efficiently, it is necessary to understand encryption overhead, key management, and all the various locations of data with the layered paradigm of cloud computing.

Third, quantum computing will be the next major development that will fundamentally alter cloud security as well as all our present encryption techniques. On April 14, 2030, according to the Cloud Security Alliance (CSA), a quantum computer will be able to compromise the current cyber security system. Quantum attacks can be employed against any current algorithm utilized for the global public key infrastructure. Organizations will need to embrace quantum-resistant encryption in a post-quantum world by using public key algorithms that are impervious to quantum computing assaults. [17]

Within the last ten years, cloud computing has grown dramatically, with important breakthroughs and advances being widely used in a variety of industries due to its more useful service and ease. Adopting cloud solutions within their organizations has advantages for enterprises. However, even though cloud security is an essential component of computer security, its widespread acceptance, and the fact that it relies on an internet connection make it subject to many security risks. This study reviews the major risks to cloud security in detail. As advice, countermeasures and threat mitigation techniques are also provided. Like this, reducing the risks related to the adoption of cloud computing depends on understanding the problems with cloud security and practical solutions.

References

[1] 2. Chaturvedi & Gupta, 2020.

[2] A. a. G. R. 2. Mondal, "ENHANCED HONEYPOT CRYPTOGRAPHIC SCHEME AND PRIVACY PRESERVATION FOR AN EFFECTIVE PREDICTION IN CLOUD SECURITY," 2020.

[3] S. A. A. M. S. a. S. H. 2. Abdul-Jabbar, " Integrity and Security in Cloud Computing Environment: A Review," 2020.

[4] T. 2. Alam, " Cloud Computing and its role in the Information Technology," 2020.

[5] A. 2. Sunyaev, "Cloud Computing. In Internet Computing," 2020.

[6] C. B. R. M. M. D. A. S. B. B. P. O. V. R. A. C. T. L. 17. Lee, "2020 The NIST cloud Federation Referance Architecture," 2020.

[7] M. I. M. S. A. J. R. H. M. L. R. L. R. L. N. M. A. W. Y. a. S. R. 12. Herman, " 2020. NIST Cloud Computing Forensic Science Challenges," 2020.

[8] M. 2. Kavis, "Architecting the cloud: design decisions for cloud computing service models (SaaS, PaaS, and IaaS).," John Wiley & Sons, 2014.

[9] D. Velev and P. Zlateva, " "Cloud Infrastructure Security", Lecture Notes in Computer Science, 1.," 2011.

[10] P. G. A. a. L. R. Negi, " 2020, January. Intrusion Detection and Prevention using Honeypot Network for Cloud Security," . In 2020 10th International Conference on Cloud Computing, Data Science & Engineering. IEEE., 2020.

[11] M. C. P. G. R. a. T. M. Birje, "Cloud computing review: concepts, technology, challenges, and security. International Journal of Cloud Computing," 2017.

[12] Singh and K. Chatterjee, " "Cloud security issues and challenges: A survey", Journal of Network and Computer Applications,," 2017.

[13] R. a. J. M. Gautam, " Cloud Computing Security: Aws Data Security Credentials," 2020..

[14] D. J. T. a. W. S. 28. Zhang, "Brief Talk on Cloud Computing Technology.," *International Journal of Social Science and Education Research*, 2020.

[15] R. Mittal, "Analysis of DDoS Attacks in Cloud. In 2020 International Conference on Smart Technologies in Computing,," 2020.

[16] L. Jansen, "Comparing cloud security directions between the academia and the Industry, A survey.".

[17] https://www.cybertalk.org/2022/07/05/the-future-of-cloud-security-2022-and-beyond/, "https://www.cybertalk.org/2022/07/05/the-future-of-cloud-security-2022-and-beyond/".

[18] K. C. A Singh, "Cloud security issues and challenges: A survey," india, 2017.