Cloud Computing Security for Multi-Cloud Service Providers: Controls and Techniques

[1]**Ayush Dewangan**, [2]**Mr. G Raghavendra Prashad**

Amity University Chhattisgarh
Amity Institute of Information Technology
Amity University, Raipur, India

***Abstract*- In order to provide instantly accessible computer resources and services, cloud computing, a distributed architecture that centralizes server resources on a very scalable platform, is used. The various cloud deployment models, the top security risks and issues that are now plaguing the cloud computing industry. Any business that wants to secure its apps and data from malicious users must priorities security in cloud computing. Your data and apps are accessible to authorized users thanks to cloud security. Cloud Computing security is three different models: private. Public hybrid. Cloud service providers need to educate potential customers about cloud deployment models such as public, private and hybrid. One of the biggest security worries with the cloud computing model is the sharing of resources (multitenancy). Cloud service proactively informs their existing customers of the level of security that they provide on the cloud. The cloud computing system transfers work now carried out in individual computers and private data centers to a bigger computing facility that is accessible to all users and dispersed throughout the internet. One or more hosts may provide services to a virtual server, and a single host may contain many virtual servers.**

***Key words* - Cloud security challenges, cloud security models, Architecture, Storage security.**

I. INTRODUCTION

1. Cloud computing allows for the metered usage of computer and storage resources, which lowers an organization's investment in its computing infrastructure.(Singh, 2018). Instead than being a new technology, cloud computing is a new way to distribute information and services utilizing already existing technologies. It enables communication between client-side and server-side services and applications by utilizing the internet infrastructure. (Weiss, 2007). Up until 2008, the Internet was symbolized on network diagrams by a cloud, but this was before a number of new services began to appear that made it possible to access computer resources through the Internet, which came to be known as cloud computing.(de Bruin & Floridi, 2017) Social networking and other types of interpersonal computing are included in cloud computing; nevertheless, most of the time, cloud computing is focused on accessing internet software programmes, data storage, and processing capacity.(Liu, 2012)

2. Recent studies have found that disciplined companies achieved on average an 18% reduction in their IT budget from cloud computing and a 16% reduction in data centre power costs. (McFedries, 2008) Cloud computing market sales were estimated by Gartner to be USD 58.6 billion in 2009, USD 68 billion in 2010, and USD 148 billion by 2014. These profits suggest that cloud computing is a potentially successful technology. On the other side, it makes attackers more motivated to identify any model flaws that already exist.(Al Morsy et al., 2010). Despite the potential benefits and revenues that could be gained from the cloud computing model, the model still has a lot of open issues that impact the model creditability and pervasiveness.(Zissis & Lekkas, 2012)

3.Cloud computing security challenges and issues discussed by various researchers. The Cloud Computing Use Cases group discusses the different use case scenarios and related requirements that may exist in the cloud computing model.(Sengupta, 2011) They take into account use cases from several angles, including those of consumers, developers, and security engineers. ENISA looked at the many security concerns associated with adopting cloud computing, as well as the assets impacted, the risks' possibility, impacts, and cloud computing's flaws that may cause such risks.(Barron et al., 2013).

4. In a manner comparable to utility-based systems like electricity, water, and sewage, they can provide a central pool of reconfigurable computing resources and computing outsourcing methods that permit diverse computing services to different persons.(Wang et al., 2010) In electricity, for example, people started to connect with central grids, supported by power utilities rather than relying on their own electricity production capabilities. This migration is beneficial in reducing the cost and time of production and in providing better performance and reliability.(Ryan, 2013) Similar to this, clouds provide their clients more affordable high performance and more dependable computer services including email, instant messaging, and online services. Clouds provide several advantages for both consumers and businesses. Clouds enable cost reductions, resource sharing, outsourcing techniques, accessibility from anywhere at any time, on-demand scalability, and service flexibility. By hiding technical information from its clients, such as software upgrades, licensing, and maintenance, clouds reduce the requirement for user interaction.(Al Morsy et al., 2010)

5.To successfully address the cloud security issues, we need to understand the compound security challenges in a holistic way. Specifically, we need to: (i) investigate various cloud security attributes including vulnerabilities, threats, risks, and attack models; (ii) identify the security requirements including confidentiality, integrity, availability, transparency, etc.; (iii) identify the involved parties (clients, service provides, outsiders, insiders) and the role of each party in the attack-defense cycle; and (iv) understand the impact of security on various cloud deployment models (public, community, private, hybrid).(Shaukat et al., n.d.)(The main contribution of this paper is that it provides a holistic study of the security issues in the clouds that cover almost all the cloud components (data centers, computing infrastructure, interfacing and networking, etc.), network layers (application, transportation,

IP, etc.), and cloud stakeholders (providers, consumers, third party contractors, etc.).(Beri, 2015) As needed, cloud resources are made available as a service. Large numbers of commodity-grade servers are frequently used in the cloud itself to provide extremely scalable and dependable on-demand services. Users are given more resources in the cloud system when they require them and fewer resources when they do not.(Fundamentals et al., n.d.)
6.In cloud computing, a large number of computers that are dispersed throughout the internet are used for data storage and computation instead of local computers and servers. The cloud computing system transfers work now carried out in individual computers and private data centers to a bigger computing facility that is accessible to all users and dispersed throughout the internet. One or more hosts may provide services to a virtual server, and a single host may contain many virtual servers.(Alzain et al., 2012) If the environment is built correctly, virtual servers will not be affected by the loss of a host. Hosts may be removed and introduced almost at will to accommodate maintenance. The grid computing do not rely on virtualization as much as the cloud computing do and each individual organization maintain full control of their resources. The user need not computing and storage resource and don't provide the application in the cloud computing. (Almorsy et al., 2011) The grid computing want to solve the assignment of computing and resource storage and the cloud computing want to share the computing, storage and application resource. The grid computing do not rely on virtualization as much as the cloud computing do and each individual organization maintain full control of their resources.(Almond, 2009) Internal data centers of a company or other entity that are not accessible to the general public are referred to as private clouds. An organization that sells cloud services to the general public or to a major industrial corporation owns the cloud system infrastructures. The security of the public cloud, which operates online, is quite complicated. Virtualized data centers are known as public clouds, and service providers make resources accessible to customers through a public Internet network upon request. (Al Morsy et al., 2010)
7.On the other hand concerns persist about loss of control over certain sensitive data, and the lack of security for stored kernels entrusted to cloud providers. If those providers have not done good jobs securing their own environments, the consumers could be in trouble.(Herrera Perez et al., 1989) Measuring the quality of cloud providers' approach to security is difficult because many cloud providers will not expose their infrastructure to customers.(Chen, 2012) Due to the cloud computing industry's relative youth, there is ambiguity over the level of information security these services provide. Virtualization technology is a key component of infrastructure-as-a-service (IaaS) cloud services since it is thought to offer all the security and process separation a client might need. Virtualization and multi-tenancy offer an effective computing strategy.(Shahzad, 2014)

Literature Review:

The development of how we use computers, known as cloud computing, is currently gaining popularity at a rapid rate because to improvements in internet technology. It is practical in many ways, but mainly because you can access it and save money if you have internet access.(Zissis & Lekkas, 2012) It is difficult to define "the cloud," but in essence it is a computer that is accessible from anywhere with just an internet connection—which is incredibly handy now that everyone owns a smartphone. There are several varieties of cloud services.(Douglas & Sutton, 2010) Email is among the most popular; for example, the files in your inbox are stored on the server of your email provider. For a long time, people would send emails to themselves with the documents they needed attached. Most email providers then offered some space for file uploads, and today there are services like Google Drive that offer more than 10 Gb of free storage space for uploading anything.(Lee & Son, 2017)

Cloud Computing Characteristics and Storage security

Cloud services exhibit five essential characteristics that demonstrate their similarities and differences from traditional computing approaches. (Herrera Perez et al., 1989)

- Resource pooling: The provider's computing resources are pooled to serve multiple consumers using a multitenant model with different physical and virtual resources dynamically assigned and reassigned according to consumer demand.(Mohabbattalab, Elnaz Mohabbattalab, 2014) There is a degree of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or data-center). Examples of resources include storage, processing, memory, network bandwidth, and virtual machines. Even private clouds tend to pool resources between different parts of the same organization. (Singh, 2018)
- Rapid elasticity: In some circumstances, capabilities may be automatically and swiftly supplied to scale out quickly and swiftly released to scale in. The capabilities that are offered for provisioning frequently seem limitless to the user and may be acquired in any amount at any moment.(Alzain et al., 2012)
- Measured service: By utilizing a metering capability at a certain degree of abstraction relevant to the kind of service, cloud systems automatically manage and optimize resource utilisation (e.g., storage, processing, bandwidth, or active user accounts). Resource utilization may be tracked, managed, and reported, ensuring openness for both service providers and customers. (Ryan, 2013)
- On-demand self-service: Without needing to speak to a service provider directly, a customer may autonomously provide computer resources like server time and network storage as needed automatically. (Almorsy et al., 2011)
- Broad network access: In order to encourage usage by diverse thin or thick client platforms (such as mobile phones, laptops, and PDAs) as well as other conventional or cloud-based software applications, capabilities are made available over the network and accessed by normal protocols.(Zissis & Lekkas, 2012)

Storage security - Despite the enormous financial and technological benefits of the cloud, one of the main obstacles blocking its mainstream adoption has been the security and privacy worry. The owners eventually cede to the CSPs total control over their data, especially for outsourced data services 8. For instance, Google's most current privacy statement says that they essentially have the freedom to treat the uploaded user data however they see fit.(Barron et al., 2013) As a result, from the data owners point of view, whenever their outsourced data contain sensitive personal information, such as financial and medical records, and social network profiles, it can no longer be considered as private as before.(Mohabbattalab, Elnaz Mohabbattalab, 2014) On the other hand, despite the fact that CSPs typically enforce data security through tools like firewalls and virtualization, these safeguards do not completely protect against risks of unauthorized data access from insiders, outsiders, or other cloud tenants due to the non-bug-free deployment and low level of transparency. There are occasionally well-known data breach occurrences, such as the recent Sony PlayStation data breach10 and Drop Box privacy leak.(Shahzad, 2014)

One of the most commonly used cloud service is data storage, where end users can outsource any amount of data to cloud servers to enjoy virtually unlimited hardware/software resources and ubiquitous access, with no or little investment.(Zhang et al., 2011) Indeed, many well-known cloud service providers have started providing these services since last few years, including Microsoft SkyDrive 14, Amazon S315, Dropbox16, Apple iCloud, and Google Drive 8. In the cloud, there are following two important characteristics that impose challenges to the development of data protection techniques: (Prakash & Dasgupta, 2016)

- A network of service providers may offer a cloud service. The principal provider, then, makes use of the resources of other providers (the identity to these indirect providers may be unknown to the user). As a result, hackers and data mining are more likely to target the outsourced files.(Yu et al., 2010)
- It's also important to take into account any potential modifications to the cloud service's indirect suppliers. As an illustration, a participating provider could be forced to move its operations and users' data to another party due to a business sale, merger, government seizure, etc.(Barron et al., 2013) This means the user’s files may remain on several inactive hard drives even after user’s request for deletion or close of account.(Hashemi & Bardsiri, 2012)
- In compliance with security best practises, AWS integrates security into its services and provides documentation on how to utilize the security features. Utilizing AWS security capabilities and industry standards is crucial for customers who want to create an environment for their applications that is adequately secure.(Jansen et al., 2011) Ensuring the confidentiality, integrity, and availability of user’s data is of the utmost importance to AWS, as is maintaining their trust and confidence 18. AWS takes the following approaches to secure the cloud infrastructure: (Jansen et al., 2011)

General Security Measures - Certifications and accreditations. AWS has in the past successfully completed multiple SAS70 Type II audits, and now publishes a Service Organization Controls 1 (SOC 1) report, published under both the SSAE 16 and the ISAE 3402 professional standards. In addition, AWS has achieved ISO 27001 certification, and has been successfully.(Ashish Agarwal, 2011) validated as a Level 1 service provider under the Payment Card Industry (PCI) Data Security Standard (DSS). In the realm of public sector certifications, AWS has received authorization from the U.S. General Services Administration to operate at the FISMA Moderate level, and is also the platform for applications with Authorities to Operate (ATOs) under the Defense Information Assurance Certification and Accreditation Program (DIACAP). (Achar, 2022)

Physical security. Large-scale data centers are something that Amazon has designed, built, and operated for many years. The AWS infrastructure is housed in data centres under Amazon's management all over the world. Only those employees of Amazon who need to know the locations of the data centers for proper business purposes have access to this information. To prevent illegal entry, the data centers are physically protected in a number of different methods. (Achar, 2022). Secure services. Every service in the AWS cloud is designed with security in mind. While maintaining the freedom that clients desire, the services have a variety of features that limit illegal access or use.(R B & Tiwari, 2017)

Cloud Software as a Service (SaaS): The possibility to use appliances that are cloud-based is provided by this programmed. These appliances can be obtained by using common interfaces like a web browser or an online (e-mail) client. SaaS appliances may be accessed from a variety of devices, including mobile and workstations, anytime, anyplace. (Upadhyay, 2017)

Cloud Network as a Service (NaaS): NaaS provides the capability to use the network services and inter-cloud network connectivity services. Improvement of possession allocation services include in view of network and computing resources. These type of services involved extensible, enhanced virtual private network.(Che et al., 2011)

Cloud Deployment Models

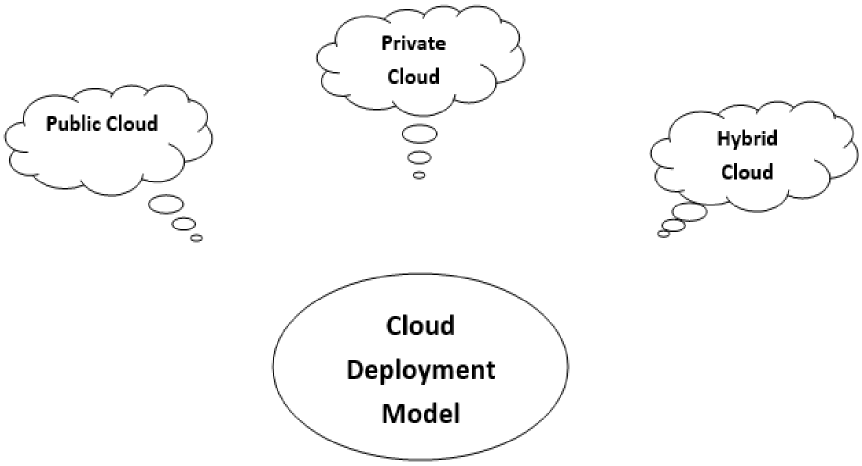

Fig 1. Cloud Deployment models

Based on ownership, scale, and access as well as the nature and function of the cloud, the cloud deployment model determines the particular sort of cloud environment. A cloud deployment model specifies the location of the servers you're using and who owns them.

Public Cloud: The term "public cloud" relates to the classic concept of "cloud computing," which is the availability of effective, easily accessible techniques online from a small party that separates its assets and charges its users on a utility basis. The cloud organization is controlled and run by a provider, and they advocate for its restoration to the public domain. Online cloud services are offered, for instance, by Google, Amazon, and Microsoft.(Lee & Son, 2017)

Private Cloud: The phrase "private cloud" refers to a proprietary computer architecture that is made available as services over business networks. Large businesses typically adopted this sort of cloud computing to enable the administrators of their private networks and information centres to effectively transform themselves into internal "service providers" that cater to consumers within the company. A third party manages a cloud organization for a specific aggregate in accordance with a service level agreement. Only one company opted to use the corporate cloud for operations.(Douglas & Sutton, 2010)

Hybrid Cloud: Enterprises will undoubtedly seek a hybrid cloud that combines resources from private and public suppliers. A hybrid cloud is one that combines both private and public clouds. For instance, a business may decide to use external services for general computing, and its own data centres include its own data centres.(Castro-Leon et al., 2012)

Industrial systems are well-known for using cloud services to offer data exchange and integration services for product traceability. Malicious cloud services, however, make it difficult for businesses to accurately get product traceability. Acids is a trustworthy and rapid auditing schema for large-scale industrial data in an uncertain cloud computing environment, according to a recent research.(Almorsy et al., 2011) Industry participants may serve as product consistency auditors by utilizing this schema. According to testing results compared to earlier procedures, the recommended Acids are successful in data consistency verification of modest volumes of items at a reasonable cost. The proposed Acics schema shows better read or write latency rates. As it has not been tested on large items, this schema can be investigated in subsequent research.(Singh, 2018)

We categories cloud computing (CC) in conjunction with other study fields. Education, Internet of Things, Blockchain, mobile computing, and resilience are some of these areas. Mobile computing is one of these fields that have been extensively researched. However, two survey papers [SP25] and [SP31] on blockchain technology and cloud computing were just released. The earlier survey study is a brief conference paper that omits a thorough examination of how blockchain technology might help resolve security concerns with cloud computing.(Sengupta, 2011). Acids offer a reliable and effective auditing schema for the vast amounts of industrial data in the hazy cloud computing environment. By using this schema, industry players can act as auditors of product consistency. The recommended Acics is effective in data consistency verification of moderate amounts of items at a reasonable cost, according to experimental results compared to past approaches. Lower read or write latency rates are present in the proposed Acics schema.(Almond, 2009).

This schema can be studied in later studies because it hasn't been applied to large things. Previous research has shown that cloud computing poses a serious security risk to its customers' data. Customers move their data to the CSP's storage but fail to check the security measures put in place at the CSP to safeguard their private information. The standards for judging the security measures performed by the CSP Company are established by the Cloud Security Alliance (CSA). A user of cloud services benefits from having faith in CSPs' products. The main problem is that the CSA's questionnaire-based security evaluation cannot verify that the responses are accurate.(Al Morsy et al., 2010). External users, however, have no way to exploit the findings of a third party examination. To further assess the quality of cloud providers' services and boost users' confidence in an organization's cloud services, user feedback is required.(Shahzad, 2014)

Cloud Architecture

Cloud computing has five key attributes which grant it some advantages over similar technologies and these attributes include:(Jansen et al., 2011)

- Multitenancy (shared resources): In contrast to earlier computing models, which presupposed dedicated resources allocated to a single user or owner, cloud computing is built on a business model in which resources are shared at the network, host, and application level.(Alzain et al., 2012)
- Massive scalability: Cloud computing provides the ability to scale to tens of thousands of systems, as well as the ability to massively scale bandwidth and storage space. (Al Morsy et al., 2010)
- Elasticity: Users may quickly raise and reduce the amount of computing resources they have available as needed. They can also release resources when they are no longer needed.(Ryan, 2013)
- Pay as you go: Users pay for only the resources they actually use and for only the time they require them.(Zissis & Lekkas, 2012)
- Self-provisioning of resources: Users self-provision resources, such as additional systems (processing capability, software & storage) and network resources (Mather, Kumaraswamy, & Latif, 2009).

History of Cloud Computing

Older systems that were utilized in real-time long before cloud computing existed can be used to trace the evolution of cloud computing. The term "cloud" refers to a carrier or provider who offers services through the Internet in "cloud computing." The term "computing" refers to the processing of computations, calculations, or other resources made available by computers. "If computers of the sort I have proposed become the computers of the future, then computing may eventually be structured as a public utility much as the telephone system is a public utility," wrote John McCarthy in 1961 at MIT. This is the origin of the term "cloud computing."(Al Morsy et al., 2010)

The computer utility may serve as the foundation for a significant new enterprise. Sales force founded one of the first businesses to deal with the idea of "cloud computing" in the late 1990s. The business began offering its Software as a Service (SaaS), which gives consumers customer relationship management. In addition to "Platform as a Service" (PaaS), which gives users access to development platforms like Microsoft Azure and Google's Application Engine, one of the common patterns of cloud computing is the Salesforce model.(Liu, 2012) The other form is “Infrastructure as a Service” (IaaS) model such as Amazon Elastic Compute Cloud (EC2) started in 2006. In 2007, many of the US universities started collaborating with Google and IBM and promoted cloud computing programs at their universities. This helped reduce the cost for academic research, sharing the resources between the students, and to build substantial processing power or computing power to access it over the Internet.(de Bruin & Floridi, 2017) In the years that followed, a lot of colleges all across the world continued the same pattern. A cooperative initiative between NASA and Rackspace named OpenStack was launched in July 2010 and involves multiple suppliers, including AMD, Intel, and Dell. Later, several other organizations joined the initiative. In September 2012, the Open Stack Foundation was established as a non-profit with the goal of advancing OpenStack. Currently, the project has the support of over 500 businesses. Approximately 6800 businesses use OpenStack to roll out their cloud services. CSA's Trusted Cloud Initiative issued a white paper in October 2011 to assist cloud service providers in creating cloud services that adhere to industry standards and are safe, controllable access, interoperable, and managed.(Wang et al., 2010)

Cloud Application

Cloud computing development is directly or indirectly related to various applications using Cloud Services. (Beri, 2015)

A. Software Development and Testing Cloud computing has a lot of influences from software development and testing over the last couple of years or decades.

Software development: In the development of a cloud computing environment, software technology and software architecture have a lot of influence. Because of various reasons such as: (Herrera Perez et al., 1989)

1) The software or apps created must work with the cloud. Due to the fact that the cloud platform functions in conjunction with a number of factors, including the underlying deployment architecture, storage capacity, and computing platform/processing power.

2) The application should be able to serve a large user base with huge amounts of data without any problems.

3) These services must be provided over the Internet

4) The services are offered online, thus there is a considerable danger of disclosing private information. Higher security is thus required for the application or services. Such that it can withstand assaults and safeguard the users' and organizations’ private information and data.

5) These services should be independent of platforms used by customers. i.e., users can use any device to access these services without any issues. (Al Morsy et al., 2010)

Software development and the working environment have altered significantly compared to conventional software development because of the cloud computing environment. The cloud-based development tools, development platform, development environment, team cooperation, and remote working of diverse group members are largely responsible for these improvements. The cloud has been used to launch their services online, test the services or software, and assess them for the services' appropriate operation. (Al Morsy et al., 2010)

Software testing: With the adoption of a cloud computing environment for software development, software testing has some changes to cope with the new situation. (Liu, 2012)

The use of the cloud computing environment for software development, as stated in section V-A1, has various changes in technology and architecture, thus software testing also has to alter in accordance with these changes. In order to comply with the demands of a cloud computing environment, such as dynamic capabilities, supporting a large number of users, security, and cross-platform compatibility, software testing should adhere to conventional metrics and also adapt the changes.(Beri, 2015)

In the cloud computing environment, many of the things for software development has changed such as tools, environment, and working patterns to meet the present environment. According to these changes software testing tools, environment, and working patterns should also change to meet the cloud.(Herrera Perez et al., 1989)

Cloud storage - A novel addition to cloud computing is cloud storage, which is used to store files on a network. Cloud combines the software programmers and storage space needed for it to operate properly. The core of a cloud computing environment contains processing and computational capacity; when this system is prepared to store or manage massive volumes of data utilizing big storage devices, the cloud computing environment may also be thought of as a cloud storage system. Consequently, the administration of the primary cloud computing environment through a data storage management system.(Aikat et al., 2017)

Cloud Computing and Big Data - The two paradigms of big data and cloud computing are inextricably linked from a technological standpoint, making it impossible to separate them. Big Data makes evident that there is a vast quantity of data that cannot be handled on a single computer but rather requires a sizable system with a lot of processing capacity. Which may either be accomplished utilizing distributed processing, distributed databases, and cloud storage, or, to put it another way, requires the usage of cloud computing. Due to the fact that cloud computing can supply the necessary number of resources for processing Big Data. (Mohabbattalab, Elnaz Mohabbattalab, 2014)

Gaming - The console from the client side will connect to the server through the Internet and interact, getting the data connected to the game in real time. All games in cloud-based gaming are server-side applications. In order to interface with the server and receive data via the Internet, the client side does not require sophisticated video-capable hardware or a lot of computing power. The conversion of cloud-based gaming solutions into actual gaming solutions will be achievable with the deployment of new technologies like 5G mobile networks. Users will save a lot of money if they choose a cloud-based gaming solution because some architecture may not support certain games while moving between them of games. (Zhang et al., 2011)

Internet of Things (IoT) - Kevin Ashton first used the phrase "Internet of Things" (IoT) in 1999. The only items connected to the Internet make up the Internet of Things. The Internet serves as the building block of the Internet of Things, and a wider network of connected devices is dependent on it for information exchange and communication. According to K. Rose et al., "The term Internet of Things refers to situations where network connectivity and computing capability extend to objects, sensors, and commonplace items not typically considered computers, allowing these devices to generate, exchange, and consume data with little to no human intervention."(Yu et al., 2010)

Discussion:

1. What is cloud computing?

- In their presentation, "Effectively and Securely Using the Cloud Computing Paradigm," Peter Mell and Tim Grance from the National Institute of Standards and Technology (NIST) Information Technology Laboratory described cloud computing as follows:
- Cloud computing is a model for easy, on-demand network access to a shared pool of dependable and trustworthy computing resources (such as networks, servers, storage, applications, and services) that can be quickly provisioned and released with little involvement from the customer or the service provider.

2. What is the issue of cloud computing security?

- Illegal data access and data leakage between virtual machines operating on the same server
- Failure of a cloud provider to manage and safeguard sensitive data appropriately.
- Release of sensitive information to law enforcement or the government without the client's consent or awareness.
- The capacity to satisfy legal and regulatory standards.
- System faults and breakdowns that result in prolonged outages of the cloud service.
- Hackers stealing and disseminating sensitive data by hacking into client apps stored in the cloud.
- The strength of the security measures put in place by the cloud provider.
- The level of compatibility present, allowing a customer to migrate apps across multiple cloud providers without difficulty and prevent "lock-in".

3. What is the risk of cloud computing?

The unique cloud environment raises various security and privacy concerns.

- Outsourcing: Users may lose control of their data. Appropriate mechanisms needed to prevent cloud providers from using customer's data in a way that has not been agreed upon in the past.
- Extensibility and Shared Responsibility: There is a trade-off between extensibility and security responsibility for customers in different delivery models.
- Virtualization: There needs to be mechanisms to ensure strong isolation, mediated sharing and communications between virtual machines. This could be done using a flexible access control system to enforce access policies that govern the control and sharing capabilities of VMs within a cloud host.
- Multi-tenancy: Issues like access policies, application deployment, and data access and protection should be taken into account to provide a secure multi-tenant environment.
- Service Level Agreement: The main goal is to build a new layer to create a negotiation mechanism for the contract between providers and consumers of services as well as the monitoring of its fulfillment at run-time.
- Heterogeneity: Different cloud providers may have different approaches to provide security and privacy mechanisms, thus generating integration challenges.

Conclusion:

Security is one of the main concerns with the cloud computing concept (multitenancy). The degree of security offered by cloud service providers needs to be disclosed to their current clients. Cloud service providers must inform prospective clients on the advantages and disadvantages of various cloud deployment methods, including public, private, and hybrid clouds. We are looking at the issue of cloud security management and suggest using an adaptive model-based strategy to tackle the issue. Models will aid in the problem-abstraction process and in the capture of various stakeholders' security needs at various degrees of specificity. The feedback loop will assess the security state in order to assist improve the present cloud security model.

The use of the cloud computing paradigm is steadily expanding. America spent $20 billion on IT migration to cloud computing technologies in 2010, according to estimates. Analysts predict that the cloud's ability to lower costs will hasten the adoption of the technology in government sectors. Researchers and professionals have begun to pay attention to security due to the tremendous increase in cloud computing use, but this focus is still insufficient. In this paper, we are performing a survey on the cutting-edge security solutions and the current challenges with cloud security. We are discussing the most advanced generic countermeasures for attacks on cloud security and assess their efficacy. We also draw attention to the drawbacks of these systems, such as their poor detection coverage and efficiency due to significant communication and processing cost.

REFERENCE:

1. Achar, S. (2022). *Cloud Computing Security for Multi-Cloud Service Providers: Controls and Techniques in our Modern Threat Landscape*. *September*. https://doi.org/10.5281/zenodo.7084251
2. Aikat, J., Akella, A., Chase, J. S., Juels, A., Reiter, M. K., Ristenpart, T., Sekar, V., & Swift, M. (2017). Rethinking Security in the Era of Cloud Computing. *IEEE Security and Privacy*, *15*(3), 60–69. https://doi.org/10.1109/MSP.2017.80
3. Al Morsy, M., Grundy, J., & Müller, I. (2010). An Analysis of the Cloud Computing Security Problem Mohamed. *Apsec*, 1–6.
4. Almond, C. (2009). *A Practical Guide to Cloud Computing Security What you need to know now about*. *August*.

5. Almorsy, M., Grundy, J., & Ibrahim, A. S. (2011). *Collaboration-Based Cloud Computing Security Management Framework*.
6. Alzain, M. A., Pardede, E., Soh, B., & Thom, J. A. (2012). *Cloud Computing Security : From Single to Multi-Clouds*. https://doi.org/10.1109/HICSS.2012.153
7. Ashish Agarwal, A. A. (2011). The risks associated with cloud computing. *International Journal of Computer Applications in Engineering Sciences*, *1*, 20. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.207.9119&rep=rep1&type=pdf
8. Barron, C., Yu, H., & Zhan, J. (2013). *Cloud Computing Security Case Studies and Research*. *II*, 1–5.
9. Beri, R. (2015). Descriptive Study of Cloud Computing An Emerging Technology. *International Journal on Recent and Innovation Trends in Computing and Communication*, *3*(3), 1401–1404. https://doi.org/10.17762/ijritcc2321-8169.1503108
10. Castro-Leon, E., Shekhar, M., Kennedy, J. M., Wheeler, J., Harmon, R. R., Martinez Elicegui, J., & Yeluri, R. (2012). on the Concept of Metadata Exchange in Cloud Services. In *Intel Technology Journal* (Vol. 16, Issue 4). http://search.ebscohost.com/login.aspx?direct=true&db=buh&AN=89557221&site=ehost-live
11. Che, J., Duan, Y., Zhang, T., & Fan, J. (2011). Study on the security models and strategies of cloud computing. *Procedia Engineering*, *23*, 586–593. https://doi.org/10.1016/j.proeng.2011.11.2551
12. Chen, D. (2012). *Data Security and Privacy Protection Issues in Cloud Computing*. *973*, 647–651. https://doi.org/10.1109/ICCSEE.2012.193
13. de Bruin, B., & Floridi, L. (2017). The Ethics of Cloud Computing. *Science and Engineering Ethics*, *23*(1), 21–39. https://doi.org/10.1007/s11948-016-9759-0
14. Douglas, K. M., & Sutton, R. M. (2010). Kent Academic Repository. *European Journal of Social Psychology*, *40*(2), 366–374.
15. Fundamentals, C. C., Architecture, C. C., Computing, C., Security, S., Computing, C., Issues, R., Computing, C., Challenges, S., Computing, C., Architecture, S., Computing, C., Cycle, L., & Steps, U. N. (n.d.). *No Title*.
16. Hashemi, S. M., & Bardsiri, A. K. (2012). Cloud Computing Vs. Grid Computing. *ARPN Journal of Systems and Software*, *2*(5), 188–194. http://www.scientific-journals.org/
17. Herrera Perez, J. L., Fajes Alfonso, A., & Alvarez, D. (1989). Retinopatia Diabetica E Hiperlipoproteinemia. *Revista Cubana de Medicina*, *28*(4), 333–340.
18. Jansen, W., Grance, T., Jansen, W., & Grance, T. (2011). *Leica Microsystems - Multiphoton Microscopy*. https://www.leica-microsystems.com/science-lab/topics/multiphoton-microscopy/
19. Lee, K., & Son, M. (2017). DeepSpotCloud: Leveraging Cross-Region GPU Spot Instances for Deep Learning. *IEEE International Conference on Cloud Computing, CLOUD*, *2017-June*, 98–105. https://doi.org/10.1109/CLOUD.2017.21
20. Liu, W. (2012). Research on cloud computing security problem and strategy. *2012 2nd International Conference on Consumer Electronics, Communications and Networks, CECNet 2012 - Proceedings*, 1216–1219. https://doi.org/10.1109/CECNet.2012.6202020
21. Mohabbattalab, Elnaz Mohabbattalab, B. (2014). *1 Introduction 2 Cloud computing concept 3 Research Methodology*. *3*(5), 1–5.
22. Prakash, C., & Dasgupta, S. (2016). Cloud computing security analysis: Challenges and possible solutions. *International Conference on Electrical, Electronics, and Optimization Techniques, ICEEOT 2016*, *March 2016*, 54–57. https://doi.org/10.1109/ICEEOT.2016.7755626
23. R B, M., & Tiwari, H. (2017). a Review on Cloud Computing Security Issues and Challenges. *International Journal of Research -GRANTHAALAYAH*, *5*(4RACSIT), 76–80. https://doi.org/10.29121/granthaalayah.v5.i4racsit.2017.3357
24. Ryan, M. D. (2013). The Journal of Systems and Software Cloud computing security : The scientific challenge , and a survey of solutions. *The Journal of Systems & Software*, *86*(9), 2263–2268. https://doi.org/10.1016/j.jss.2012.12.025
25. Sengupta, S. (2011). *Cloud Computing Security – Trends and Research Directions*. *July*. https://doi.org/10.1109/SERVICES.2011.20
26. Shahzad, F. (2014). State-of-the-art Survey on Cloud Computing Security Challenges , Approaches and Solutions. *Procedia - Procedia Computer Science*, *37*, 357–362. https://doi.org/10.1016/j.procs.2014.08.053
27. Shaukat, M. W., Raza, S. M., Suh, D. Y., & Piran, J. (n.d.). *A Review of Machine Learning Algorithms for Cloud Computing Security*. 1–25. https://doi.org/10.3390/electronics9091379
28. Singh, H. (2018). *A Review of Cloud Computing Security Issues A Review of Cloud Computing Security Issues*. *October 2015*. https://doi.org/10.14257/ijgdc.2015.8.5.21
29. Upadhyay, N. (2017). Managing Cloud Service Evaluation and Selection. *Procedia Computer Science*, *122*, 1061–1068. https://doi.org/10.1016/j.procs.2017.11.474
30. Wang, L., Von Laszewski, G., Younge, A., He, X., Kunze, M., Tao, J., & Fu, C. (2010). Cloud computing: A perspective study. *New Generation Computing*, *28*(2), 137–146. https://doi.org/10.1007/s00354-008-0081-5
31. Yu, S., Wang, C., Ren, K., & Lou, W. (2010). Achieving secure, scalable, and fine-grained data access control in cloud computing. *Proceedings - IEEE INFOCOM*. https://doi.org/10.1109/INFCOM.2010.5462174
32. Zhang, O. Q., Kirchberg, M., Ko, R. K. L., & Lee, B. S. (2011). How to track your data: The case for cloud computing provenance. *Proceedings - 2011 3rd IEEE International Conference on Cloud Computing Technology and Science, CloudCom 2011*, *June 2014*, 446–453. https://doi.org/10.1109/CloudCom.2011.66
33. Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. *Future Generation Computer Systems*, *28*(3), 583–592. https://doi.org/10.1016/j.future.2010.12.006