Resilience Cloud Security Framework

Amitabha Yadav

Department of IT, DDUKK, National P.G. College, Lucknow, Uttar Pradesh, India

Corresponding author: Amitabha Yadav, Email: amitabha.engg@yahoo.com

Cloud security refers to the practices, technologies, policies, and measures designed to protect data, applications, and infrastructure in cloud computing environments. Cloud security is crucial because organizations are cloud for their data storage which is very sensitive in nature and process critical applications in the cloud, making them potential targets for cyberattacks. Because of the ever-increasing popularity, cloud computing has garnered considerable attention during the last several decades. Businesses are getting benefited by using Cloud data storage like virtual use of Information Technology infrastructure and their management, virtually remote access from any location with a steady connection to the internet. The cloud storageis also providing monitoring savings. Anyone can easily access the cloud storage on pay-as-you-go model which needs more investigation towards the security and privacy of cloud computing. The paper includes the criticalliterature of Resilience Cloud Security Framework which acts as an Antivirus for securing cloud Systems against Cyber Attacks through Cryptography Techniques. The paper covers cloud security concerns and requirements along with acknowledged cloud attacks and vulnerabilities. The purpose of the paper is to analyze various-cloud security components along with privacy issues. The paper includes a new kinds of security solutions. The paper is survey based and focused on different kinds of security vulnerabilities that risked the services of cloud. The paper proposed future possibilities and explores in depth the security concerns that cloud companies such as cloud vendors, data owners, and cloud users face.

Keywords: Cyber Attacks, Cloud, Security, Cryptography

2023. In Satyasai Jagannath Nanda & Rajendra Prasad Yadav (eds.), *Data Science and Intelligent Computing Techniques*, 433–441. Computing & Intelligent Systems, SCRS, India. https://doi.org/10.56155/978-81-955020-2-8-39

1. Introduction

Cloud Computing is nowadays popularizing as a hot topic in respect of storage. Everyone is using the cloud as a storage media to easier their work. India is becoming more digital and digitally linked. Internet users are currently more than 80 crores, with that number rising daily. Due to the launch of 5G in the year 2022 after COVID-19, the number is anticipated to rise significantly [1]. Users' devices are getting more and more vulnerable as a result of the growing number of users, which also increases the likelihood of cyberattacks. Because the majority of users in this digital age are not tech-savvy, online users need to be more cautious. In 2022 Nortan Labs claims that greater effort would be required in the area of online security because thieves now have access to new methods [2]. The data of recent cyberattacks are equally frightening. According to the report provided by Global Cyber Security Firm Trend Micro in the first half of 2021, over 40.9 billion emails with threats, harmful files, and URLs were banned [3].

According to the statistics of Malware attacks in 2023, Although malware is still a significant concernglobally, its nature is changing and evolving every year. In 2022, Hackers adopted new ways to target fresh and not used vulnerabilities for injecting malware in cloud [4]. There are currently indications that hackers are turning their attention to targeted infections via email and IoT. Particularly when it comes to ransomware attacks, the government and big enterprises continue to receive more attention than the typical web user.

Table 1. Malware Statistics

Types of Malwares	2020	2021	2022
Employees with infected machines Like phishing, Spyware, Trojans and Worms.	61%	74%	75%
Ransome ware Attacks	51%	61%	70%

As per Table 1 till 2022 malware attacks are increasing year by year. There is no way to tell what new threats may emerge and how the malware landscape may shift. Hackers change their tactics only when their efforts become unprofitable [5]. With the massive growth of data and increasing complexity challenges, organizations are looking for a new way to modernize I.T. to take advantage of data, backup, and disaster recovery. Earlier mode of data storage was physical, but as the data is growing day by day in Gigabytes physical mode is not sufficient. It is also not suitable to bring storage media along with it every time. Nowadays everyone wants the data on one click from anywhere and anytime basis. For this purpose, we need 24 hours of an available virtual environment for the fast access of data.

Instead of purchasing, occupying, and maintaining offline data centers and software, services can access via technology like computing power storage databases provided by cloud providers like AWS, Microsoft Azure, Google, and many more on a pay-for-its basis [10]. It has three dimensions such as SaaS, PaaS, and IaaS. To use any cloud computing service, one can gain instant access to a broad range of new technology so that one can innovate faster in the field like ML, AI, IoT, and many more [6]. Cloud computing changed the whole world in the World of Virtualization which is governed by the Internet and cloud providers. In cloud computing, everything is stored and sealed in a secure place. All it needs to access with a simple Web Browser. So, cloud Computing is a demand for ideas, sources, or the Internet [9]. While usingcloud via Internet, the security of the cloud come to mind because Government, Industry, Health care departments, Research Departments, Education Departments, etc., all are moving towards cloud computing [7]. Fig 1 depicts that the whole earth is going towards virtualization via using cloud computing services.

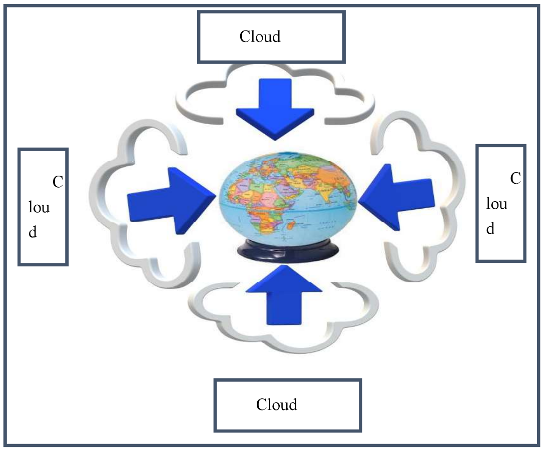

Fig 1: Earth Virtualization via Cloud Computing

The increased demand for organizations to supply services is one of the driving causes for the emergence of cloud computing. However, because data and resources in the cloud are kept and managed in the data centers of third-party Cloud service providers, data security and privacy are top issues for cloud computing customers (CSP) [7]. Furthermore, cloud users connect to the cloud through the Internet; if they do not have an Internet connection, they will not be able to access their documents and applications present on the cloud, resulting in monetary loss. The same problem arises in the case of cyberattacks on different clouds [8]. Although technology emerging day by day for cyber security but day by day attacking ideas are also getting new signatures. So, cloud security is taking an important role in the perspective of different cyberattacks. So, there is a requirement for a security framework for a cloud computing environment. So, we need to work on a Resilience Security Framework in which whenever an attack happens, the framework detects the attack, segment the infected part, Resolve the issue, and at last attach the segmented part to the working system.

2. Related Work

According to National Institute of Standards and Technology (NIST) explain cloud computing as a paradigm for allowing usable, on-demand network access to a shared pool of programmable computer resources.[5] It provides a variety of services in three different models: SaaS, PaaS, and IaaS. Fig b demonstrates that services in blue color are managed by the user itself and services in red color are managed by Cloud service providers. The services provided by the providers are at high risk in terms of security and need to pay more attention because we are relying on a third party. Every service is been controlled by the providers.

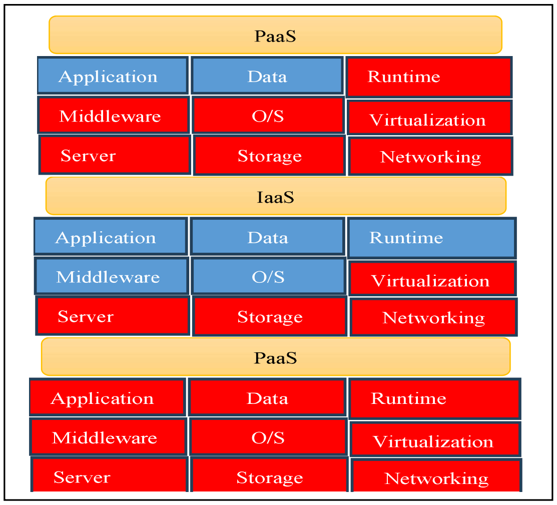

Fig 2: Earth Virtualization via Cloud Computing

Kavin et al. [11] developed a framework based on cloud security to secure data on cloud storage. Author proposed an algorithm for generating very secured keys using Elliptic Curve Cryptography technique. Author also introduced algorithm based on two phase encryption and decryption to protect data. Author proposed Lightweight Digital Signature for data integrity.

Tabrizchi et al. [12] includes critical literature of issues, needs known threats on cloud security. Author highlights the various components of cloud and focuses on problems based on security and privacy. The paper is completely survey based on service providers, cloud users and owners security challenges thar are faced while using the services of cloud.

Patil et al. [13] developeda framework that identify malware attack in virtual machines based on artificial intelligence. Author suggested that detect malware at the early stages of virtual machine. Detection of malware is applied on layers of Virtual Machines by using signature and hypervisor techniques which find out known and unknown malwares. The framework provides a benefit by reducing communication cost and pass on the unknown malware for detection at layer of hypervisor.

Sgandurra and Lupu [15] established the scientific process for assaults in system virtualization to identify various levels and source for attacker's mind. They intend to demonstrate the origin of threats, security, and trust considerations in virtual servers at various levels like hardware, operating system, and application.

Kaur and Singh [16] provided an overview of security concerns. Author focused on location of data, database storage, security, availability and integrity. The analysis is focused on basically security problems, formally it emphasized the security vulnerabilities without proposing potential remedies.

Kumar et al. [17] illustrated various kinds of challenges in data security along with some solution for security problems in a multi-tenant context. The article is entirely dedicated to data security challenges, as well as techniques for protecting data and privacy.

Khalil et al. [18] gives meta-analysis for cloud security services and privacy issues. Many kinds of classification are given on security risk and their assaults along with different types of vulnerabilities. Author presents shortcomings of known solution and gave future security perspectives.

Bashir and Haider [19] conducted a comprehensive analysis to identify the demanded susceptible cloud computing security concerns. Furthermore, by giving analysis linked to the various security models and technologies, the review study analyses theimportant security issues connected with cloud computingend users and suppliers.

Ryan [20] presents critical literatureresearch ways like data protection strategy which intends to keep data secure from the cloud platform provider. Furthermore, the paper provides a browser key translation approach that enables a software-as-a-service application to deliver secrecy services. Cloud computing provides high quality services and sharable resources [21] by using the use of computers as a utility where user access the data remotely. Because the bulk of cloudrelated technologies have shown numerous indicators of advancement in today's world, security concerns have evolved and new issues have emerged. There is extensive need of study along with the identification of prospective issues and the development of innovative solutions.

3. Cloud Attack

Cloud attacks refer to a range of cybersecurity threats and attacks that target cloud computing scenarios, including cloud infrastructure, platforms, and services. Cloud computing has become increasingly popular because of its scalability, flexibility, and cost-effectiveness, but it also introduces new security challenges[21]. Additionally, it the responsibility of the cloud user to better understand the shared responsibility model, where the provider is responsible for certain aspects of security, while the customer is responsible for others. This collaboration is essential for ensuring the security of cloud environments. Following are some common kinds of cloud attack as shown in the Fig 3.:

3.1 Data Breaches

Sensitive Data storage by any unauthorized access on cloud repositories is a prevalent threat. Attackers may exploit vulnerabilities in cloud service configurations or use stolen credentials to gain access to data [23].

3.2 DDoS Attacks

Distributed Denial of Service (DDoS) attacks to overwhelm cloud services with a flood of traffic, causing them to become unavailable [24]. This can disrupt businesses and services that rely on the cloud.

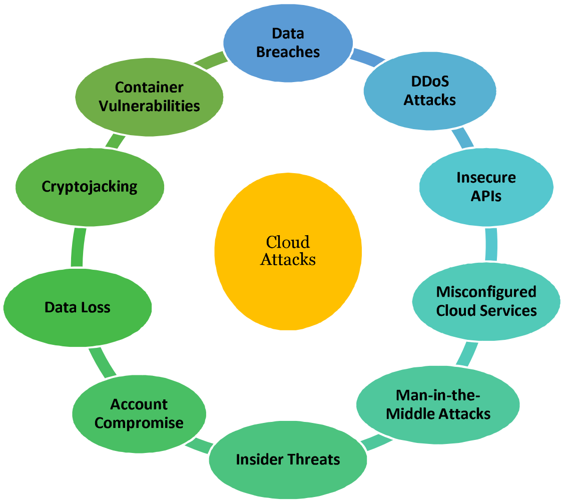

Fig 3: Cloud Security Attacks

3.3 Insecure APIs

Cloud services often offer APIs (Application Programming Interfaces) to interact with them. To access the resources of the cloud, Insecure APIs may be breached to provide authentication [25].

3.4 Misconfigured Cloud Services

Misconfigurations in cloud service settings, such as improperly configured security groups or access control lists, can expose data and resources to attackers [26].

3.5 Man-in-the-Middle Attacks

Attackers intercept and manipulate communications between cloud users and services to steal data or launch other attacks [27].

3.6 Insider Threats

Malicious insiders, like users or mediators with access to cloud resources, can misuse their privileges to steal data or cause damage [28].

3.7 Account Compromise

When cloud user accounts are compromised through techniques like phishing or weak passwords, attackers can gain access to cloud resources [29].

3.8 Data Loss

Storage of Data on the cloud can be lost due to accidental deletion, data corruption, or inadequate backup procedures [30].

3.9 Cryptojacking

Attackers may use cloud resources to mine cryptocurrencies without the knowledge or consent of the cloud owner, leading to resource consumption and increased costs [21].

3.10 Container Vulnerabilities

Containers and container orchestration platforms like Docker and Kubernetes can have security vulnerabilities that attackers can exploit [22].

To protect against cloud attacks, organizations should implement robust security practices, including:

- Strong access controls and authentication mechanisms.
- Regular security audits and vulnerability assessments.
- Proper configuration management.
- Monitoring and logging of cloud resources for suspicious activities.
- Employee training and awareness programs to prevent insider threats.
- Deploying DDoS mitigation measures.
- Keeping cloud service and software updated with security coverage.

4. Cloud Security Framework

The reason is as follows why Cloud Security Framework is playing an important role in today's digital era:

- Frameworks contains system standards, techniques, guidelines, and processes which connect policy, business, and technology nears to cyber risk management.
- It includes in finding, evaluating, and controlling the risk offered by cyber by providing data security measures and controls.
- Identify the possibilities for improvement which may be reached via future collud with specific industries and standards setting bodies.
- Prioritize a flexible, performance-based, repeatable, cost-effective strategy.
- Comply with voluntary international standards
- It leads to a shift in focus from compliance to action and a specified objective

5. Conclusion

Now a days cloud computing plays an important role towards the advancement of Information Technology. Every cloud consumer continues to demand the best service possible, mainly in terms of security. The lack of standardized norms in the cloud world's security framework, particularly in the cloud computing community, became an unending challenge. Most cloud providers, by default, adhere to the best security policies and actively defend the functionality of their systems. When it comes to securing data, apps, and workloads in the cloud, enterprises must make their own decisions. As the digital ecosystem evolves, security risks have gotten increasingly sophisticated. Because of an organization's total lack of coverage in data access and movement, these attacks expressly target cloud computing providers. Organizations might face considerable governance and management risks when handling client data, irrespective of where it is housed, if they do not actively enhance their cloud security.

However, cloud application adoption is contingent on having enough countermeasures in place to fight against modern-day cyberattacks. Whether the company works in a public, private, or hybrid cloud environment, online security products and best practices are essential for guaranteeing business continuity. Every organization's approach to cloud security is unique and can be influenced by a variety of factors. However, the National Institute of Standards and Technology (NIST) has developed best practices guidelines for establishing a safe and long-term cloud computing architecture. The NIST has developed the procedures required for every company to self-assess their security preparedness and adopt suitable preventative and recovery security measures for their systems. These principles are based on the five pillars of a cyber security architecture established by the NIST: identify, protect, detect, respond, and recover.

Although technology for cyber security is evolving daily, new attack concepts are also developing daily. So, the research will help to work on a resilience security framework, which means that whenever an attack occurs, we must detect it quickly, and segment part of the system, which is analogous to amputating a part of the body so that other parts of the body can survive, resolve the issue, and then reattach the segmented part to the system so that the system can function normally.

References

[1] Subramanian N, Jeyaraj A (2018) Recent security challenges in cloud computing. ComputElectrEng 71:28–42

[2] Mell P, Grance T (2018) SP 800-145, The NIST Definition of cloud computing | CSRC (online)Csrc.nist.gov. https ://csrc.nist.gov/publicatio ns/detai l/sp/800-145/final . Accessed 11 Dec 2018.

[3] Xu X (2012) From cloud computing to cloud manufacturing. Robot ComputIntegr Manuf28(1):75–86

[4] Pippal SK, Kushwaha DS (2013) A simple, adaptable and efficient heterogeneous multi-tenant database architecture for ad hoc cloud. J Cloud Comput Adv Syst Appl 2(1):5

[5] Shi B, Cui L, Li B, Liu X, Hao Z, Shen H (2018) Shadow monitor: an effective in-VM monitoring framework with hardware-enforced isolation. In: International Symposium on Research in Attacks,Intrusions, and Defenses. Springer, Berlin, pp 670–690

[6] Bhamare D, Samaka M, Erbad A, Jain R, Gupta L, Chan HA (2017) Optimal virtual network function placement in multi-cloud service function chaining architecture. ComputCommun 102:1–16

[7] Alzahrani A, Alalwan N, Sarrab M (2014) Mobile cloud computing. In: Proceedings of the 7th Euro American Conference on Telematics and Information Systems (EATIS'14)

[8] Deka GC, Das PK (2018) Application of virtualization technology in IaaS cloud deployment model.In: Design and Use of Virtualization Technology in Cloud Computing: IGI Global, pp 29–99

[9] Oracle.com (2018) The Oracle and KPMG Cloud Threat Report 2018 | Oracle (online). https ://www.oracl e.com/cloud /cloud -threa t-repor t.html. Accessed 11 Dec 2018

[10] Roman R, Lopez J, Mambo M (2018) Mobile edge computing, fog et al.: a survey and analysis of security threats and challenges. Future Gener Comput Syst 78:680–698

[11] Prabhu Kavin, B., Ganapathy, S., Kanimozhi, U. and Kannan, A., 2020. An Enhanced Security Framework for Secured Data Storage and Communications in Cloud Using ECC, Access Control and LDSA. Wireless Personal Communications, 115(2), pp.1107-1135.

[12] Tabrizchi, H. and Kuchaki Rafsanjani, M., 2020. A survey on security challenges in cloud computing: issues, threats, and solutions. The Journal of Supercomputing, 76(12), pp.9493-9532.

[13] Patil, R., Dudeja, H. and Modi, C., 2019. Designing in-VM-assisted lightweight agent-based malware detection framework for securing virtual machines in cloud computing. International Journal of Information Security, 19(2), pp.147-162.

[14] Yu S, Wang C, Ren K, Lou W (Mar 2010) Achieving secure, scalable, and fine-grained data access control in cloud computing. In: Proceedings of the IEEE INFOCOM

[15] Sgandurra D, Lupu E (2016) Evolution of attacks, threat models, and solutions for virtualized systems.ACMComputSurv 48(3):1–38

[16] Kaur M, Singh H (2015) A review of cloud computing security issues. Int J Adv Eng Technol 8(3):397–403

[17] Kumar PR, Raj PH, Jelciana P (2018) Exploring data security issues and solutions in cloud computing.ProcComput Sci 125:691–697

[18] Khalil I, Khreishah A, Azeem M (2014) Cloud computing security: a survey. Computers 3(1):1–35

[19] Bashir SF, Haider S (Dec 2011) Security threats in cloud computing. In: Proceedings of the International Conference for Internet Technology and Secured Transactions, pp 214–219

[20] Ryan MD (2013) Cloud computing security: the scientific challenge, and a survey of solutions. J Syst Softw 86(9):2263–2268

[21] Wang C, Wang Q, Ren K, Lou W (Mar 2010) Privacy-preserving public auditing for data storage security in cloud computing. In: Proceedings of the IEEE INFOCOM

[22] Singh S, Jeong Y-S, Park JH (2016) A survey on cloud computing security: issues, threats, and solutions. J NetwComput Appl 75:200–222

[23] Khalil IM, Khreishah A, Azeem M (2014) Cloud computing security: a survey. Computers 3(1):1–35

[24] Ahmed M, Litchfield AT (2018) Taxonomy for identification of security issues in cloud computing environments. J Comput Inf Syst 58(1):79–88

[25] Fotiou N, Machas A, Polyzos GC, Xylomenos G (2015) Access control as a service for the Cloud. J Internet Serv Appl 6(1):11

[26] Sumitra B, Pethuru C, Misbahuddin M (2014) A survey of cloud authentication attacks and solution approaches. Int J Innov Res ComputCommun Eng 2(10):6245–6253

[27] Fernandes DA, Soares LF, Gomes JV, Freire MM, Inácio PR (2014) Security issues in cloud environments:a survey. Int J Inf Secur 13(2):113–170

[28] Subashini S, Kavitha V (2011) A survey on security issues in service delivery models of cloud computing.JNetwComput Appl 34(1):1–11

[29] Zhang Y, Chen X, Li J, Wong DS, Li H, You I (2017) Ensuring attribute privacy protection and fastdecryption for outsourced data security in mobile cloud computing. Inf Sci 379:42–61

[30] Abbas H, Maennel O, Assar S (2017) Security and privacy issues in cloud computing. Springer,Berlin