Available Online at www.ijcsmc.com/journal

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IMPACT FACTOR: 7.056

IJCSMC, Vol. 11, Issue. 11, November 2022, pg.4 – 12

Cloud Computing Safety Concern and Its Confronts: A Compressive Investigation

[1]Ms. Swati Jaiswal; [2]Dr. Tryambak Hiwarkar

[1]Research Scholar; [2]Professor

[1,2]Department of Computer Science and Engineering

[1,2]Sardar Patel University Balaghat

DOI: https://doi.org/10.47760/ijcsmc.2022.v11i11.002

Abstract: ***Cloud computing is a new approach to data storage and processing in the field of computer science. Computing in the cloud refers to the use of a network's or the internet's hosted servers and other associated resources. Cloud computing is an expansion of other computing methods such as grid computing and distributed computing. Currently, cloud computing is utilized by both industries and universities. The cloud is a service that helps its users by giving them access to online virtual resources.***

There are always new methods being developed, and cloud computing is a sector that is growing rapidly. In tandem with the growth of the cloud computing environment comes a corresponding rise in the difficulty of ensuring the system's safety. Users trust the cloud with their data, but if their data isn't secure, they may stop using it.

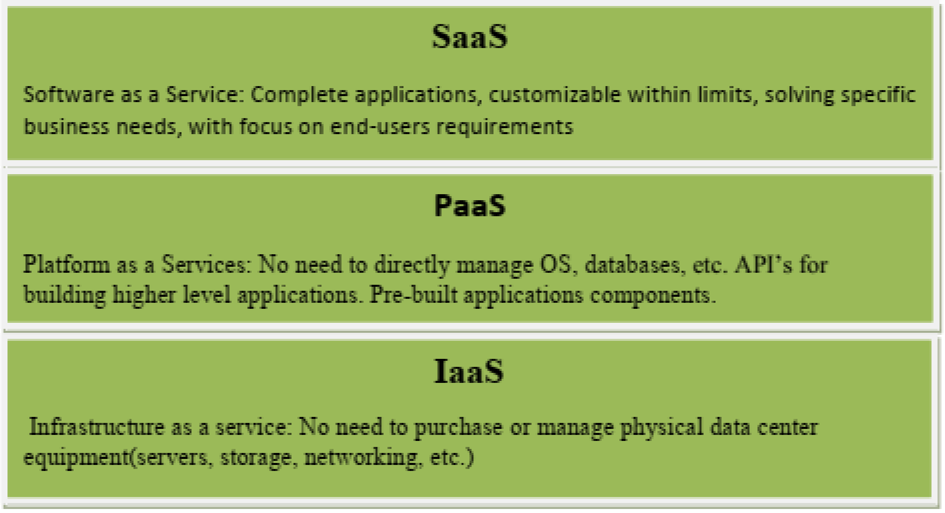
Some of the concerns with cloud security, such as multi-tenancy, will be explored in this paper. Mobility, adaptability, availability, etc. Current security methods and strategies for a safe cloud environment are also discussed in the article. The information presented in this paper will help researchers and practitioners get more familiar with the various security threats and the models and methods provided to combat them.

Keywords: ***Cloud Computing, Security, Attack***

1. Introduction

The term "cloud computing" is used to describe data processing that takes place through the Internet. The National Institute of Standards and Technology (NIST) defines cloud computing as "a model for enabling on-demand and convenient network access to a shared pool of configurable computing resources (e.g., networks, servers, storage applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction[9]." To some, it's a paradigm that facilitates access to cloud-based software and data, while to others, it's merely a means of gaining access to such resources. The scalability, adaptability, and accessibility of the cloud have made it a popular choice for businesses and universities. Since cloud computing facilitates information exchange inside a business, it also helps keep costs down. Companies can upload their data to the cloud for the benefit of their investors. Cloud computing may be seen in action with Google Apps.

There are a number of advantages to using the cloud, but there are also some drawbacks, particularly when it comes to keeping data private. Some of the challenges in cloud computing research include vendor lock-in, multi-tenancy, loss of control, service disruption, data loss, etc. [2]. In this study, we take a look at the risks associated with the cloud computing paradigm. The primary focus is on researching and understanding the many methods that can be used to protect the cloud infrastructure from attack.



SaaS

Software as a Service: Complete applications, customizable within limits, solving specific business needs, with focus on end-users requirements

PaaS

Platform as a Services: No need to directly manage OS, databases, etc. API's for building higher level applications. Pre-built applications components.

IaaS

Infrastructure as a service: No need to purchase or manage physical data center equipment(servers, storage, networking, etc.)

Figure 1 . Layers of Cloud Computing

2. Cloud safety problems

Every type of cloud service, including Infrastructure as a Service, Platform as a Service, and Software as a Service, as well as public, private, and hybrid cloud models, is used by businesses today. There are several cloud security concerns with these models and services. There are a few issues with each of the carrier versions. Carrier Company prioritizes customer safety by overseeing all aspects of customer identification and ensuring the safety of the services provided with their help. The patron perspective ensures that the carrier the customer is using is reliable.

2.1 Multi-tenancy

As a result of the need to pool assets like storage space, processing power, and memory, a cloud-based variant is developed [2]. When resources are shared amongst multiple tenants, costs are reduced. Sharing means that several tenants on the same physical/logical platform at the provider's premises share compute resources, offers storage, and alerting. This compromises data security by allowing unauthorized access to sensitive information, preventing proper encryption of sensitive data, and increasing the likelihood of assaults.

2.2 Elasticity

The degree to which a system is elastic is measured by how well it can respond to changes in workload through autonomic provisioning and resource reorganisation, with the goal of making the available resources match the current demand as closely as feasible. Scalability is a key aspect of elasticity. Scalability as needed is mentioned, meaning that clients have that option. With this scaling, tenants can make use of a service that was previously allocated to another tenant. However, there may be concerns about privacy if too many people know about it.

2.3 Insider attacks

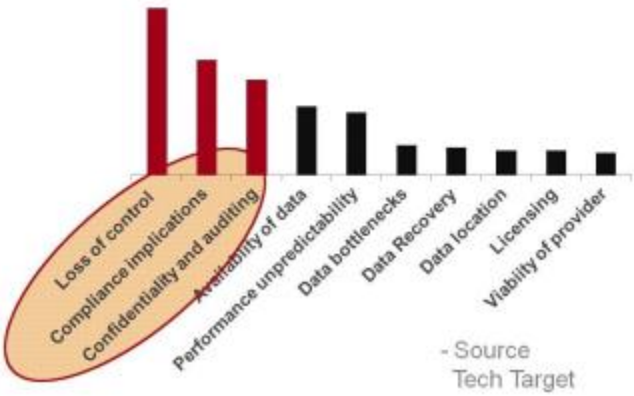
The cloud version is a multitenant based version that is managed centrally by the supplier. That's a risk that crops up in any big company. When it comes to cloud workers, there aren't any strict stipulations for hiring or benefits packages [1]. As a result, a vendor or hacker can easily gain access to a company's internal data and use malicious software to alter the data or sell it to competitors.

2.4 Outsider attacks

This is the one of the predominant regarding problem in a corporation as it releases the exclusive facts of a corporation in open. Clouds aren't like a personal network, they have extra interfaces than personal network. So hackers and attackers have gain of exploiting the API, weak point and might do a connection breaking [1] .These assaults are less dangerous than the insider assaults due to the fact with inside the later we from time to time not able to pick out the attack.

2.5 Loss of control

Cloud makes use of a area transparency version with the aid of using which it permit agencies to unaware approximately the area in their offerings and information. Hence issuer can host their offerings from everywhere in the cloud. In this situation agency might also additionally lose their information and in all likelihood they're now no longer conscious approximately protection mechanism installed region of the issuer.



- Source
Tech Target

Figure 2. Loss of Control over Data

3. REVIEW OF LITERATURE

The writers first considered this by presenting a paper about cloud computing services including networks, storage, servers, products, and programmers that can be used without really having access to them. Overhead of the large device has been reduced in terms of chance, information leakage, etc., as noted in the paper's comments [1]. Cloud services provide flexible, as-needed Internet access. The cloud is an adequate answer for those who do not need to set up infrastructure in personal device if the company providing the internet services wishes to invest large sums of capital cash for infrastructure and difficulties like system failure, disc failure, software insects, etc. [2] According to the research presented here, cloud customers are reluctant to spend money on necessary infrastructure upgrades, preferring instead to pay for their services on a usage basis. In 2012, authors discussed cloud security, noting that while data is expanding exponentially, the security of infinite and comparatively simple to access resources is still debatable. This study explores security risks stemming from cloud computing environments, characteristics, cloud delivery models, and cloud stakeholders. [4]. In their brief, the writers touch on the topic of cloud security. Because more and more people are sending, receiving, and storing sensitive data on the cloud, ensuring the safety of the cloud community has become an increasing priority. [5] These paintings' creators discuss a few of their Risks to cloud security include leaks of sensitive data and the possibility of a man-in-the-middle attack or data corruption. As a result of its malleability, value performance, and information translation between client and server, the cloud is one of the most researched areas of technology. [6] This paper goes into detail about how a popularity control device helps to keep the transaction desk secure, which contains sensitive information. In spite of virtualization's importance to cloud computing, its security has received little attention as of yet [7]. This paper presents a review of cloud security, with a focus on the effects of virtualization attacks on various deployments of cloud computing services. With the aid of virtualization, cloud computing provides a shared platform for hardware, software, and other resources [8]. With a cloud-based service, you may expect a more adaptable and dependable service environment. Information stored in the cloud can be encrypted using the RSA rule set and a digital signature, both of which are examples of the types of protection offered by cloud security. In order to increase the safety of data stored in the cloud, models of protective control and standards for it are outlined in [9], and RSA rules and a digital signature are used to ensure its integrity throughout transmission.

The Internet of Things (IoT) and cloud computing are the most pivotal technologies at present. Consequently, Cloud IoT—the combination of Internet of Things and cloud computing—has been highlighted as one of the most pressing needs in the current internet infrastructure. The cloud is a shared, online resource that lets users access a shared pool of shared resources. Most companies are moving their data to the cloud, which means it's important to talk about the security threats that come along with using cloud resources including infrastructure, network, platform, software, and storage. One of the most serious threats is the diversity of a Denial-of-

Service (DOS) attack, and its larger aspect is a Distributed Denial-of-Service (DDOS) attack; these are the various types of network intrusion in a cloud computing environment [15] are proposing a method that can filter and detect most attacked traffic within a cloud.

4. Techniques to Secure Data in Cloud

4.1 Authentication and Identity

There are a number of methods for establishing a user's or a system's credibility, but cryptography is by far the most prevalent [8]. Customers can be verified in a number of ways, including through the use of individually recognized passwords, security tokens, and quantifiable amounts like fingerprints. When an organization uses multiple CSPs, it can be difficult to use traditional identification methods in a cloud environment[8]. Regardless of the application, it's not always feasible to scale up the process of matching user IDs with the appropriate government agency. When moving infrastructure toward a cloud-based answer, other problems arise with traditional identification approaches.

4.2 Data Encryption

Consider using statistics encryption methods if you intend to store sensitive data on a large data storage system. Passwords and firewalls are helpful, but hackers can still gain access to your data if they really want to. Statistics that has been encrypted is in a format that cannot be read without the corresponding decryption key. To the intruder, the numbers mean absolutely nothing. It's a way to decipher mysterious messages based on statistical analysis. In order to decipher the encrypted data, you must have access to the game key or password, which is also known as the encryption key.

4.3 Data truthfulness and Privacy

Cloud computing makes data and resources available to authorized users. Through web browsers, both legitimate users and malicious actors can access the resources [2]. Creating an atmosphere of mutual trust between service providers and their customers is a practical approach to solving the issue of information integrity. One alternative is to implement strong authentication, authorization, and accounting controls that require multiple checks on data access before allowing it [2]. For example, RSA certificates and SSH tunnels should be made available as secure access mechanisms.

4.4 Malware-injection attack solution

This solution creates a no. of client virtual machines and stores all of them in a central storage. It utilizes FAT (File Allocation Table) consisting of virtual operating systems [10]. The application that is run by a client can be found in FAT table. All the instances are managed and scheduled by Hypervisor. IDT (Interrupt Descriptor Table) is used for integrity checking.

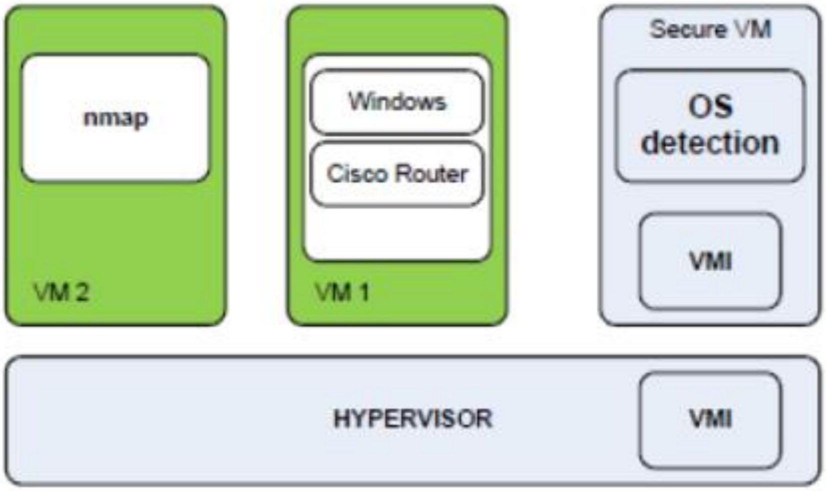


Figure 3. Malware-Injection attack solution

4.5 Flooding Attack Solution

When talking about the cloud, all of the servers together are referred to as a fleet. We use one set of servers for system-level requests, another set for memory management, and a third set for computations at the heart of the system. Each of the fleet servers has the ability to talk to every other fleet server. If a server becomes too busy, a backup server is brought in to take its place, and a third server, the "name server," is used to keep track of the servers' current statuses and make necessary changes to their destination addresses and operational statuses. The use of a hypervisor for task management is demonstrated in [10]. The hypervisor is also responsible for the authentication and authorization of jobs. It is possible to trace a legitimate request from a Customer by its PID. The PID can also be encrypted using RSA.

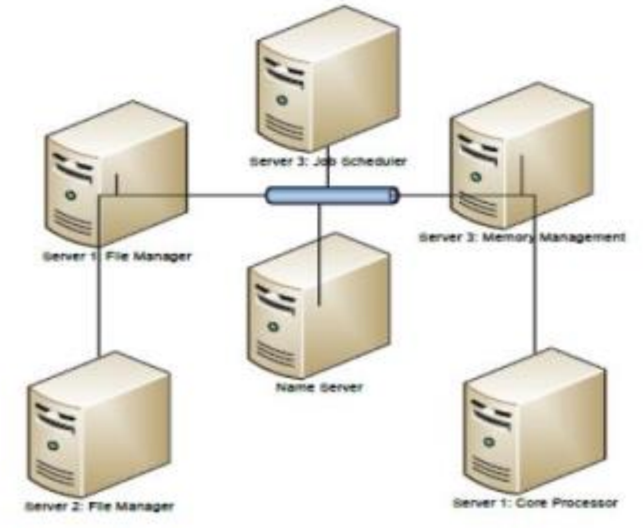


Figure 4 . Flooding Attack solution

5. Conclusion

This paper explains what the cloud is and how it works, including its scalability, independence from other platforms, low cost, elasticity, and dependability. However, in this paper, we have discussed some of the security challenges in cloud computing and also the techniques to prevent them, which can be used to keep the communication secure and get rid of the security issues. The primary goal of this survey is to examine the various approaches to eradicating issues like attacks, data loss, and unauthenticated access to data. Because of the ever-changing nature of the cloud, the tried-and-true security measures employed in other contexts do not translate well to its virtualized ones. Cloud computing security is being worked on by groups like the Cloud Security Alliance (CSA) and the National Institute of Standards and Technology (NIST). While we have covered a few security methods in this paper, there are many others currently under development. As many systems communicate and perform operations in a cloud, certain standards are also specified that can be used to maintain secure communication and security.

References

1. Akhil Behl (2011), Emerging Security Challenges in Cloud Computing (An insight to Cloud security challenges and their mitigation).

2. Akhil Behl & Kanika Behl (2012), An Analysis of Cloud Computing Security Issues.

3. L. Ertaul, S. Singhal & G. Saldamli, Security Challenges In Cloud computing.

4. Peter Mell, Tim Grance, The NIST Definition of Cloud Computing, Version 15, October 7, 2009.

5. Cloud Computing: Benefits, Risks and Recommendations for Information Security. ENISA(European Network and Information Security Agency), Crete, 2009.

6. Cloud computing security forum http://cloudsecurity.org/

7. Cloud Computing – A Practical Approach by Velte, Tata McGraw- Hill Edition (ISBN-13:978-0-07-068351-8).

8. Yashpalsinh jadeja & kirti modi (2012) cloud computing- concepts, architecture and challenges.

9. Satyendra singh rawat & Mr. Alpesh Soni (2012) ,A Survey of Various Techniques to Secure Cloud Storage.

10. R. Balasubramanian, Dr.M.Aramuthan (2012) Security Problems and Possible Security Approaches In Cloud Computing.

11. Anup Bhange , Dr Harsh Mathur "Performance Evaluation, Analysis and Design of an Innovative Structure to Secure the Payment Gateways using Hybrid Cryptography" Asian Journal of Information Technology Volume: 20, Issue 2, 2021 ISSN: 1682-3915.

12. Anup Bhange, "DDoS Attacks Impact on Network Traffic and its Detection Approach" International Journal of Computer Applications (0975 – 8887) Volume 40– No.11, February 2012.

13. Anup Bhange, "Anomaly Detection and Prevention in Network Traffic Based on Statistical approach and α-Stable Model "International Journal of Advanced Research in Computer Engineering & Technology ISSN: 2278 – 1323 Volume 1, Issue 4, June 2012.

14. Anup Bhange "Comparative Analysis of Several Cryptography Algorithm with Its Effectiveness towards the Security and Its Performance" in JGRS (UGC CARE) ISSN: 0374-8588 Volume 21 Issue 6 October 2019.