Online at: https://researchtrendsjournal.com
Indexed Journal

ISSN No: 2584-282X
Peer Reviewed Journal

INTERNATIONAL JOURNAL OF TRENDS IN EMERGING RESEARCH AND DEVELOPMENT

Volume 3; Issue 6; 2025; Page No. 112-116

Received: 21-08-2025
Accepted: 30-09-2025
Published: 14-11-2025

An Analytical Study of Security Challenges and Vulnerability Models in Cloud Computing

[1]Abhishekh Samaiya and [2]Dr. Bimal Kumar Rai

[1]Research Scholar, Department of Computer Science & Application, Mahakaushal University, Jabalpur, Madhya Pradesh, India
[2]Associate Professor, Department of Computer Science & Application, Mahakaushal University, Jabalpur, Madhya Pradesh, India

DOI: https://doi.org/10.5281/zenodo.18265930

Corresponding Author: Abhishekh Samaiya

Abstract

The infrastructure and ideas of the computers of the future are based on cloud computing. A shift towards cloud-based architecture is happening quickly in the world's computer infrastructure. While expanding cloud computing's applications to other industries is crucial, concerns about data security in the cloud should not be overlooked. A new business trend centred on cloud technology has emerged as a result of the evolution of cloud-based services and service providers. Now that there are so many cloud services offered by widely scattered cloud providers, sensitive data belonging to various entities is often kept on distant servers, which leaves them vulnerable to intrusion in the event that those servers are hacked. The reliability and adaptability of cloud computing would be severely compromised in the absence of strong and consistent security measures. In this article, we will take a look at the fundamentals of cloud computing and the security concerns that come with it.

Keywords: Cloud computing, cloud service, cloud security, computer network, distributed computing, security

Introduction

The term "cloud computing" refers to the practice of providing resources such as data storage, servers, databases, networking, and software over the Internet. A new age in IT has begun with cloud computing's meteoric rise to the top of the digital economy. One must have a firm knowledge of cloud computing's foundational ideas and architecture in order to completely comprehend the security issues it poses.

Cloud computing has provided previously unseen degrees of efficiency, scalability, and adaptability in data storage, processing, and management. Concerns about the safety of cloud-based systems have grown in recent years due to the widespread use of cloud services by both people and organisations. When placed in the context of a dynamic digital world, cloud computing signifies a dramatic change from on-premises IT solutions to internet-based services. Although there are many positive aspects to this change, it also brings a new set of security concerns. Cloud services, because to their decentralized structure and resource sharing, might introduce new types of vulnerabilities not seen in conventional information technology settings. A common cloud computing architecture is shown in Figure 1. The gravity of security breaches in the cloud cannot be emphasised enough, as they may lead to devastating outcomes such as the loss of data, invasion of privacy, financial losses, and a general decline in user confidence. It is also more difficult to provide consistent security across various cloud services due to their dynamic and scalable nature service models and deployment types, including IaaS, PaaS, and SaaS, as well as public, private, and hybrid clouds.

Computer substantially altered both the nature and practice of computing and the idea of computer resources. It is common practice in cloud computing for users to access

resources located on another party's premises or network from a distant location (Petre, 2012; Ogigau-Neamtiu, 2012; Singh & Jangwal, 2012) [5, 6, 7]. Processing is done remotely, which means that user input (such as data) must be sent to a server or cloud infrastructure for processing. Once processing is complete, the input is returned. Storage on distant cloud servers may be necessary or even feasible in some situations. Specifically relevant to the operational setting of cloud computing are the following three delicate situations or states:

- The transmission of personal sensitive data to the cloud server.
- The transmission of data from the cloud server to clients' computers and
- The storage of clients' personal data in cloud servers which are remote server not owned by the clients

Literature Review

Ouali, Sami. (2023) [1]. Businesses of all sizes and in every sector are increasingly relying on cloud computing to streamline their operations, save expenses, and gain more operational flexibility. On the other hand, there are now more security concerns than ever before due to the widespread use of cloud computing and the fact that important systems and sensitive data are being transferred to infrastructure in the cloud, which may be overseen by outside parties. Data breaches, malware, and cloud-based assaults are just a few examples of the cyber hazards that organizations face in the cloud. This chapter covers these threats and how organizations may safeguard their data, infrastructure, and applications against them.

Javaid, Adeel. (2013) [2]. Due to the proliferation of cloud topologies, cloud computing has become an increasingly hot topic among IT security professionals. Google, Amazon, Microsoft, Oracle, Sun, Canonical, Eucalyptus, and many more providers provide public clouds. Virtualization software providers like VMware, Citrix, and Microsoft are just a few of the hundreds of companies providing cloud solutions. Another option is private cloud technologies, which include installing cloud software on local or in-house server infrastructure. In response to a query for "private cloud hosting," Google returned 581,000 pages. It all starts with the infrastructure when it comes to cloud security.

Patil, Prerna. (2024) [3]. We need strong cybersecurity measures since cloud computing is becoming more and more important to contemporary infrastructures. In this article, we take a look at the new cybersecurity risks associated with cloud computing, with an emphasis on sophisticated assaults such as data breaches, vulnerabilities in virtualization, insider threats, DDoS attacks, and APTs. It delves into mathematical models for risk assessment, encryption efficiency evaluation, and threat probability assessment.

Bhadra, Sompurna *et al*. (2020) [4] With the advent of new technologies like Big Data, the Internet of Things, and Cloud Computing, the computer sector is undergoing rapid transformation in this age of the Fourth Industrial Revolution. The corresponding increase in the size and complexity of computer activities and processes is unprecedented. In today's informational environment of the networked society, Cloud Computing (hereinafter shortened as CC) is becoming a maze despite the huge benefits it provides to its stakeholders, both people and organisations. The availability of high-capacity network systems, less expensive computers and scalable storage tools, reliable hardware virtualization, and necessary service orientated architectural frameworks has led to the global establishment of CC as a popular and promising domain of technological paradigm.

Cloud Service Models

Computing in the cloud refers to the practice of third-party providers making available to end users a shared pool of shared computing resources, including data storage, applications, and servers. Web browsers allow end users to access cloud services on demand. Cloud computing service providers guarantee the quality of their services and provide particular cloud options. There are essentially three levels to cloud computing: system, platform, and application.

Concerns about data privacy and security in the cloud persist regardless of the terms of service agreements between cloud providers and their clients. Even now, they are a danger in cloud environments, especially when the supplier doesn't have enough data to implement proper security measures. A common cloud service model's abstract layers are shown in Figure 1.

Particularly with public clouds, many users mistakenly believe that only cloud providers are responsible for the security and integrity of their data.

Software as a Service (SaaS)

Software is rented out to cloud users under this arrangement, and the facility is meant to supply everything. The service grants customers access to the apps hosted in the provider's cloud. The ability to maintain and control the underlying infrastructure's network, operating systems, servers, storage, and individual applications' capabilities is solely with the cloud provider, as may be stipulated in the Service Level Agreement.

The term "software as a service" refers to the ability for customers to use a cloud-based application. Any Internet-connected device, including desktop PCs, laptops, and mobile phones, may access the program. Because the approach is provided as on-demand services, there is often no upfront cost associated with SaaS. No underlying infrastructure costs, such as those for servers, operating systems, networks, and storages, are involved in this approach, therefore the cost to host applications is very minimal; clients only need to pay for, operate, and maintain the hosted applications. Zoho Expenses, Salesforce, Azure, and Microsoft are just a few examples of SaaS.

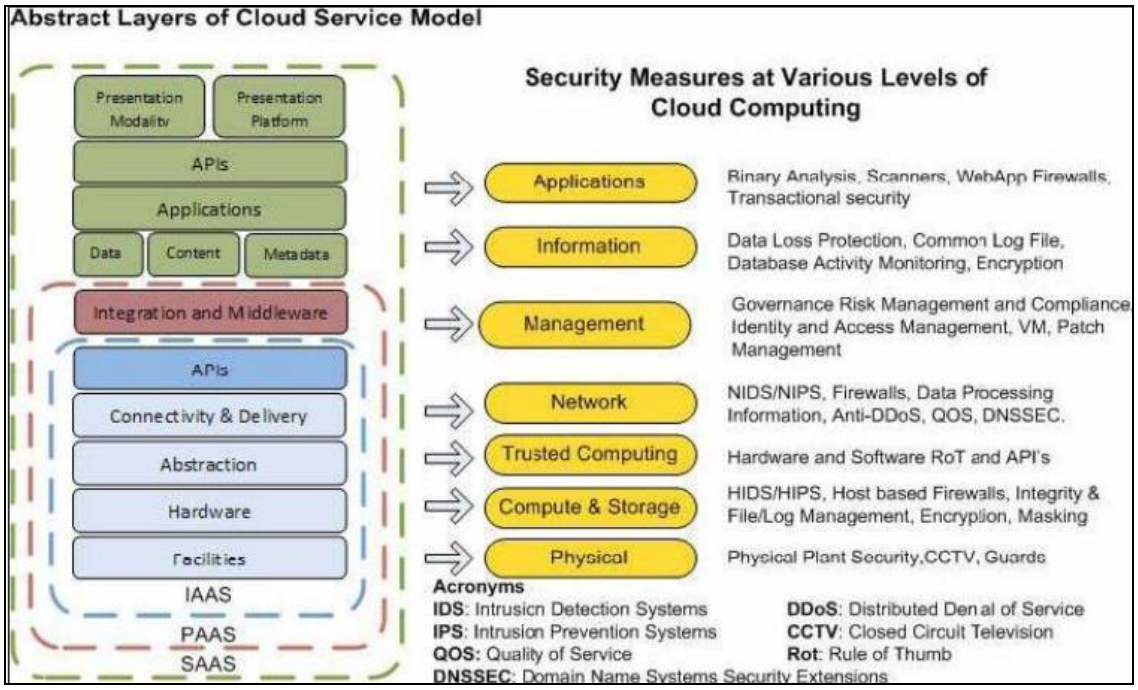

Fig 1: Cloud Service Models

Platform as a Service (PaaS)

Cloud users now have the option of building their apps on the provider's infrastructure platform or using the provider's application-designed interface, thanks to this feature. After then, the architecture of the cloud provider supported a programming language and its associated tools. The client just has authority over the applications that have been installed and the setup of the hosting environment for those applications; the supplier of cloud services handles the management and control of the cloud's infrastructure, which includes servers, networks, storage, and operating systems.

Infrastructure as a Service (IaaS)

Customers using the cloud infrastructure have access to this service. Customers of cloud providers have complete freedom to install and operate whatever operating system or applications they choose, while providers only provide the bare minimum of computer resources (network, storage, server, etc.). While cloud customer does not have management or control over the cloud infrastructure under the IaaS SLA, he does have some rights that let him manage and control aspects of storage, installed applications, operating systems, and limited control over networking component selection.

Security Problems in Cloud Computing

The term "cloud computing" refers to the practice of making available, over the internet, shared, elastic, and often virtualized computer resources. Users are not required to understand or be proficient in the underlying "cloud" technological architecture. We are seeing a sea shift in data storage and application operation due to cloud computing. Everything is moved to the "cloud"-a network of interconnected servers and computers that can be accessed over the Internet-rather than to any one desktop device. Common commercial applications are often made available online via cloud computing services; users access these applications using a web browser, and data and software are stored on servers connected to the Internet.

There are interoperability problems with cloud computing standardization efforts, and more importantly, there are security risks with cloud services, such as vulnerabilities and threats, which may occur with any SPI architecture. This subject will serve as the foundation of the literature study and will evaluate cloud computing security challenges, providing a basic summary of how vulnerabilities and threats are identified. Based on the focus of this research, a number of security holes have been discovered and classified. The army chief. The report analyses data gathered from the literature review and security, along with its correctness actions, to provide practical solutions to the identified gaps and issues, and it discusses relevant mitigations and security measurements to ensure homogeneity and prevent attacks. Integration of various APIs and interfaces into cloud services allows for dynamic resource allocation in response to input from systems and applications, as well as provisioning, management, self-services, and orchestrations. Whether you're using a public or private cloud, these factors affect the likelihood and compatibility of SPI models. Both lead to variations in availability, configuration, security, and control (Jaydip Sen, 2014) [8].

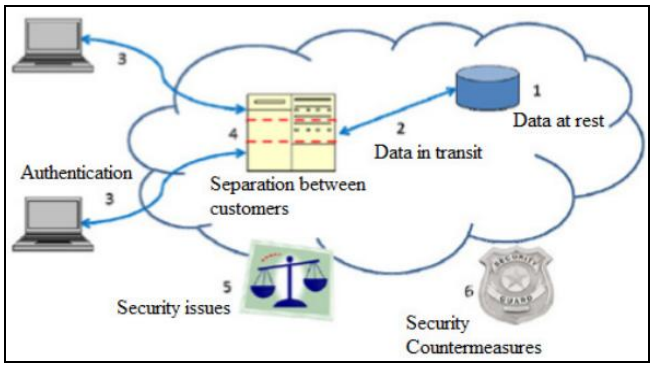

Fig 2: Areas of security concerns in cloud computing.

Security flaws and dangers that need countermeasures have received a lot of attention. As more and more businesses migrate to the cloud, the security risks and vulnerabilities that come with it are constantly evolving. There are new and diverse methods to exploit and manifest cloud service systems, applications, data, and content beyond the existing vectors in cloud computing.

Cloud Computing Vulnerabilities

The Open Group's risk taxonomy defines vulnerability as the likelihood that an asset may be susceptible to attack. A threat agent may cause an item to be vulnerable if the force they are applying is greater than the object's resistance to that force. This section enumerates the most significant vulnerabilities that are unique to the Cloud and pose a significant threat to cloud computing.

A vulnerability may be considered cloud-specific if it satisfies a number of requirements, as shown in the study. Some of the fundamental technologies of cloud computing include cryptography, virtualization, and service-oriented architecture. A vulnerability is considered cloud-specific if it affects these essential technologies often and fundamentally.

On the other side, some features of the cloud include elasticity, resource sharing, and a pay-as-you-go mode. When a vulnerability's origin lies in one of those traits, we say that it is cloud specific. The difficulty in adapting preexisting security measures to new cloud-based services is another factor that could identify a vulnerability as cloud-specific.

Their fourth criterion is that it must be common among top-tier, long-standing cloud providers. If you want to find security holes in the cloud, you need to know what makes them cloud unique.

- **Session Riding and Hijacking:** Hackers may take use of this vulnerability in online applications to execute malicious operations like session hijacking, where they utilize a valid session key to obtain unauthorized access to the computer systems of legitimate users. Meanwhile, session riding is the practice of sending instructions to a web application in order to fool the user into opening an email or visiting a malicious website that deletes the user's information.
- **Reliability and Availability of Service:** Taking this into account, cloud computing isn't ideal as many internet-based services and apps can stop functioning when the number of services built on top of the cloud infrastructure increases. As an example, the study uses a several-hour outage in 2008 that affected Amazon's Web Service cloud storage system. Problems with data loss and access were created by this.
- **Insecure Cryptography:** The insecurity of cryptography stems from the fact that adversaries always find new ways to crack it. It is usual practice to find vulnerabilities in cryptographic methods that render previously robust encryption insecure.

Conclusion

Technologists all around the world have taken an interest in cloud computing since it is one of the most powerful breakthroughs. The most significant benefit of cloud computing is the possibility it offers for cost savings to organisations. Other significant benefits include scalability, quick flexibility, measurable services, and more. The advent of cloud computing has been revolutionary for many types of businesses. Security risks and assaults on cloud computing networks are the primary focus of this study, which aims to fill a unique knowledge vacuum in the field. To accomplish our study goals, we have implemented a technique that involves conducting a survey by questionnaire and building algorithms as recommended solutions. This follows a thorough examination of the relevant literature.

The current knowledge gap on the security aspects of cloud computing is being filled by this research project. The research gap was identified and remedies were developed after a comprehensive review of fifty research publications. Three subareas were selected for further research: reasons for reluctance to embrace cloud technology, assaults on network security, and attacks on data security. The study's practical findings may be used to strengthen Cloud Computing's security measures. Our proposed solutions include algorithms, an analysis of the reasons people are hesitant to use cloud computing, and recommendations for best practices in this area. also, potential avenues for further study within the same domain.

References

1. Ouali, Sami. (2023). Cloud Computing Cyber Threats and Vulnerabilities. 10.4018/978-1-6684-8133-2.ch001.
2. Javaid, Adeel. (2013). Top Threats to Cloud Computing Security. SSRN Electronic Journal. 10.2139/ssrn.2325234.
3. Patil, Prerna. (2024). An Analysis of Emerging Cybersecurity Threats in Cloud Computing. Computer Fraud and Security. 84-91. 10.52710/cfs.64.
4. Bhadra, Sompurna & Publications, Research. (2020). CLOUD COMPUTING THREATS AND RISKS: UNCERTAINTY AND UNCONROLLABILITY IN THE RISK SOCETY. SSRN Electronic Journal. 7. 1047-1071.
5. Petre R. Communiquer le passé dans le présent: les jeunes voix parlent du communisme et des communistes en Roumanie. ESSACHESS-Journal for Communication Studies. 2012(02):269-287.
6. Ogigău-Neamţiu F. Cloud computing security issues. Journal of Defense Resources Management (JoDRM). 2012;3(2):141-148.
7. Singh S, Jangwal T. Cost breakdown of public cloud computing and private cloud computing and security issues. International Journal of Computer Science & Information Technology. 2012;4(2):17.
8. Singh D, Jaydip R. Management for carotid body tumors: A single center experience. Indian Journal of Vascular and Endovascular Surgery. 2014;1(1):8-11.