E-ISSN: 2583-9667
Indexed Journal
Peer Reviewed Journal
https://multiresearchjournal.theviews.in

Received: 02-04-2025
Accepted: 07-05-2025
Published: 04-07-2025

INTERNATIONAL JOURNAL OF ADVANCE RESEARCH IN MULTIDISCIPLINARY

Volume 3; Issue 3; 2025; Page No. 324-327

Security Threats, Attacks, And Mitigation Strategies in Cloud Computing: A Mixed-Method Study

[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.18263872

Corresponding Author: Abhishekh Samaiya

Abstract

Cloud computing is a cutting-edge method that provides pooled resources for managing servers and stock caches. By transforming technical solutions for enterprise-level systems into server-to-service frameworks, cloud computing helps any business save time and money on monitoring. Cloud computing, however, presents a host of new security risks and issues, as does any other technology. Various cloud models and services are the main topics of this work. The current state of cloud security is our next topic of discussion. Consideration of these security trends leads us to the next set of issues, which may include things like authentication, insufficient diligence, phishing, key exposure, auditing, privacy preservation, cloud-assisted Internet of Things applications, and data breaches. Based on the security trends and challenges, we then suggest attacks and responses tailored to the various cloud models. Finally, we highlight a few future prospects and consequences that are pertinent to cloud model security. Academic and business researchers will be able to use the future directions to their advantage as they strive to secure cloud computing.

Keywords: Cloud computing, security threats, security attacks

Introduction

Cloud computing has several advantages, such as lowering overall costs, pooling and combining computer resources, providing on-demand service, and being very flexible and scalable. Furthermore, internet-based services made possible by cloud computing have grown in popularity. Built on top of earlier iterations of computer technologies like virtualization, utility computing, and distributed computing, the cloud computing paradigm now offers enterprise-level applications the scalability and availability they need. It has a large physical resource pool and also provides services to virtual machines that are allocated to it. Online self-service, network accessibility, pooling of resources, high-speed resilience, and quantifiable services are the five essential characteristics of cloud computing. Large corporations are increasingly moving their IT operations to the cloud because of these advantages. Data security in the cloud is essential for dependable services. Data misuse, hostile insiders, unsecured interfaces and access points, shared technical issues, data loss, and hijacking are some of the common cloud hazards that cloud computing encounters. So, to successfully utilise cloud computing, one must have an accurate grasp of cloud security.

Safeguarding data, programs, and hardware in the cloud is what cloud security is all about. Any company may benefit from many of the same security measures in public, private, or hybrid cloud settings. The term "cloud security" refers to an all-encompassing set of measures used to protect data and the infrastructure supporting cloud computing. The whole reliance on cloud computing to safeguard data is unsettling for many business and research groups. Cybercriminals target both on-premises and cloud-based information technology systems. Cloud security, like that of any computer environment, requires sufficient safeguards. As a result, both the data and the network are secure, and they can detect and respond to any anomalous activity quickly. To prevent unauthorized access or disruptions, cloud security must be up-to-date and effective. In order to overcome the difficulties and concerns associated with the cloud, service providers must ensure the reliability and

security of their customers' data and resources. When designing multi-tenant infrastructures, cloud providers should keep tenant data separate. Verifying the dangers of outsourcing data is the first step in developing a solid model for use in the cloud. This can only be accomplished by sorting the data according to the risks associated with it.

Literature Review

Mozumder, Deba Prasead *et al*. (2017) [1]. By providing a robust computing platform, cloud solutions empower individuals and organisations to carry out a wide range of tasks, including; using an online storage system; adopting business applications; developing specialized software; and establishing a functional network environment. A tremendous amount of data has been stored in cloud computing settings, and the number of individuals utilising cloud services has skyrocketed in recent years. Because hackers are always looking for new methods to attack security holes in the cloud's architecture, the number of data breaches involving cloud services is likewise rising annually.

Tank, Darshan *et al*. (2020) [2]. Every year, new forms of cybercrime and risks emerge. No company is safe from cybercriminals, no matter how big or little. Any business worth its salt in today's interconnected world must prioritise cybersecurity. Most susceptible data and computations are the targets of side-channel attacks (SCA), one of the recognized security dangers in a virtualization system. Major security interests are being bolstered by SCA, which calls for a fresh perspective. Protecting the cloud computing environment as a whole requires careful virtualization infrastructure deployment, which is a subset of cybersecurity.

Dahbur, Kamal *et al*. (2011) [3]. The way information technology services are used is being transformed by cloud computing (CC). Reduced capital expenses and ease from maintaining complicated IT infrastructure are only two of the many appealing promises that CC is being pushed and presented with, drawing in many enterprises and managers worldwide. But there are hazards and security problems that need to be thought about and handled properly, just as there are desired advantages. This article presents a comprehensive overview of the security concerns raised by the "cloud" and organizes them into several categories. It then goes on to examine the risks, threats, and vulnerabilities connected with cloud computing and offers solutions to assist promote its advantages while mitigating its hazards.

El Kafhali, Said *et al*. (2022) [4]. In order to handle and store more data, emerging technologies like 5G Internet, the Internet of Things (IoT), and smart cities rely on cloud computing services. As a result, the cloud paradigm will face several security risks due to the diversity of the new businesses that have adopted these technologies. At now, every part of cloud computing is included, including users, networks, access control, and infrastructures. The security community has a hard time with issues like data duplication, slow threat identification, losing control over data access and protection, and meeting regulatory requirements when they don't have a clear picture of the cloud architecture.

Research Methodology

Research Design: The research methodology design is the most crucial aspect of the study in order to attain the research goals. Our study technique is based on our goals, which were refined following a thorough literature analysis. There has been much discussion in this chapter on the study's issue statement, objectives, methodology, techniques, data sources, questionnaire design, and intended participants. doing a literature search to find research on cloud computing information security risks. We also made advantage of SLR to pick out existing security metric identification frameworks. For SLR, we mostly relied on the internet citation databases Scopus and Engineering Village. We established inclusion and exclusion criteria that were used to select the studies. Using predetermined criteria, a suitable framework was chosen. We discovered SLA-based cloud information security metrics by analysing the chosen framework and conceptualizing the COBIT framework.

Secondary Data through Literature Review

An essential and important part of every research project is the literature review, which is used to analyse secondary data. It is simple to identify and assess the issue after reviewing the publicly accessible secondary material, such as research papers, articles, books, and anything else pertaining to our study field. We can provide a sense of previous work in the topic and how ours differs by examining secondary sources of information.

Primary Data through Survey Questionnaire

One of the ways that data is gathered is by use of a survey questionnaire, which is a main data collecting technique based on easy sampling. To find out how many people in the IT, education, government, and non-IT sectors in the NCR understand cloud computing, how many have used it, and what their biggest worries are about it, we ran an online poll. Our questionnaire consists of eleven questions; the first four concern the company's or consumer's personal information, while the remaining questions pertain to our goal of using cloud computing.

Sources Used for Data Collection

In order to gather information, surveys and literature reviews are used. To begin, literature research was carried out in order to have a better understanding of the cloud computing issues and to explain them. The plan for gathering data was based on the literature study. It makes use of both primary and secondary sources of information.

Secondary data

Secondary data consists of information gathered from previously published sources, such as books, journals, research papers, articles, and newspapers. This method of data collecting is the easiest. Saving time and providing access to bigger, higher-quality datasets that would be difficult for a single researcher to amass via primary data collection are further benefits of secondary data analysis.

Primary Data

Researchers use methods such as questionnaires, market

research, and experiments to gather primary data from respondents in order to accomplish their objectives. It is often done after the researcher has gotten a better understanding of the difficulties from reviewing secondary data or analysing primary data that has already been acquired by another researcher.

Analysis

Data Security Attacks

When it comes to protecting sensitive information from common cyberattacks, data security is a hotly debated topic. If data processing takes place in publicly accessible cloud services, various privacy, security, and confidentiality standards may apply. Better security measures to safeguard data in a cloud computing environment must be put in place once all potential security risks and assaults have been identified.

While there are many potential dangers to cloud data, we are just focussing on assaults that might compromise web apps. Cybercriminals launch assaults on the web in order to take advantage of security holes in Web 2.0, the underlying technology that makes SaaS possible in the cloud.

SQL Injection Attack

In order to execute SQL injection, software security holes must be exploited. Hackers aim for SQL servers running susceptible database applications, so they may bypass authentication and get unauthorized access to the database by exploiting web-server vulnerabilities and injecting malicious code. Typically, botnets-which are private networked infected computers-also known as zombie armies-are the ones that begin it. If the hacker succeeds, they will be able to remotely run system commands, access sensitive data, change database contents, and even take over the web server. An SQL injection attack is launched by means of botnets, which consist of thousands of bots that have been outfitted with an injection kit.

Worldwide, millions of URLs on various websites have been compromised by botnets that inject SQL. Using software as a service (SaaS) application, merchants in the cloud host their items and sell them online. Three further types of SQL injection exist.

Inference or Blind SQL injection

DBMS-specific

Compounded SQLI

- SQL injection + insufficient authentication
- SQL injection + DDoS attacks
- SQL injection + DNS hijacking
- SQL injection + XSS

Cross-site scripting (XSS) Attack

This sort of exploitation is a potent effort at phishing, a dishonest method of acquiring sensitive information. Typically, this kind of attack gathers data by means of a hyperlink that includes harmful material. After the web app has gathered the user's information, it will provide an output page that mimics the website's legitimate content while actually including the harmful data that was initially given to it.

Cloud Adoption

We offered five possible answers to this topic to the IT industry. We observed that 61% of industrialists chose "Cloud Computing is A type of outsourcing of IT," 28% find it a fascinating technology, 8% find it an unknown or ambiguous issue, and 2% feel it's something else entirely.

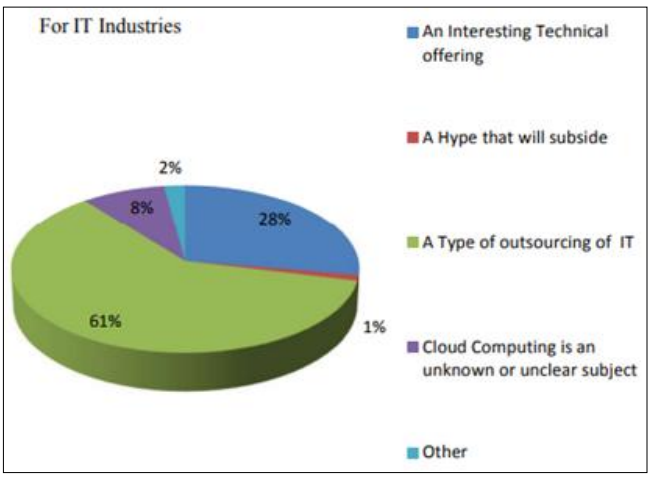

Fig 1: Cloud Computing Understanding (IT)

What does Cloud Computing primarily mean to your organization (EDUCATION industry)?

We polled the education industry's upper and middle management, including directors, teachers, and IT staff, with this question. Our research shows that among educators, 42% think "Cloud Computing is an unknown or unclear subject," 29% see it as "An Interesting Technical offering," 13% see it as "a hype that will subside," 12% see it as "a type of outsourcing of IT," and 4% think it's something else entirely.

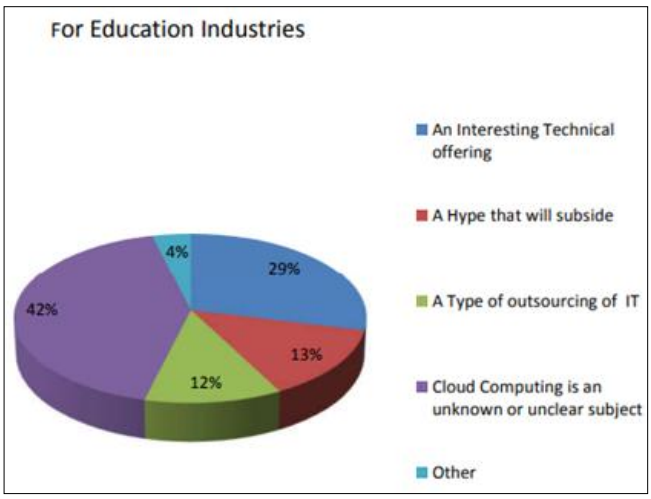

Fig 2: Cloud Computing Understanding (Education)

Q1. What does Cloud Computing primarily mean to your organization (EDUCATION industry)?

We polled the education industry's upper and middle management, including directors, teachers, and IT staff, with this question. Our research shows that among educators, 42% think "Cloud Computing is an unknown or

unclear subject," 29% see it as "An Interesting Technical offering," 13% see it as "a hype that will subside," 12% see it as "a type of outsourcing of IT," and 4% think it's something else entirely.

Conclusion

In addition to extensive research on computing as a whole, the literature evaluation uncovered a number of security threat concerns, often known as vulnerabilities, in cloud computing networks. The vast variety of vulnerabilities inherent in any type of cloud computing system is the root cause of the majority of cloud computing security issues, as we discovered when we reviewed the literature and narrowed the research gap to three main areas. Organisations are hesitant to embrace cloud computing for a variety of reasons, including the lack of trustworthy security regulations. Attacks and security risks to cloud systems are the primary focus of our research. Network security assaults, data security attacks, and the reasons for people's reluctance to embrace cloud technology are three of the numerous security dangers that we've identified.

Security breaches in cloud networks are the primary focus of our first subcategory. The two most common types of attacks that fall under this category are man-in-the-middle and denial-of-service attacks. After doing additional research into DoS (Denial of Service) attacks, we discovered that distributed denial of service (DDoS) attacks needs greater effort from the attacker in order to reduce resource depletion. To that end, we have developed a DDoS avoidance algorithm that makes use of a three-filter approach. It is a tried-and-true method for protecting and keeping tabs on cloud networks against DDoS attacks.

Security breaches in cloud systems constitute our second subcategory. Malware injection attacks, which may take two forms-the SQL-injection assault and the XSS (Cross Site Scripting) attack on cloud systems-are the most prevalent and noticeable data security threats to web-based applications, according to our study. on an effort to fill this knowledge vacuum, we have proposed mitigation strategies grounded on data security best practices to fend against malware injection assaults.

Cloud services should only be used by organisations when they prove to be cost-effective. Cloud computing is a branch of IT that is growing at a fast pace. Cloud computing is being considered by many firms as a practical and economical solution for their company's computer needs. Cloud computing has already won the trust of several companies concerned about the security of their sensitive data. Furthermore, several issues exist, which makes individuals wary about using cloud computing. Data processing and storage outside of the customer's control raises privacy, security, and legal problems. Further complicating matters is the absence of a criteria for evaluating the SLA. To that end, this study set out to investigate the potential of SLA metrics for bolstering cloud data protection. This study found that cloud computing is just as vulnerable to security breaches as traditional data centers.

References

1. Mozumder DP, Nayeen Mahi MJ, Whaiduzzaman M. Cloud computing security breaches and threats analysis. International Journal of Scientific and Engineering Research. 2017;8:1287–1297.
2. Tank D, Aggarwal A, Chaubey N. Cyber security aspects of virtualization in cloud computing environments: analyzing virtualization-specific cyber security risks. In: Handbook of Research on Cloud Computing and Big Data Applications. Hershey (PA): IGI Global; c2020. doi:10.4018/978-1-7998-2253-0.ch013.
3. Dahbur K, Mohammad B, Tarakji A. A survey of risks, threats and vulnerabilities in cloud computing. Proceedings of the ACM Conference on Data and Application Security and Privacy. 2011;12:1–8. doi:10.1145/1980822.1980834.
4. El Kafhali S, El Mir I, Hanini M. Security threats, defense mechanisms, challenges, and future directions in cloud computing. Archives of Computational Methods in Engineering. 2022;29:223–246. doi:10.1007/s11831-021-09573-y.
5. Hatwar SV, Chavan R. Cloud computing security aspects, vulnerabilities and countermeasures. International Journal of Computer Applications. 2015;119:46–53. doi:10.5120/21163-4218.