International Journal of Advances in Engineering and Management (IJAEM)
Volume 7, Issue 07 July 2025, pp: 217-223 www.ijaem.net ISSN: 2395-5252

Cyber Security in Cloud Computing

Fatima Muntaqa Tijjani Usman, A. Senthil Kumar, Olufemi Ayinde Foloronso

School of Science and Information Technology, Skyline University Nigeria, Kano, Nigeria
School of Science and Information Technology, Skyline University Nigeria, Kano, Nigeria
School of Science and Information Technology, Skyline University Nigeria, Kano, Nigeria

Date of Submission: 01-07-2025 Date of Acceptance: 10-07-2025

ABSTRACT
Cloud computing cybersecurity must be offered by the elements that make up its structure. Accurately identifying the hazards associated with this technology is the first step towards improving its cybersecurity. This research proposes a new cybersecurity reference model for the cloud system, which is composed of parts that constitute different cloud computing layers. The virtualization and service layers, as well as other crucial elements for ensuring cloud computing cybersecurity, are not thoroughly covered by the reference models of cloud computing security that are currently available. Additionally, the social media IoT sensor layer, which gathers text data entered by attackers to launch cyberattacks on cloud infrastructure, and the cloud computing's cyber resilience issues are not taken into account. Furthermore, this study investigates cloud computing service models' cybersecurity concerns and builds an attack model to safeguard cloud systems. It provides an understanding of laws and standards about cloud computing cybersecurity. Clarification of cloud system cybersecurity and cyber resilience concepts is given by security aspects. Intelligent cloud systems' cyber resilience architecture is designed. The proposed cyber resilience model has an advantage over the existing one in that it identifies the cloud computing's information security and cybersecurity elements and combines them to build the cloud systems' cyber resilience aspects.

Keywords— Cloud computing, cyber security, cyber resilience, cyberattack model, SaaS, PaaS, and IaaS

I. INTRODUCTION

Eric Schmidt, an executive of Google, coined the phrase "cloud computing" for the first time in late 2006. As of right now, cloud computing is regarded as the most inventive technology in developed nations and is one of the key elements of the fourth industrial revolution [1]. Cloud computing's cybersecurity concerns extend to individual parts of its intricate architecture [2]. Special information processing methods are included in cloud computing content, where customers can choose how the computer system's resources are used as an Internet service. One characteristic of cloud computing is that its fundamental structure is concealed from users, and its resources are dynamic. The physical environment for data storage, the virtual environment the hypervisor creates, and the services offered to users are the major components of the cloud system. Cybersecurity risks may impact each of the cloud computing components in this list [3]. The complexity of security challenges is increased by the multiplicity of components that comprise the cloud paradigm, including the network, hardware, architecture, and application software interface. This results in insecurity flaws that are caused by different cloud element combinations for both the cloud provider and its client [4]. The creation of a conceptual model is the first step required to give cloud computing's cybersecurity a sophisticated structure [5].

The physical environment for data storage, the virtual environment the hypervisor creates, and the services offered to users are the major components of the cloud system. Cybersecurity risks may impact each of the cloud computing components in this list [3]. The complexity of security challenges is increased by the multiplicity of components that comprise the cloud paradigm, including the network, hardware, architecture, and application software interface. This results in security flaws that are caused by different cloud element combinations for both the cloud provider and its client [4]. The creation of a conceptual model is the first step required to give cloud computing's cybersecurity a sophisticated structure [5].

International Journal of Advances in Engineering and Management (IJAEM)
Volume 7, Issue 07 July 2025, pp: 217-223 www.ijaem.net ISSN: 2395-5252

II. LITERATURE REVIEW

The paper's structure is arranged as follows: The architecture of the suggested cybersecurity reference model for the intelligent cloud computing system is shown in Section 2. In Section 3, the created cyberattack model for cloud systems is described, and the cybersecurity concerns of cloud computing service delivery methods are discussed. The security guidelines and relevant laws are introduced in Section 4 on cloud computing. The hazards to information security, cloud computing system vulnerabilities, and cyber threats are covered in Section 5. The security and cyber resilience features of cloud computing are described in Section 6. Common architectures for cybersecurity and cyber resilience in intelligent cloud computing systems are provided in Section 5. The study's contribution and findings are compiled in Section 6.

III. RESEARCH METHODOLOGY

It is necessary to first outline the architecture of the cloud system in order to guarantee the cybersecurity of cloud computing. In this context, major institutions like Microsoft, IBM, and NIST offer reference models for cloud computing. The five key participants in the standard model of cloud computing information systems are the cloud client, cloud provider, cloud auditor, cloud auditor, and cloud broker, according to the NIST organization [6]. Layers named Orchestration, Service, Resource abstraction and management, Physical resources, cloud service administration, and security make up the NIST reference model. Here, the following concerns are taken into account for the cloud computing system's security:
Verification and approval of clients using cloud services.
Resources are assigned and allocated for node recovery, updates, and connections.
Surveillance of digital assets
Tracking cloud activity and providing performance reports.
Choosing the service level agreement's (SLA) parameters.
Observing the SLA's execution by the established security policy.

IBM has put up another cloud computing reference model [7]. Three roles characterise the cloud computing system, according to IBM's reference model: customer, operator, and cloud service creator. Individual entities, groupings of entities, or organizations can carry out these roles. This architecture covers the physical infrastructure, cloud services, and cloud management platform while taking performance, security, and resilience to failures into common consideration.

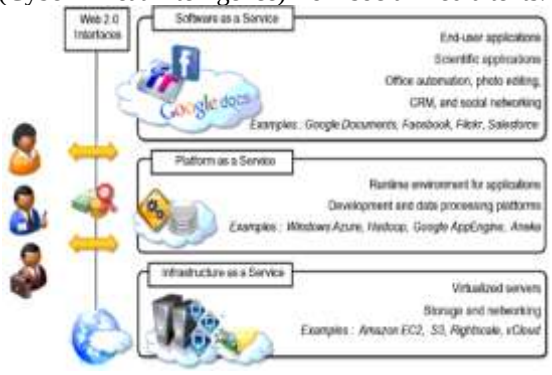
Existing reference models for cloud computing security do not account for the social media IoT (Internet of Things) sensor layer, which gathers text data typed by attackers to launch cyberattacks on the cloud infrastructure, or the cyber resilience issues associated with cloud computing. They also do not describe the virtualization and service layers and the critical components for providing the cybersecurity of cloud computing in detail. Regarding this, the study that is being presented suggests a new cloud computing system's security reference model that consists of elements that make up each cloud computing layer. The following is a representation of the new model.

The cloud consumer and the cloud operator are the two primary subjects of the suggested cloud computing system paradigm. The application layer, service layer, virtualization layer, data transmission layer, physical resources layer, Internet of Things social media sensor layer, cyber security layer, and cyber resilience layer make up this concept. In the context of the suggested cloud computing system model, the following

Concerns are considered regarding security:
Defect identification

The following are some of the key areas of focus:

- Sensitive Data Privacy.
- Cyberattack Clustering.
- Identity Management.
- Trust Management.
- Anomaly Detection.
- Task Scheduling.
- Risk Assessment.
- Cloud Security Monitoring.
- Identification of cyber threats and CTI data (Cyber Threat Intelligence) from social media texts.

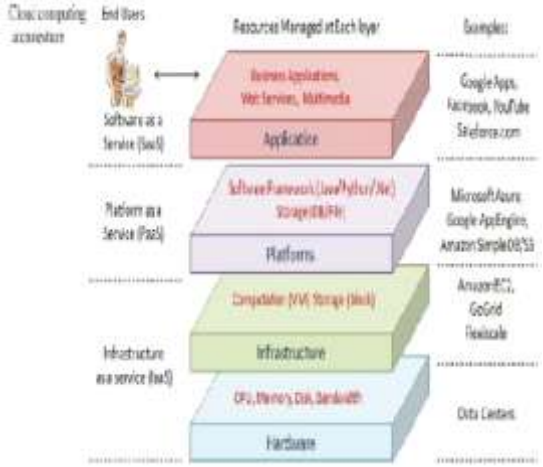


International Journal of Advances in Engineering and Management (IJAEM)
Volume 7, Issue 07 July 2025, pp: 217-223 www.ijaem.net ISSN: 2395-5252

IV. CYBERSECURITY VULNERABILITIES IN CLOUD COMPUTING SYSTEMS' SERVICE DELIVERY MODELS

Three service models are used by cloud computing to offer users a variety of services. Customers can access application platforms, infrastructure resources, and software resources as a service through cloud computing's SaaS (Software as a Service), PaaS (Platform as a Service), and IaaS (Infrastructure as a Service) service models. Different security requirements are placed on the cloud environment by each service model.

The lowest fundamental tier of the cloud computing service model stack is called Infrastructure as a Service (IaaS). According to [8] (Fig. 2), the SaaS model is positioned at the top layer of the PaaS model, which is positioned above the IaaS model.



The four tiers of the cloud computing architecture are depicted in Fig. 2: application layer, platform layer, infrastructure layer, and hardware layer. These strata are arranged over one another. Every layer is constructed using the loosely coupled approach with the layers that come before and after it. Each layer is allowed to operate independently because of this characteristic.

Layer of Hardware. The cloud's physical resources are managed by this tier. Physical servers, routers, switches, power, and cooling systems are some examples of these resources.

Layer of Infrastructure. The virtualization layer is another name for this layer. This layer's job is to use virtualization technologies to build a pool of compute and storage resources.

Layer of the Platform. The infrastructure layer is the one above this one. Operating systems are included in this tier.

layer of applications. Compared to typical apps, the cloud's application layer is different. Auto-scalability in cloud applications allows for cost-effective performance and increased availability.

Certain security-related problems with the service models fall under the purview of the cloud providers, while other issues are the responsibility of the cloud users.

- **Problems with security in the SaaS model**

The SaaS model stores each customer's data in the data center of the SaaS provider next to the data of other customers. To ensure availability, the cloud provider also replicates data to several sites across international borders. Businesses in conventional information systems are aware of data storage guidelines. Nonetheless, there are serious security problems because users are unaware of the guidelines for storing and safeguarding their data in the SaaS model. Here, the introduction of issues like accessibility, software program vulnerabilities, and data leaking causes harm that is both financially and legally significant.

The supplier bears full responsibility for cloud security management under the SaaS model. Apps are the resources that SaaS offers. To create the ideal SaaS model, the following security concerns should be investigated in detail: Data leakage, virtualization vulnerabilities, data security, network security, colocation, data integrity, data segregation, data access control, authentication and authorization, and data secrecy.

- **Security issues of the PaaS layer**

Web application security, data leakage, data security, colocation, data integrity, data segregation, data access control, authentication and authorization, data secrecy, and virtualization vulnerabilities are some examples of data security and network security.

- **Security issues of the IaaS layer**

Users are granted authority over security management through the IaaS layer. The provider's and the customer's security obligations differ greatly depending on the service model. Elastic Compute Cloud, or EC2, is an infrastructure solution from Amazon that gives the provider protection up to the hypervisor. Providers are limited to managing virtualization, environmental, and physical security in this instance. In turn, the client has the power to handle security-related issues pertaining to the data, operating system, apps, and IT system.

Attacks directed at cloud systems include:

Zombie attack. By using the Internet to make requests from innocuous hosts on the network, an

International Journal of Advances in Engineering and Management (IJAEM)
Volume 7, Issue 07 July 2025, pp: 217-223 www.ijaem.net ISSN: 2395-5252

attacker attempts to overwhelm the target object. We refer to these hosts as zombies. Any user can request access to cloud-based virtual machines (VMs) via the Internet. Zombies allow an attacker to send several queries. By influencing the accessibility of cloud services, this kind of assault impairs cloud performance. Here, the servers are the target of DoS or DDoS (Distributed Denial of Service) assaults since the cloud is overworked and unable to handle the volume of requests.

Service injection attack. The attacker tries to inject a malicious service or a new virtual machine into the cloud system and initiates providing malicious services to users. Malware affects cloud services by altering or blocking cloud functions. Here, an attacker creates a malicious service, such as a SaaS, PaaS, or IaaS, and adds it to the cloud system. In this case, genuine user requests are automatically redirected to malicious services, and as a result, malicious services begin to be provided to the user.

Virtual machine bypassing. Through this attack, the isolation layer is broken by the attacker's programme operating in the virtual machine (VM), which also has access to the hypervisor's privileges. An attacker can now speak with the hypervisor directly thanks to this.

At the virtual layer, VM bypass from isolation takes place. An attacker can access additional virtual machines (VMs) running on the physical machine as well as the host operating system by using VM Escape.

Rootkit in the hypervisor. Rootkits for virtual machines (VMs) compel the hypervisor to infect the host OS. In order to execute unauthorised code on the system, the hypervisor further establishes a covert channel. This gives an attacker the ability to take over and alter any virtual machine (VM) that is operating on the host computer.

Man in the middle assault. Any attacker can access the data shared between the two parties if the SSL (Secure Socket Layer) is not configured appropriately. An attacker can access data center-to-data center communications in the cloud.

Spoofing metadata. The attacker alters the file that contains details about the service sample in this kind of attack.

Phishing attack. In order to obtain sensitive data, this attack attempts to alter a web connection and reroute the user to an incorrect link. By setting up a phishing attack website on a cloud service, an attacker gains access to other users' accounts or services.

Back door channel attack. The compromised machine can be accessed remotely thanks to this exploit. Hackers can take control of the target's resources and transform them into zombies in order to launch a DDoS assault by utilising backdoor channels.

Attacks of Deception. Industrial companies are moving their management systems to the cloud because it is more efficient with storage and processing resources. [6] creates a neural network-based method to identify Deception Attacks that are directed at cloud-based industrial control systems' actuator signals. Deception Attacks aim to intentionally modify the delivered data to undermine the integrity of the control signal [5].

Attacks that deny service. This kind of attack aims to overload a system, application, or network with too many connections, requests, or traffic for it to handle. A method for estimating the status of nonlinear systems impacted by a denial-of-service attack and ambiguous input data is presented in [3].

Security guidelines and laws about cloud computing

Many cloud standards have had to be developed in this industry due to the extensive use of cloud computing.

The ISO 2700x series of standards, SSAE 16, and ISAE 3402 principles are used to determine whether the providers have a suitable governance structure in place. The following can be ascertained using the ISO 2700x standard:

- protection of the client assets from unauthorized access by provider staff.
- protection of the client assets from intentional or unintentional access by client partners or employees.
- guarantee that the client's applications and data will be isolated in a shared, multi-tenant environment.

V. ANALYSIS AND SYSTEMATIZATION OF CYBER THREATS TO CLOUD SYSTEMS

Information security risks in cloud computing

Risk is a statistical measure of the likelihood that a threat would exploit an object's vulnerability to harm the organization [7]. The ratio of the likelihood of an accident occurring to the harm it causes is how the organization calculates risk. Two higher-level risk variables [7] are used by many standardization organizations to evaluate risk: the likelihood of a damaging accident occurring (frequency of damage) and the impact of that accident (magnitude of potential damage). The magnitude of the likely loss influences the detrimental event's expenses. When a threat agent effectively takes advantage of a vulnerability, a loss event takes place. This event's likelihood is determined by two things:

International Journal of Advances in Engineering and Management (IJAEM)
Volume 7, Issue 07 July 2025, pp: 217-223 www.ijaem.net ISSN: 2395-5252

(1) How frequently does the danger agent try to take advantage of the weakness. The number of contacts an agent has to attack a target is called its frequency.
(2) The distinction between the threat agent's ability to attack and the system's ability to fend off an attack. The following are concerns about information security in cloud computing:

Insufficient supervision. Customers lose control over their data when they transfer it to a cloud hosted by the provider; additionally, they are unable to implement any organisational or technical safeguards that would guarantee the data's availability, completeness, confidentiality, transparency, isolation, compliance, and protection against intrusion.

Insufficient clarity. Inadequate transparency in cloud service operations puts controllers at risk while processing data. Data entities are likewise seriously threatened by this circumstance. They are unable to recognize the prerequisites since they are ignorant of the hazards and the threats. The controller may face risks if personal data is processed in different geographic locations.

Hazards to systems in the cloud

A threat is a circumstance or an occurrence that has the potential to harm an organization's operations, resources, people, or country by granting unauthorized access to information systems [3]. Cloud computing exposes customers and cloud service providers to various security risks. These security dangers are becoming more and more varied [2]. Since 2010, the CSA organization has released a list of dangers to cloud security. As stated in the CSA's 2016 list, organizations could encounter the following 12 threats when implementing cloud computing [3]:

Data leaking. Unauthorized parties now have a chance to get sensitive information because of this threat.

Inadequate access control, credentials, and identification. An attacker obtains unauthorized access to data by pretending to be a legitimate user.

An application programming interface that isn't secure. Resource allocation is managed by application programming interfaces, which are made available to cloud clients. Attackers can take advantage of the cloud environment using these interfaces. Web services provide the basis of these APIs' design. Web services are not immune to attacks.

Vulnerabilities in systems and applications. This hazard manifests as a result of systemic flaws. All services and data are susceptible to security risks due to flaws in the kernel program, application tools, and operating system libraries.

Account hijacking. This is a traditional type of threat that is also relevant to any computer system and cloud computing. This threat allows gaining access to the system by capturing the credentials and password of the genuine user. In the cloud, when attackers take over a user's account, they can redirect users to illegitimate sites, manipulate data, provide false information, and track transactions.

Malicious insiders. A current or former employee or any business partner with authorized access to an information system is considered a malicious insider if they intentionally abuse that access to violate the security and privacy aspects of the information system.

Advanced Persistent Threats, or APT. APTs are an advanced kind of attack with a particular objective and target in mind. It is quite challenging to identify these attacks because they adapt to the security measures that have been put in place.

Data loss. This risk encompasses instances of data loss resulting from not just cyberattacks but also from inadvertent deletion, unforeseen harm, and natural calamities (such as fire, earthquake, or flood).

Inadequate research and analysis. It entails assessing prospective cloud computing users to ascertain whether cloud service providers adhere to different regulations. Security hazards arise as a result of this operation's inadequate execution.

Harmful and nefarious use of cloud computing resources. Poor cloud protection and unregistered, mishandled, fraudulent, free user accounts are the causes of this issue. These conditions provide attackers access to computer resources, which they can then misuse to target things. Abuse of cloud services can take many forms, such as using the cloud to execute DDoS attacks, send spam and phishing emails, acquire digital currencies, commit large-scale click fraud, employ brute force assaults against databases of stolen identities, and host dangerous and pirated material.

A Breakdown in Service. makes it impossible for authorized users to access their data because cloud resources are unavailable. The attacker coerces the target cloud service to consume a larger portion of the allotted resources, which slows down the system and keeps legitimate customers from using it.

Technology Shared. One of the main aspects of cloud computing that applies to all three service types is shared technology. In a multi-user

International Journal of Advances in Engineering and Management (IJAEM)
Volume 7, Issue 07 July 2025, pp: 217-223 www.ijaem.net ISSN: 2395-5252

environment, when multiple users' applications are located in one area, the components that allow for the shared use of technologies are not thought to guarantee isolation. Vulnerability in shared technologies results from a lack of isolation. Take the hypervisor vulnerability, for instance.

Furthermore, cloud computing has been linked to issues related to service outsourcing, regulatory compliance, data placement, shared environments, business continuity, disaster recovery, hard environments for looking into illicit activities, and long-term viability [3]. The primary causes of data confidentiality violations are the resource sharing and multi-tenancy capabilities of the cloud, which give rise to the concerns mentioned above [3].

Threats and issues that target services include misconfigurations, targeted attacks, etc. [3]. Every one of the three cloud computing tiers is susceptible to these dangers. The IaaS layer can only be affected by ordinary technological threats, but the PaaS and SaaS layers can be affected by malicious cloud computing use.

Cloud system vulnerabilities. A threat source can exploit a vulnerability in an information system, security protocols, or internal control mechanisms [4]. The likelihood that an object will be unable to withstand the acts of a danger agent is known as vulnerability. When there is a difference between the strength of the threat agent and the resistance of the object to this strength, it can be assumed that a vulnerability already exists. For this reason, a vulnerability must be defined as being resilient against some type of attack.

Additionally, there is the idea of computer vulnerability. These are security-related errors. Buffer overflow is a vulnerability that reduces the system's resistance to code execution. Depending on his skills, an attacker may use this vulnerability in a variety of ways. These flaws include:

- Vulnerabilities in Internet protocols;
- Application and interface flaws;
- Platform flaws;
- Infrastructure deficiencies, unauthorized access to the management interface

The vulnerabilities include injection weaknesses, web browser, and application programming interface flaws.

Finding Anomalies. The memory and CPU resources of the cloud infrastructure servers exhibit unusual behavior as a result of a variety of events that transpire in the cloud environment. This module develops a classifier ensemble-based semi-supervised technique for identifying anomalies in cloud infrastructure performance metrics. [7]. For anomaly clustering, an optimisation technique with many criteria is created.

Monitoring of Cloud Security. The practice of assessing, quantifying, and controlling workloads in the cloud to predetermined metrics and thresholds is known as cloud monitoring. Cloud monitoring assesses if cloud services are meeting service level agreements (SLAs), finds security vulnerabilities, pinpoints issues with quality indicators, and does cost analysis [4]. The QoS indicators listed in the SLA are used to monitor cloud systems [5]. Numerous factors, including response time, speed, accessibility, and availability, affect cloud service quality of experience metrics [6]. Accurate real-time information about the operational resources (components) of PaaS, SaaS, and IaaS services can be obtained through regular monitoring of QoS attributes [7].

VI. CONCLUSION

The reference models for cloud system cybersecurity and cyber resilience were presented in this research. The primary elements of the suggested model were the focus of a taxonomy of attacks, and their objectives were deciphered. We examined the dangers, weaknesses, and possibilities associated with cloud computing. Intelligent cloud systems now share a common architecture for cybersecurity and cyber resilience. The distinct countermeasure to counter cyberattacks comprised the functional components of the architecture. Because these were intended to be independent clouds, the intelligent cloud system was able to bounce back from unforeseen failures. The benefit of this strategy was that the virtualization layer and services—the two key elements required to guarantee cloud computing's cybersecurity—were not included in the reference models that were already in place. Apart from the Internet of Things sensor layer for social media, which gathers text input entered by attackers to initiate cyberattacks on cloud infrastructure, cloud computing's cyber resilience challenges were not considered at all. Future research will focus on creating software for "Everything as a Service" models that will guarantee the cyber resilience of intelligent cloud systems. Deep learning-based techniques for detecting SLA violations in the system will be developed to effectively monitor the cybersecurity of cloud services.

REFERENCES

[1]. Onik MH, Kim CS, Yang J. Personal data privacy challenges of the fourth industrial revolution. In: Proc. of the international conference on advanced communications technology, ICACT. 2019, p. 635–8. http://dx.doi.org/10.23919/ICACT.2019.8701932.

[2]. Nita SL, Mihailescu MI. On artificial neural network used in cloud computing security – a survey. In: Proc. of the IEEE 10th international conference on electronics, computers and artificial intelligence. ECAI, 2018, p. 1–6. http://dx.doi.org/10.1109/ECAI.2018.8679086.

[3]. Parast FK, Sindhav C, Nikam S, Yekta HI, Kent KB, Hakak S. Cloud computing security: A survey of service-based models. Comput Secur 2022;114:1–4. http://dx.doi.org/10.1016/j.cose.2021.102580.

[4]. Ghobaei-Arani M, Jabbehdari S, Pourmina MA. An autonomic resource provisioning approach for service-based cloud applications: A hybrid approach. Future Gener Comput Syst 2018;78(1):191– 210. http://dx.doi.org/10.1016/j.future.2017.02.022.

[5]. Alguliev RM, Abdullayeva FC. Identity management based security architecture of cloud computing on multi-agent systems. In: Proc. of the IEEE third international conference on innovative computing technology, INTECH. London, UK; 2013, p. 123–6. http://dx.doi.org/10.1109/INTECH.2013.6653643.

[6]. NIST cloudcomputing reference architecture. SP. 500-292, Recommendations of the National Institute of Standards and Technology; 2011, p. 35.

[7]. IBM cloud computing reference architecture overview. 2012, p. 42.

[8]. Almorsy M, Grundy J, Müller I. An analysis of the cloud computing security problem.2016, p. 1–6. http://dx.doi.org/10.48550/arXiv.1609.01107.