Enhanced Security for Protecting Data in Cloud using Layered Approach

Nwankwo, U. C[1](OCID 0000-0002-9536-6472), Ugochukwu, E.C[2], Nwaeze, A.S[3], Ugwu, E. C[4], Abundance, M. A[5], Eze, H.O[6], Ozuomba U.C[7], Amadi, E.G[8], Ngene, N.J [9]
[1]Guide, ,[3,4,5] Lecturer, Department of Computer Science, Caritas University, Amorji, Nike Enugu, Enugu State, Nigeria
[2]Student, School of Computer Science and Technology, University of Bedfordshire, UK
[6]Lecturer, Department of Urban and Regional planning, Caritas University, Amorji Nike Enugu, Enugu State, Nigeria
[7]Lecturer, Department of Architecture, Caritas University, Amorji Nike Enugu, Enugu State, Nigeria
[8,9]Lecturer, Department of Computer Science, Enugu State University of Science and Technology, Enugu State, Nigeria

Abstract:- The major concerns that keep most organizations away from cloud computing are Security and information authenticity. People are wary about providing confidential information to unauthorized parties. Individuals or hackers may intercept and modify electronic documents. Using a password to encrypt data is risky because hackers can gain access to it and exploit it to steal data. As a result, this research provides a solution by building a model for protecting data in the cloud via a layered approach. To implement these concepts, a web system developed with PHP and MySQL was employed. The OODM technique was used for components in the system modules, allowing for easy coupling, decoupling, modification, encapsulation, and reuse, as well as easy maintainability. When compared to the previous system, which depended simply on passwords for authentication, the new technique developed produces a high level of data security.

Keywords: *Data protection, Cloud computing, layered approach.*

I. INTRODUCTION

Transferring data manually or semi-automatically leaves it open to tampering. The electoral body is wary of publishing online election results for fear that hackers will attempt to modify the tally. Recent events in developing economies suggest that storing data in the cloud is a secure option for sharing data electronically.

The term "cloud" refers to a network of distant servers that are hosted on the Internet and used to store, manage, and process data. Cloud computing allows users to access and use computer resources such as servers, storage, and apps through the Internet without the need for local infrastructure or hardware.

What cloud computing has done for the IT industry is revolutionary. This information technology can greatly reduce the time and resources required to bring a product to market. With cloud computing, several users can share resources like storage space and computations. It's best to construct and oversee one's infrastructure.

Cloud computing's progress is now linked to the growing popularity of big data, which leads to new trends such as industry 4.0 big data analysis. In reality, cloud computing offers the processing, storage, software, and networking required to handle big data applications [3][4] Cloud computing's progress is now linked to the growing popularity of big data, which leads to new trends such as industry 4.0 big data analysis.

The cloud is defined as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable resources that can be rapidly provisioned and released with minimal management effort or interaction from service providers." Citing the National Institute of Standards and Technology (NIST) [1], the strategic implementation of digital health solutions can bring about transformative benefits. These solutions, including electronic health records, monitoring equipment, telehealth, electronic communications, data analysis, and cloud-based tools, have the potential to diminish health inequalities and enhance user well-being by revolutionizing the delivery of care and health services to patients [5].

II. CHARACTERISTICS OF CLOUD COMPUTING

According to the National Institute of Standards and Technology (NIST), cloud computing has five important qualities.

➢ *Self-Service on Demand:*

Cloud computing enables customers to deploy computer resources such as servers, storage, and applications automatically and on demand, without the need for human interaction from a service provider.

Cloud computing resources are available via the network and may be accessed by a variety of devices, including PCs, laptops, tablets, and mobile phones.Cloud computing resources are pooled and shared among several users, allowing for more effective

Resource utilization and cost reduction as needed, resources can be dynamically assigned and de-allocated.

- *Rapid Elasticity:*

Cloud computing resources may be swiftly scaled up or down to meet changing Demand, allows customers to alter their computer resources quickly and simply as needed. Cloud computing resources are monitored and assessed, and customers are charged based on their actual resource utilization rather than a flat price. This enables cost reductions and is more Effective. Resource deployment [2]: Fig. 1 briefly demonstrates the essential characteristics of cloud computing.

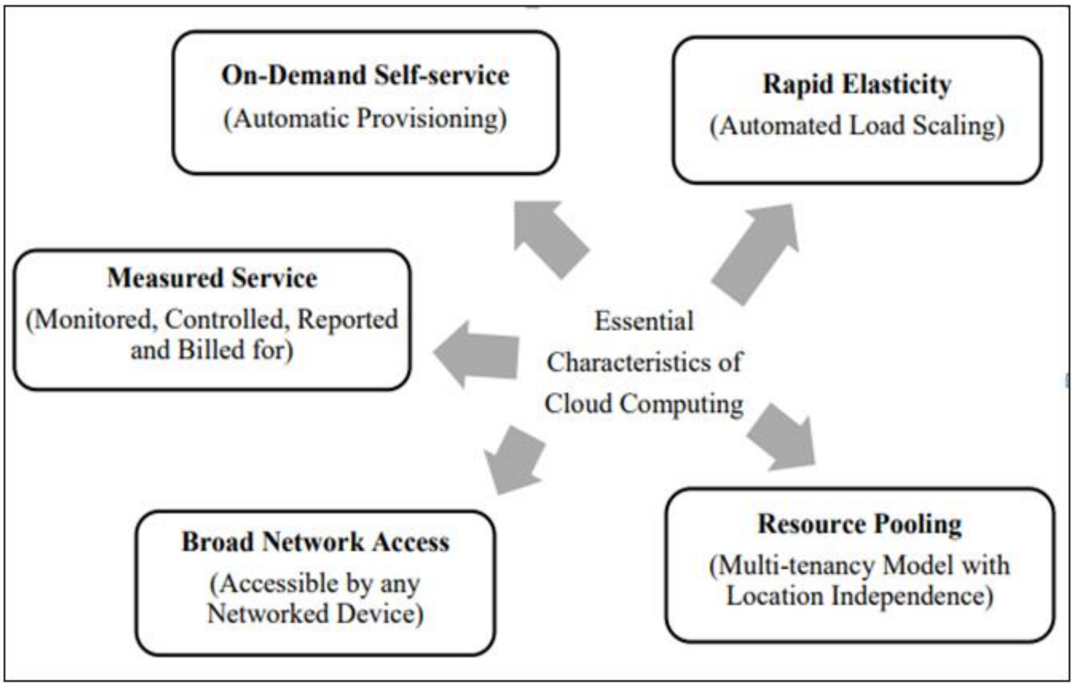
On-Demand Self-service
(Automatic Provisioning)
Rapid Elasticity
(Automated Load Scaling)
Measured Service
(Monitored, Controlled, Reported and Billed for)
Essential Characteristics of Cloud Computing
Broad Network Access
(Accessible by any Networked Device)
Resource Pooling
(Multi-tenancy Model with Location Independence)

Fig 1 The Essential Characteristics of Cloud Computing

III. CLOUD COMPUTER DEPLOYMENT MODELS

Choosing the appropriate form of Cloud Computing to be implemented by an institution is the first and most crucial stage since it guarantees a successful Cloud Computing The successful implementation of Cloud Computing in an institution is contingent upon understanding that different types of Cloud Computing require distinct skills and resources. Numerous institutions have experienced project failures due to selecting the wrong Cloud computing model. To prevent implementation failures, it is crucial for institutions to thoroughly assess their data before determining the most suitable form of Cloud Computing to adopt. Previous research in Cloud Computing has categorized deployment models into four distinct types based on their distribution and physical location [1].

- *Private Cloud:*

The concept of a private cloud involves the delivery of cloud services through an organization's infrastructure, which can be located either on-premises or off-premises. The crucial aspect is that the infrastructure is dedicated solely to the organization. Setting up a private cloud is considered relatively simple as it eliminates the challenges associated with equipment, application, or transfer speed charges. The organization only incurs costs for the services and resources it has actually used. On the other hand, for public cloud services, customers typically pay a monthly fee. Private clouds do not require any additional hardware since they operate on the fundamental principle of scalable storage demand. Examples of recognized private cloud instances include Amazon Elastic Cloud Compute, Google App Engine, Blue Cloud from IBM, and Azure Services Platform with Windows [9]. In summary, private clouds are renowned for providing services to the general public or larger institutions through a third-party provider via the Internet. It is important to note that client data is not publicly exposed, as public cloud providers always ensure authorized and authenticated access control for their clients. Private clouds offer a cost-effective and flexible solution [9]. According to Parsi & Laharika [10], the public cloud has four fundamental characteristics, which are as follows:

- *A Versatile and Scalable Environment:*

The public cloud, exemplified by platforms like Google App Engine and Amazon Elastic Cloud Computing, provides users with a highly adaptable cloud environment.

- *Self-Service Empowerment:*

The public cloud encourages users to create their own cloud infrastructure without the need for external assistance. This is known as pre-configured clouds, readily accessible on the Internet.

- *Pay-per-use Model:*

This distinctive feature makes cloud technology more accessible to organizations, enabling them to operate in a coordinated manner. As businesses embrace cloud services, their future prospects improve. However, users are charged based on the fundamental cloud services they utilize.

- *Accessibility and Reliability:*

One of the notable advantages of the public cloud is its availability to all users, prioritizing agility. Users have the flexibility to manage their tasks from any location across the globe at any time. This not only allows for the execution of essential business operations but also enhances customer engagement on a global scale.

- *Public Cloud:*

The public cloud follows a paradigm where third-party providers offer cloud services through the internet. These services are available to anyone who wishes to use them, and the resources are shared among multiple users. The public cloud model offers numerous advantages as it provides applications, data storage, and various other services to consumers through service providers. This is made possible by the characteristics of the pay-as-you-go model. Designed to offer unlimited storage capacity and improved data transfer over the internet, this cloud architecture is hosted, owned, and operated by a third-party service provider. It caters to the requirements of businesses of all sizes, ranging from small to medium to large enterprises.

- *Hybrid Cloud:*

The hybrid cloud model combines public and private cloud services, allowing businesses to leverage the benefits of both. This may involve transferring data and applications across the two clouds or dynamically moving workloads as needed.

By distributing costs among organizations, this model helps minimize spending on infrastructure establishment. While government agencies within a single region may share resources, non-government agencies typically do not have the same level of resource sharing [10].

Yet, enterprises can keep their costs and security at a reasonable level; yet, there are some difficulties related to cloud standardization and interoperability that should be considered. Sujay [11] identifies the following hybrid cloud characteristics:

- *Optimal use:*

The usual data centers in the server resources are used from 5% to 20%. The reason for this is the crest loads, which are ten (10) times more than the normal weight. As a result, servers are often idle, incurring unnecessary costs. By extending out to open assets to take care of hosts, the hybrid cloud could extend server use.

- *Data Center Consolidation:*

Rather than providing the ability to adapt to the most speculative situations, a private cloud just requires resources in normal cases. The alternative option is to impact our grant server union and therefore achieve a reduction in operating expenditures. This includes hardware, electricity, cooling, maintenance, and service costs.

- *Risk Transfer:*

Organizations retain and operate their server (the hub of their data) and private cloud. The public cloud service provider must ensure that their service is always available. The risk of underestimating workloads is transferred from the service operator to the cloud seller when using a hybrid cloud. The vast majority of cloud providers have SLAs that promise an uptime of more than 99.9% continuously, for example, or downtime of no more than nine (9) hours per year.

- *Availability*:

Extreme accessibility of the company server (the heart of their data) is both inconvenient and costly, as it needs data redundancy, backup, reinforcements, and geographical dispersal. Particularly in organizations where information technology is not the primary focus, the talent pool is fairly limited. If the organization’s server (the center of their data) is unavailable due to certain faults or Distributed Denial of Service (DDoS) attacks, the public cloud may scale up or entirely overrun operations in a hybrid cloud.

- *Community Cloud:*

A community cloud concept entails organizations with similar interests or needs sharing cloud services. This could be useful for businesses that need to collaborate on projects or share resources while still maintaining some control over their data and apps. As a result, either the linked institutions or the cloud that delivers the services can manage this cloud [6]. Community clouds are examples of academic clouds. The cloud computing deployment models are graphically depicted in Fig. 2.

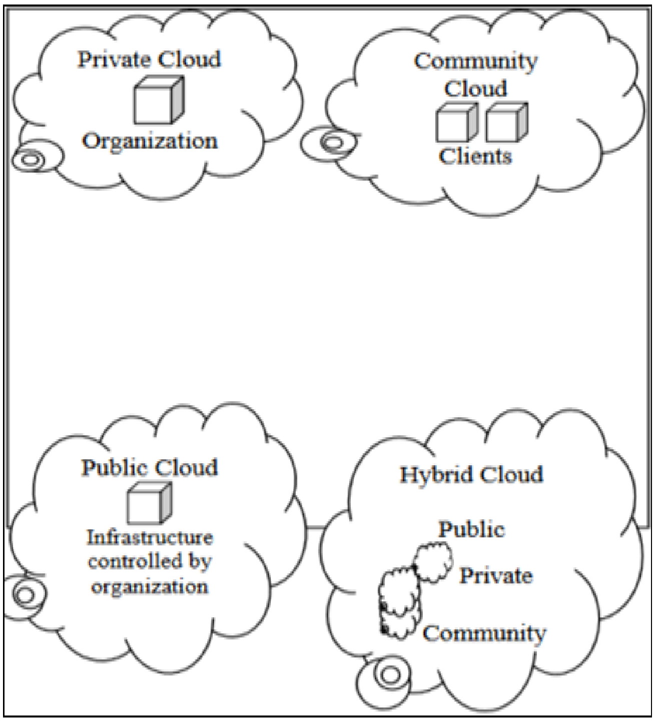

Fig 2 The Cloud Computing Deployment Models [6]

➢ *The Delivery Models in Cloud are [1]:*

- *Software-as-a-Service (SaaS):*

A client can use a browser to access software and data stored in the cloud. The user is not in charge of the cloud infrastructure, network, or servers [6]. It is distinct from traditional hardware, which SaaS does not provide. SaaS software is purchased and installed on a personal computer, similar to a distribution model in which vendors and service providers can access programs and data that is made available to end users through a standard platform, most commonly the internet. It is suitable for a gradually dominating distribution model since it highlighted the technology that carries service-oriented architecture (SOA) and web services as advanced and creative developing approaches begin to gain popularity. Software as a Service (SaaS) is sometimes coupled with a licensing structure, such as a pay-as-you-go subscription. Furthermore, service broadband has become more accessible to end customers, allowing them to access more locations throughout the world. According to the aforementioned remark, Google Docs is the best example.

- *Platform-as-a-Service (PaaS):*

Users or clients can utilize applications provided by the cloud service provider, which operate on a cloud infrastructure and can be accessed through user devices via interfaces like web browsers [7]. This approach allows users to develop their own software libraries or tools and manage software and service deployments. By adopting the Platform as a Service (PaaS) model, businesses can significantly reduce costs since they are relieved of the burden of managing both the software and hardware required for application development. This model simplifies application deployment by eliminating the complexities and expenses associated with procuring and maintaining both hardware and software, as well as provisioning hosting capabilities. Common examples of Platform as a Service (PaaS) include SQL databases and Microsoft's Azure.

- *Infrastructure-as-a-Service (IaaS):*

Clients can order resources on demand and install and run any program, operating system, or application. The user is in charge of resources like the operating system, storage, and programs. Data sharing between enterprises is one of the advantages of cloud computing. The aforementioned benefit, however, introduces a potential data risk. In the Infrastructure as a Service (IaaS) model, the provider offers essential processing, network storage, and additional computing resources, while clients have the freedom to create and operate various types of software, including operating systems and applications. Although customers are not responsible for administering or maintaining the underlying cloud computing system, they have full control over its operation, such as managing storage space, installing applications, and potentially selecting limited networking components based on regulatory requirements. This model provides users with a platform in the form of a computer environment or infrastructure, encompassing both hardware and software.

- *Figure 3 Illustrates the Hierarchical view of Cloud Computing Service Models.*

According to this data, consumers have complete control over the infrastructure cloud provider in any of these service models. Of these three (3) service models, IaaS is the one with the most control over the infrastructure providers. In comparison to IaaS, PaaS has the least amount of control over the infrastructure suppliers. Finally, SaaS is an infrastructure that is distributed to clients through a network and includes all of the services provided in IaaS. Customers of this service have only a sliver of control over the infrastructure. A portion of the providers' responsibility is to manage and control the essential infrastructure and platform.

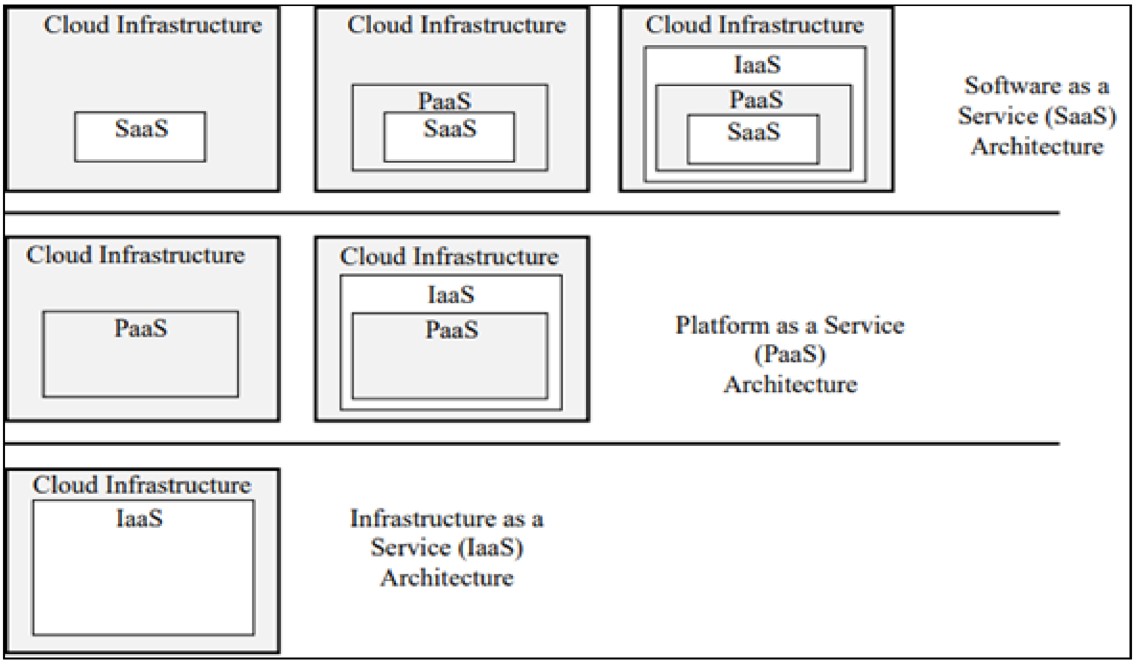

Fig 3 Cloud Computing Service Models can be Depicted in a Hierarchical view [8].

IV. LAYERED APPROACH

In a cloud context, a layered approach refers to a security strategy that entails establishing numerous layers of security controls to protect the cloud infrastructure, applications, and data from various security threats and dangers.

Cloud computing offers numerous benefits, encompassing scalability, flexibility, and cost-effectiveness. Nonetheless, it also introduces a set of distinct security challenges, including shared responsibility, data protection, and compliance.

A layered approach addresses these issues by providing a defense-in-depth strategy that protects against several sorts of cloud-specific assaults, such as data breaches, insider threats, and denial-of-service (DOS) attacks. In a cloud environment, a typical tiered approach contains the following layers:

Physical Security Layer: Implementing physical security measures such as access controls, surveillance cameras, and biometric authentication systems to protect the physical infrastructure where cloud servers are housed is part of this layer.

Network Security Layer: Implementing network security mechanisms such as firewalls, intrusion detection and prevention systems (IDPS), and virtual private networks (VPNs) to safeguard the network infrastructure on which the cloud runs.

Identity and Access Management Layer: This layer controls access to cloud resources by implementing security methods such as multi-factor authentication, identity federation, and role-based access control (RBAC).

Platform and Application Security Layer: To protect the cloud platform and apps from assaults, this layer implements security measures such as secure software development processes, vulnerability assessments, and penetration testing.

Data Security Layer: Implementing security measures such as encryption, access controls, and data loss prevention (DLP) tools to protect sensitive data stored in the cloud is part of this layer.

Compliance and Governance Layer: Implementing security measures to meet regulatory requirements and industry standards such as ISO 27001, HIPAA, and PCI DSS is part of this layer.

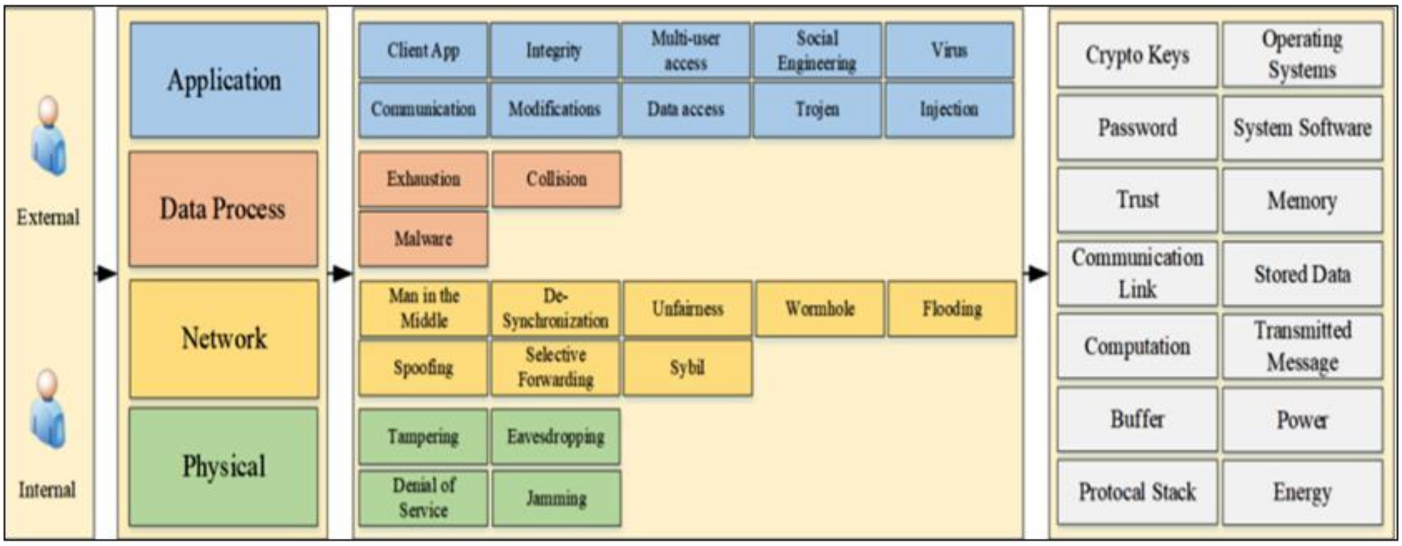

Fig 4 Threat Classification According to Cloud Layers

V. CLOUD-SPECIFIC THREATS THAT CAN BE MITIGATED USING A LAYERED APPROACH

➢ *A Layered Approach to Cloud Security can Assist Defend against a Variety of Cloud-Specific Attacks, such as:*

- *DDoS Attack:*

DDoS assaults are a common danger to cloud infrastructures. DDoS attacks flood cloud resources with traffic from many sources, rendering them inoperable for consumers. By deploying network security controls such as firewalls, intrusion detection and prevention systems (IDPS), and load balancers, a layered approach can assist avoid DDoS attacks.

- *Data Breach:*

When unauthorized individuals gain access to sensitive data stored in the cloud, a data breach occurs. By adopting data security measures like encryption, access controls, and data loss prevention (DLP) tools, a layered approach can help avoid data breaches.

- *Insider Threats:*

Insider threats occur when authorized individuals cause harm to the cloud environment, either purposefully or accidentally. By adopting identity and access management policies like multi-factor authentication, identity federation, and role-based access control (RBAC), a layered approach can help mitigate insider threats.

- *Malware and Ransomware:*

Malware and ransomware are common cloud dangers. Malware attacks cloud resources with malicious software, whereas ransomware encrypts cloud resources and demands payment for access to be restored. Endpoint security measures like antivirus software, endpoint detection and response (EDR), and host-based firewalls can assist prevent malware and ransomware.

- *API Attacks:*

API attacks are a prevalent danger to cloud environments that rely on APIs to interface with other cloud apps and services. API attacks take advantage of API flaws to obtain unwanted access to cloud resources. By incorporating platform and application security measures such as safe software development practices, vulnerability assessments, and penetration testing, a layered approach can help prevent API attacks.

VI. MEASURING THE CHANCE OF OCCURRENCE OF MULTILAYER THREATS IN THE CLOUD

Measuring the chance of occurrence of multilayer threats in the cloud may be a complex and difficult undertaking due to the numerous aspects to consider, such as the type of cloud infrastructure, security mechanisms in place, and threat landscape. Here are some actions you may take to assess the likelihood of multilayer threats in the cloud:

➢ *Threat Assessment:*

Conduct a thorough threat assessment to detect potential cloud threats and risks. This can include evaluating security logs and audit trails, as well as assessing threat intelligence reports and conducting vulnerability assessments and penetration testing.

➢ *Risk Assessment:*

Conduct a risk assessment to assess the likelihood and potential impact of each identified danger. Assigning a risk score based on the likelihood of the threat occurring and the potential impact on the cloud environment can be part of this.

➢ *Vulnerability Scanning:*

Use vulnerability scanning technologies to uncover potential cloud vulnerabilities. This can aid in identifying regions where a layered danger is more likely.

➢ *Assessment of Security Controls:*

Determine the effectiveness of the security controls in place to mitigate the identified threats. This can include auditing rules, procedures, and technical controls to ensure they are correctly established and applied.

➢ *Planning an Incident Response:*

Create an incident response plan outlining how to handle a security event in the cloud. This can include defining the incident response team's roles and duties, outlining the incident response process, and testing the incident response strategy through tabletop exercises.

VII. CONCLUSION

Although cloud computing is a new growing technology that provides numerous benefits to users, it faces numerous security challenges. The Cloud-Based system faces a lot of security concerns and this scares organizations away from hosting their database in the cloud environment. Most security concerns center on the privacy and validity of their data. This calls for a more secure authentication system for cloud computing. Any authentication system’s core strength depends upon the probability of success of breaking that system for accessing the services provided by the cloud service providers. In this research authentication scheme, the core strength is first-tier, second-tier, and third-tier authentication user credentials. For getting access to the requested service, the attacker has to break all the authentication layers. At the first tier, the username and password of the user are verified. Security analysis says that increases as the number of authentication tiers in the system, the probability of success in breaking the multi-tier authentication system reaches near zero. Hence, looking at the security model used in this research, one can say that there is very a less probability of breaking the multi-tier authentication system. Also, the layered approach by Organizations can install many levels of security measures to develop a defense-in-depth approach that protects against various sorts of cloud-specific assaults, such as data breaches, insider threats, and denial-of-service (DOS) attacks. This technique can help to lower the chance of a successful attack and improve the organization's overall security posture in the cloud. With the above security measures, data security in the cloud is guaranteed and it will encourage people to use cloud-based systems security data is guaranteed. Organizations can establish a defense-in-depth approach that protects against various types of cloud-specific attacks by deploying many layers of security controls. This technique can help to lower the chance of a successful attack and improve the organization's overall security posture in the cloud.

REFERENCES

[1]. Smitha Nisha Mendonca s “Data Security in Cloud Computing using AES”, International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181 Vol. 7 Issue 01, January-2018.

[2]. Tinankoria Diaby, Babak Bashari Rad,"Cloud Computing: A review of the Concepts and Deployment Models", International Journal of Information Technology and Computer Science (IJITCS), Vol.9, No.6, pp.50-58, 2017. DOI: 10.5815/ijitcs.2017.06.0

[3]. Mohamed Elhoseny, Ahmed Abdelaziz, Ahmed S. Salama, A.M. Riad, Khan Muhammad, Arun Kumar Sangaiah,”A hybrid model of Internet of Things and cloud computing to manage big data in health services applications”, Future Generation Computer Systems, Volume 86,2018,Pages 1383-1394,ISSN 0167-739X.

[4]. Mohamed Elhoseny, Ahmed Abdelaziz, Ahmed S. Salama, A.M. Riad, Khan Muhammad, Arun Kumar Sangaiah,”A hybrid model of Internet of Things and cloud computing to manage big data in health services applications”, Future Generation Computer Systems, Volume 86,2018,Pages 1383-1394,ISSN 0167-739X.

[5]. Nicola Raimo, Ivano De Turi, Francesco Albergo, Filippo Vitolla, The drivers of the digital transformation in the healthcare industry: An empirical analysis in Italian hospitals, Technovation, Volume 121, 2023,102558,ISSN 01664972,https://doi.org/10.1016/j.technovation.2022.102558.

[6]. Thakur, N., D. Bisen, V. Rohit, and N. Gupta, Review on Cloud Computing: Issues, Services and Models. International Journal of Computer Applications, 2014. 91(9).

[7]. Khorana, S. and A.G. Verma, Comparison of Cloud Computing Service Models: SaaS, PaaS, IaaS. International Journal of Electronics & Communication Technology IJECT, 2013. 4.

[8]. Tehran, S.R. and F. Shirazi. Factors influencing the adoption of cloud computing by small and medium size enterprises (SMEs). in International Conference on Human Interface and the Management of Information. 2014. Springer.

[9]. Kim, W., Cloud Computing: Today and Tomorrow. Journal of object technology,2009. 8(1): p. 65-72

[10]. According to Parsi & Laharika [23] public cloud provides four (4) basic characteristics, which are the following:

[11]. Professional, 2009. 11(2): p. 23-27. [25] Sujay, R., Hybrid cloud: A new era. International Journal of Computer Science and Technology (IJCST), 2011. 2(2): p. 323-326.

[12]. Ezeh Kingsley Ikechukwu, Prof. Ejiofor Virginia Ebere, Frank Ekene Ozioko, Asogwa T.C, Nzeogu Neheta Chinyere, Nwankwo Ugochukwu Cornelius,Anomaly Based Malware Detection System on Smartphone – A Systematic Review: International Journal of Advances in Engineering and Management (IJAEM) Volume 4, Issue 10 Oct. 2022, pp: 686-696.