Journal of Information Systems Engineering and Management
2025, 10(43s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Security Analysis in Cloud

Naman Kumar Verma[1], Dr. Sunil Yadav[2]

[1]M. Tech Student VBSPU, Jaunpur, [2]Assistant Professor VBSPU, Jaunpur

Email: vermanaman813@gmail.com

ARTICLE INFO

Received: 1 Dec 2024
Revised: 10 Dec 2024
Accepted: 20 Dec 2024

ABSTRACT

Cloud computing has reformed the businesses ways and provides the facilities to the people to store, get, and handle information by providing scalable and flexible computing resources. However, the rapid adoption of cloud services has introduced the security challenges that cause noteworthy dangers for confidentiality, integrity, and availability of sensitive information. These challenges include issues such as data breaches, loss of control over data, insecure interfaces and APIs, account hijacking, and inadequate access controls. Additionally, the multi-tenant environment of the cloud environments, where numerous users utilize shared resources, increases the chance of unauthorized access and data leakage. This paper investigates the various safety challenges in cloud computing, examines current threats and vulnerabilities, and discusses potential solutions and best practices to mitigate risks. It emphasizes the need for robust security frameworks, encryption techniques, identity and access management strategies, and compliance with relevant standards to ensure the safe use of cloud services.

Keywords: Cloud Computing, Cloud Evolution, Cloud Architecture, Cloud Security, Data Security, Network Security, APIs Security.

1 Introduction

Cloud computing is an innovative model that delivers internet-based applications and services. Many of the core technologies that underpin them are establishing of the cloud computing have existed for quite some time. Cloud computing involves provisioning of computing, networking and storage resources on demand and providing these resources as metered services to the user, in a “pay as you go” model. The U.S National Institute of Standards and Technology(NIST) [1] defines cloud computing as; Cloud computing provides seamless and continuous access to a shared pool of adaptable computing resources over a network as required (e.g. networks, servers, storage, application and services) that can quickly have accoutrement and attempt or cloud service provider relation. Cloud computing provides Internet- based services to users that allow for easy sharing of data and information. It is an advanced computing process that gives access to databases, servers and miscellaneous applications. Cloud services are providing to clients in distinct forms. NIST defines at least three cloud services models as follows: Infrastructure as a service, Platform as a service, Software as a service.

The first type of cloud service model is Infrastructure-as-a-service (Iaas): IaaS allows clients to allocate computing and resource of storage, which are delivered as virtual machine instances and virtual storage. The user has the power to start, stop and manage these resources. They can install and run on self-selected operating systems and application stacks on the provisioned cloud resources. These service are based on pay-and-go model. For example, EC2, RackSpace, GoGrid.

The second category of cloud service model is known as Platform as a Service (PaaS): Paas provides a platform and environment for developer to develop, run and manage applications. It provides a complete deployment and development infrastructure including operating system programming

Journal of Information Systems Engineering and Management
2025, 10(43s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

languages, libraries and tools. The service provider assumes full responsibility for the infrastructure stack compute resources, network infrastructure, OS deployments, and persistent storage systems. However, Customers assume complete control over their application stack, handling all aspects from development and deployment to configuration and operational management within the cloud environment. For example, Google app engine window azure platform.

The third type of cloud service model is Software-as-a-service(SaaS): SaaS provides fully functional software application on the internet based on service plan. Users can use these applications with the help of web browsers can be used without installing or managing it locally. The provider maintains complete control over the cloud infrastructure stack compute resources, network topology, OS deployments, persistent storage, and application runtime environments, presenting users with fully abstracted

Metric	**IaaS**	**PaaS**	**SaaS**	**Measurement Methods**
Latency(95th%ile)	8 ms (AWS EC2 c5.4xlarge)	22 ms (Azure App Service)	45 ms (Salesforce)	Synthetic API requests (10k sample)
Throughput (reqs/sec)	12,000 NGINX	7,500 (Heroku Dynos)	3,000 (Zendesk API)	Load testing (Locust, 100 concurrent users)
Max Scalable Nodes	1,000+ (Kubernetes on IaaS)	100 (AWS Elastic Beanstalk)	Vendor-limited (e.g., 50/sec)	Cloud provider docs + stress test
I/O Performance	80k IOPS (NVMe SSD)	15k IOPS (Azure SQL DB)	Not applicable	Fio benchmarks (4kB random reads)
Network Bandwidth	25 gbps (AWS enhance networking)	5gbps (Shared Paas backend)	1gbps	Iperf3 tests (intra-region)

Table 1. Performance Measurement between IaaS, PaaS and SaaS

service layer. Application are provided to the user through a thin client interface (e.g. a browser). SaaS application are platform independent. For example, Salesforce.com, Dropbox, Facebook [1] [11].

Journal of Information Systems Engineering and Management
2025, 10(43s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

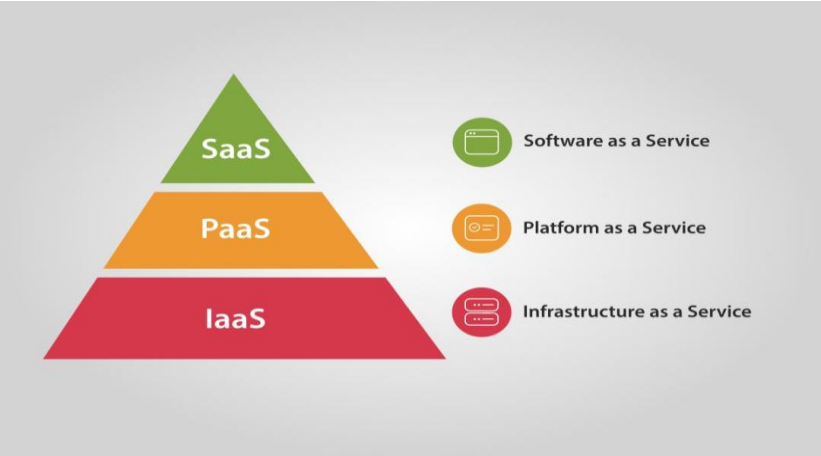

Figure1. Cloud services models

NIST also defines three cloud deployment model as follows: (1) Public cloud**:** Cloud services are accessible to the anyone or a group of organizations. The cloud services are provided by third party cloud provider. (2) Private cloud**:** It is also said to be internal cloud. Private cloud services are used by only single organization. Private cloud is ideal for application where safety is necessary. (3) Hybrid cloud**:** It is the combination of both public and private cloud. While each cloud retains its unique identity, they are interconnected using widely adopted or custom-built technology to enable effortless transfer of data and applications across platforms. This model is ideal for organizations looking to ensure secure application and data hosting in a private cloud while also reducing costs by utilizing public cloud resources for shared applications and data [4] [10].

Cloud Deployment Models	**Advantages**	**Disadvantages**
Public Cloud	Reliability and scalability of resources based on client demand, Cost effective	Insecure, Less Reliable
Private Cloud	Services can access by an organization, Secure	Costly
Hybrid Cloud	Quick speed, Flexible and Scalable, Secure	Vendor lock-in risk

Table 1. Advantages and disadvantages of cloud models

This paper is organized as follows: Section 2 offers a concise summary of the characteristics of cloud computing. In Section 3 outlines the evolution of cloud computing. In Section 4 discusses the architecture of the cloud computing. In Section 5, we examine the security challenges in cloud computing. In section 6 briefly discussed about the conclusion.

2 Cloud Characteristics

NIST moreover diagrams five key characteristics of cloud computing:

Journal of Information Systems Engineering and Management
2025, 10(43s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

On demand self-service: Users can access computing resources (such as storage, servers, and applications) as needed without human intervention from the service provider. **Broad network access:** Access your cloud services instantly from any device from office workstations, home laptops, tablets, or smartphones through our intuitive, browser-based interface. **Resource pooling:** Cloud providers employ a multi-tenant strategy where computer system resources are pooled to support several clients. These resources are allocated in real-time according to usage needs. **Rapid elasticity:** Resources are easily adjustable based on demand to meet demand, ensuring efficiency and cost savings. **Scalability:** Cloud platforms allow businesses to scale their applications seamlessly without requiring significant infrastructure investments. **Multi-tenancy:** Multiple users or organizations can share the same cloud resources while maintaining data isolation and security. [4][5].

3 Evolution of Cloud

Let's begin by discussing evolution. Evolution refers to the process of how a technology develops and changes over time. If a technology is functional today, it must have a history that led to its current form. Every existing technology has some predecessor or earlier version that, through improvements or updates, evolved into the technology we use now. These changes and updates often involve deriving new technologies that enhance performance and usability. When we talk about cloud computing, it didn't just appear out of nowhere. Before cloud computing, there were other computing methods that existed, but they had certain limitations, which led to suboptimal performance and user experience. These earlier methods were refined, improved, and updated, eventually leading to the development of cloud computing. Cloud computing takes these older technologies and builds upon them, offering a more efficient, scalable, and flexible model.

Now, let's explore the evolution of cloud computing itself, looking at the services that have shaped it and laid the foundation for its widespread use today.

.

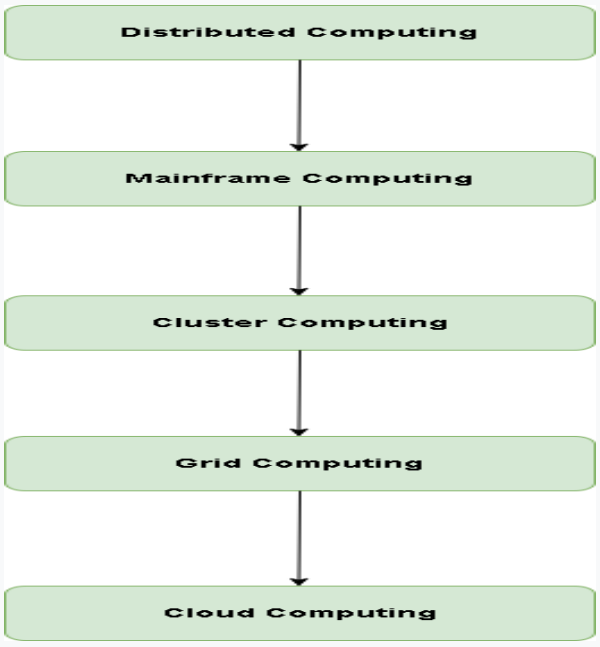

Figure 2. Evolution of cloud computing

3.1 Distributed Computing: Distributed computing involves breaking down a business or application into smaller subservices, which are then spread across different machines. This concept

Journal of Information Systems Engineering and Management
2025, 10(43s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

emerged in the 1950s. Distributed computing is a combination of multiple independent systems that work together to appear as a single system to the user. The main aim of a distributed system is to share resources and utilize them effectively and efficiently. A distributed system has several key characteristics, including scalability, concurrency, continuous availability, and heterogeneity. In such systems, a given service is divided into smaller subservices. These subservices are then distributed across various machines in the system, with the user accessing one of these services. A distributed system doesn't require all components to be located in the same physical place, allowing for more flexibility and resource sharing across different locations.

3.2 Mainframe Computing: Mainframe computing was introduced in 1951 to address the limitations and challenges of distributed computing. Mainframe systems are highly powerful and reliable machines designed to handle and process large data amount quickly, such as in online transactions. Following the advent of distributed computing, mainframe computing significantly enhanced system processing capabilities. It can be seen as an upgraded version of distributed computing, offering more centralized and efficient data processing. However, mainframe computing is quite expensive, making it less accessible for smaller organizations.

3.3 Cluster Computing: Cluster computing emerged in the 1980s to address the limitations of mainframe computing. In this model, multiple servers are grouped together to function as a single system, essentially acting as one computer. The purpose of cluster computing is to achieve the same business goals as mainframe computing but in a more distributed manner, enhancing performance and scalability. Users can access the combined resources of the clustered servers as if they were interacting with a single server.

3.4 Grid Computing: Introduced in the 1990s, grid computing was developed to overcome the limitations of cluster computing. Unlike cluster computing, grid computing involves connecting different systems located at various geographical locations. These systems are linked together via the internet, enabling them to share resources and work collaboratively on tasks across different sites.

3.5 Cloud Computing: Cloud computing came into existence in 2007 to solve some of the challenges faced by grid computing. It permits clients to store, retrieve, and use data and networking services using internet. Cloud computing is based on pay-and-go model, where users can utilize resources like storage, applications, and on-demand services. This technology supports various formats, including text, images, files, and documents, providing flexibility and scalability for users [6].

4 Cloud Architecture

Cloud architecture refers to the structure and organization of various cloud technology elements, including hardware, virtual resources, software functionalities, and virtual network, which work together to form cloud computing environments. It serves as a design plan that outlines the optimal approach to integrating resources in order to create a cloud environment tailored to a particular business requirement. The architecture of cloud computing combines both Cloud architectures commonly leverage SOA and EDA to enable modularity and responsiveness is categorized into two main parts: Frontend and Backend. The frontend of cloud computing architecture indicates the client side of the cloud computing architecture. It includes all user interfaces and applications that clients use to access cloud services and resources. For instance, a web browser used to access a cloud platform is an example of the frontend. The backend of the cloud computing architecture indicates the cloud infrastructure utilized by the service provider. It encompasses the resources, manages them, and ensures security. Additionally, it includes large-scale storage, virtual applications, virtual machines, traffic management systems, deployment models, and many more. Cloud computing architecture is general high- level view to visualize the structure of the system, various cloud resources, middleware, software component, services and relationships among them. Figure 3 represents the cloud computing architectural view.

Journal of Information Systems Engineering and Management
2025, 10(43s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Users can use various services according to their choice and usage; service providers provide those service with the help of various virtualization techniques. The customer cannot see the hidden complexities of the cloud provider such as data centres and VM management. They only see the web interface through which various services are offered simultaneously and all these services are metered according to usage. These users may be business users, developers or home users who mainly use IaaS, PaaS and SaaS [7] [13].

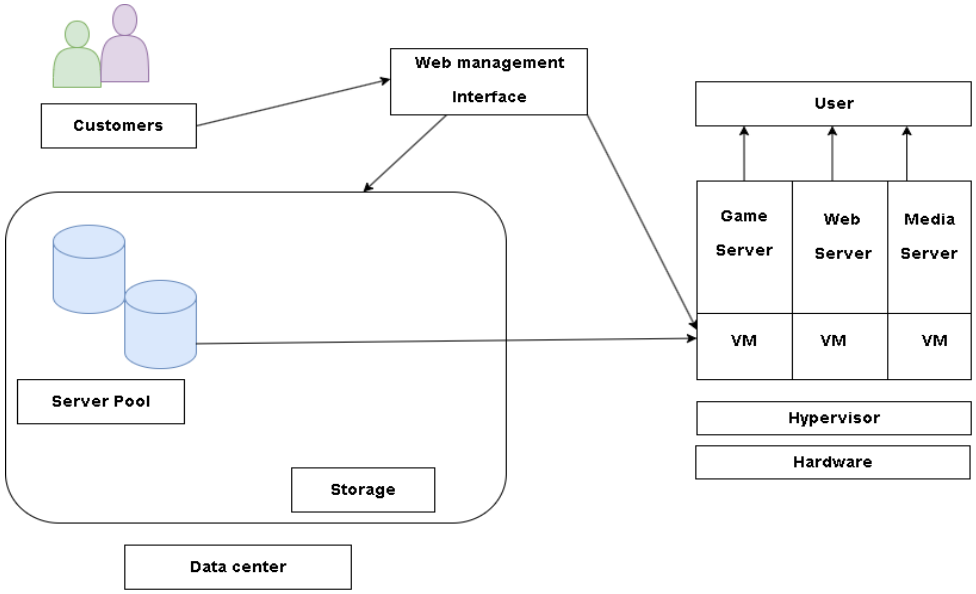

Figure 3. Cloud architecture

5 Security Attacks on Cloud Services

-Rates of Security Incident in Cloud Environment

In 2024, over 60% of organization faced cloud security breaches, and 21% of these incidents led to sensitive data exposure.

-Security Risk from Human Mistake and System Misconfiguration

Despite advanced security tools, human factors continue to enable cloud breaches. 2024 data shows 31% of the 44% reported cloud data exposures stemmed from employee errors or system misconfigurations.

-Difficulties in Sharing Data Across System

The challenges of handling data across diverse systems are clear 40% of data breaches in 2024 occurred due to data spread across multiple platforms.

-Cloud-Based Sensitive Data

Statistics shows that 47% of cloud data qualifies as sensitive, yet encryption rates remain alarmingly low, with under 10% of enterprises securing four-fifths or more of their cloud-stored information.

Journal of Information Systems Engineering and Management
2025, 10(43s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

-Phishing Attacks

Cloud security remains vulnerable to phishing, as 73% of businesses faced breaches stemming from such attacks in 2024.

-Rapid Growth in Cloud Security Solutions

Cloud security solutions are experiencing explosive growth, with industry revenues, forecasted to hit $2 billion this year.

-Financial Impact

In 2024, data breach expenses climbed to a record $4.88 million globally, representing a 10% per years the highest cost ever documented.

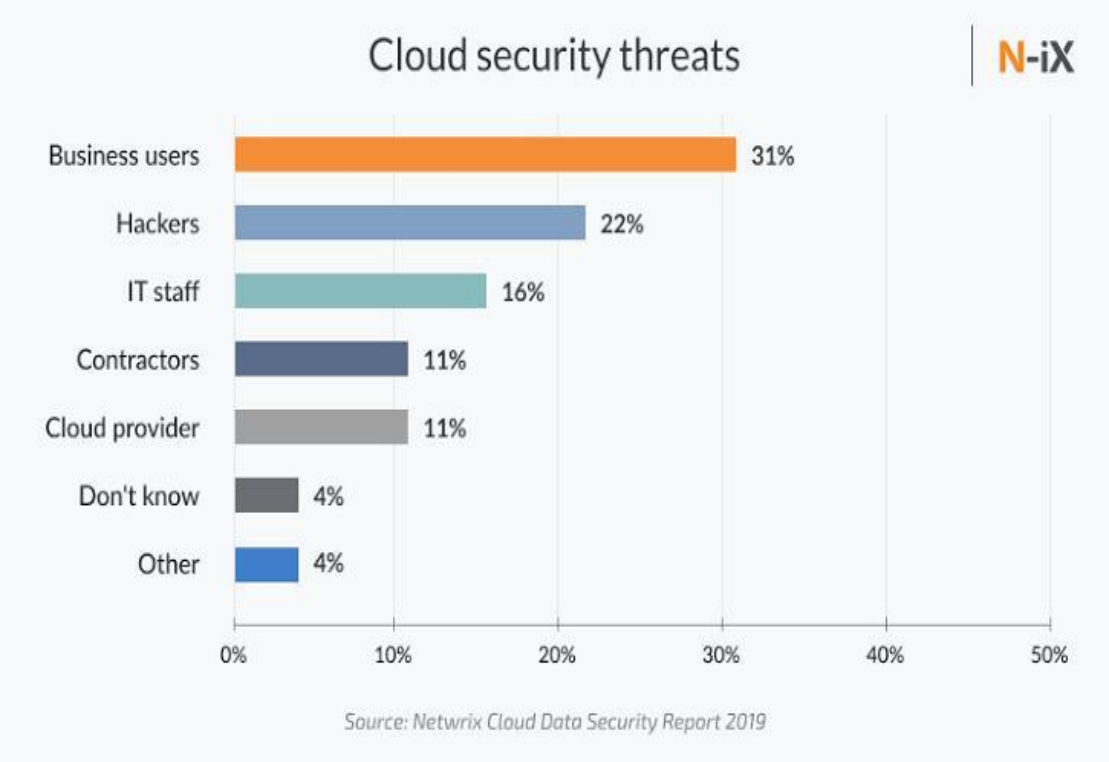

Figure 4. Graph for Security Attacks on Cloud

6 Security Issues and Challenges in Cloud

Cloud computing delivers multiple profits, including ability to scale, adapt, and reduce costs, but it also presents various security concerns. Both businesses and individuals must tackle these issues to protect the safety and integrity of their data and systems in the cloud. Most cloud service providers implement advanced security features similar to those that exist in in-house IT environment. However due to outsourced nature of the cloud, resource pooling and multi-tenanted architecture, security remains an important concern in adoption of cloud computing. Key security challenges for cloud application includes:

Journal of Information Systems Engineering and Management
2025, 10(43s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

6.1 Data Level Security

Data security is a technique through which we can secure the data from theft, unauthorized access, data corruption and loss of data throughout its lifecycle. It involves measures taken to safe the data from both at rest data (stored) and data in motion (transit data) to confirm its confidentiality, integrity, and availability. Data safety is critical in any organization to prevent breaches, ensure privacy, and comply with regulations. There are some drawbacks which affect the performance of data level security are: High Complexity, Performance Overhead, Difficult Scalability, Risk of Misconfiguration, Integration Challenges, Limited Visibility and Monitoring.

- Controlling the data loss: Outsourcing results in a loss of significant control over data. Large banks are reluctant to use cloud-based programs that could jeopardize their data through interactions with other programs. Amazon Simple Storage Service (S3) APIs offer control the access at both level the bucket levels and object levels, using preset configurations that merely allow authorized access by the creator of the bucket or object. Except a consumer specifically allows unknown access, the first step to accessing the data involves authentication through an HMAC-SHA1 signature for the request to use the private key of user. This ensures that the consumer retains all the controls over who can access their data.

- Authentication: Authentication in the cloud computing plays an important role in data security, preserving that only entrusted users and systems can access cloud-based resources. By employing a multi-layered approach to authentication (MFA, IAM, PKI, and advanced techniques like biometric and behavioural authentication), foundation can Considerably constrict the risk of unwanted access of data and data leaks, thereby improving the safety and integrity of cloud-stored data.

- Authorization: Authorization describes the procedure of defining and granting access the rights to protect the resources from some unauthorized users. In a conventional internal IT infrastructure, the organization controls these access policies and can modify them as needed. For instance, an organization can set different access policies for various departments. However, in cloud environment, authorization relies on the cloud service provider's tools and services to define and manage these access policies.

- Data Integrity: Data integrity in cloud computing refers the stored data, processed and transmitted within the cloud server must be accurate, consistent and unchanged until it can be modifying by client, user or system. Since cloud computing provide remote storage and access, maintaining the data integrity is very crucial for data security.

- Securing data at rest: Securing rest data refers to protect that data which are stored, from unauthorized user, leaks or data corrupting. This stores the data on hard drives, SSDs, database, cloud storage and other storage devices when it is not going to be transmitted and processed. Hence information may be major target for attackers. So implementing the robust security measures is essential to prevent confidentiality, integrity and availability.

- Symmetric Encryption: Symmetric encryption is a technique in which we can employs a single shared key for both data encryption and decryption operations. This secret key is common between sender and receiver. So this technique is ideal suitable to protect the which is in rest form hence the data can be accessed by authorized user's only [14].

- Asymmetric Encryption: Asymmetric encryption is a method that employs two separate keys one for encryption and another for decryption. These keys are attached to each other so that the one key encrypt plaintext to ciphertext and the other key decrypt ciphertext to plaintext. Public key can be sharable but private key not. [14].

Journal of Information Systems Engineering and Management
2025, 10(43s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

- Securing data in motion: Securing data in motion refers the data that can be transmitted from sender to receiver through an insecure network, and it is necessary to confirms the data integrity and confidentiality. Data confidentiality means data should be restricted for unauthorized use and it should be unchanged when it can be transmitted from one end to other end. Data integrity means data remains unchanged whether it is in rest or motion form. Encryption mechanism, secure communication protocols and user identification and control over access rights mechanism are used to protect data in motion.

- One Time Password (OTP): One-time password is the technique for authentication process. It is valid for a single login session or transaction and expires after a short period, making it more secure than static passwords. SMS remains the predominant delivery channel for One-Time Password (OTP) tokens due to its universal accessibility. The most widely adopted generation method employs time-synchronized cryptography through the Time-based One-Time Password algorithm, SMS/Email OTP and Push Notification OTP are some kind of OTP.

- Digital signature for controlling data loss: Digital signatures help safeguard against data loss by ensuring data integrity, authenticity, and accountability. They provide a cryptographic method to verify that the data hasn't been altered, track access and changes, and ensure the data's authenticity. Coupled with other security measures like encryption and backup systems, digital signatures can significantly contribute to reducing the risks of data loss and ensure robust data security in the cloud. While digital signatures primarily provide verification of the data's origin and ensure that it has not been altered, they also play a crucial role in maintaining control over data loss [7] [9].

6.2 Network Level Security:

- Man in the Middle Attack (MITM): A Man-in-the-Middle attack mentions an incident where an attacker intercepts communication between a user and an application. This allows the attacker to either listen in on the conversation or impersonate one of the parties, making the exchange appear legitimate. The main aim of this attack is to hijack the vulnerable information, such as login credentials, details of account. Common aim includes users of financial services, SaaS platforms, e-commerce websites, and others sites that require login credentials. The stolen information is applicable for various malicious purpose, such as impersonation for fraudulent purposes, unauthorized money transfers, or restricted password modifications.

- Distributed Denial of Service (DDOS) Attack: DDoS attacks are categorized as cyber-attacks in which the attacker sends all internet traffic to a targeted system, server or network through flood. This slows down the performance of the system and the attacker gains access to the system. DDoS attack sends heavy data traffic using multiple servers and internet. The DDoS attack ranks as one of the most well-known attack methods in cyber security platforms. When a website crashes, it means a DDoS attack has happened to the victim. The entities infected devices are called zombies (bots), and a collection of these bots forms a botnet. Once the botnet is in place, the attacker can issue remote commands to each bot to launch an attack. When a botnet targets a victim's server or network, each bot in the network sends requests to the target's IP address, overwhelming the system with traffic. [12].

- IP Spoofing: IP spoofing is a cyber-attack technique where attackers alters the origin of their Internet Protocol (IP) address with IP spoofing someone intentionally modifies or "spoofs" their IP address to trick others into thinking they are someone else or somewhere else. It's like wearing a disguise online. This can be used in various types of cyberattacks, such as DDoS attacks, where the attacker disguises their identity to avoid detection, or to deceive the target into responding to a malicious request. Amazon's host-based firewall system prevents any instance from sending network traffic that uses a source IP or MAC address different from its own [7].

- Data Packet Sniffing: Data packet sniffing refers to the process of capturing and analysing data packets that are transmitted over a network. This technique is often used for monitoring network traffic,

Journal of Information Systems Engineering and Management
2025, 10(43s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

troubleshooting, or detecting unauthorized activity, but it can also be employed for malicious purposes, such as intercepting sensitive information**.**

- Session Hijacking: Session hijacking generally occurs on a website or an entire network in which the attacker gains access to sensitive information. By exploiting weaknesses in the session management, the attacker can impersonate the authorized user and obtains unauthorized access to sensitive information. [7] [8].

6.3 APIs Level Security

Securing APIs is essential for tackling security issues in cloud computing. Since APIs serve as the foundation of today's cloud-based services, protecting them is key to safeguarding data, applications, and infrastructure from potential threats.

-OAuth

OAuth is an open standard developed by Blaine Cook and Chris Messina, designed to provide a secure and standardized way for web applications to authorize access to APIs. It enables safe publishing and interaction with protected resources. For developers, it offers a simplified approach to managing access permissions. OAuth (Open Authorization) is a widely adopted open standard that allows secure, delegated access to resources without the need to share user login details. Within cloud computing, OAuth is essential for ensuring secure interactions among cloud-based services, applications, and users by providing detailed and controlled access permissions and authorization. Fundamentally, OAuth enables an application (known as the client) to access resources located on another service (the resource server) on a user's behalf. This process is managed by an authorization server, which issues access tokens. These tokens provide defined, temporary permissions that allow access to APIs or services without revealing the user's login credentials.

In cloud environments, OAuth is commonly utilized in various scenarios, including:

- Allowing third-party applications to securely access cloud-based APIs, such as Google Drive, Microsoft Graph, or AWS services.
- Facilitating Single Sign-On (SSO) across different cloud platforms and services for a seamless user experience.
- Protecting RESTful APIs used by microservices, especially those deployed in containers or serverless architectures, by managing secure access and authorization [7].

-IAM

IAM is a crucial element of an organization's security framework, ensuring that authorized users have appropriate access to necessary resources. In cloud environments, IAM becomes even more vital as organizations depend on distributed systems and multiple external services. By adopting robust IAM solutions, organizations can improve security, simplify access control, and meet regulatory compliance standards. Through IAM we can achieve authorization like Role-based access control (RBAC) and Attribute-based access control (ABAC) and authentication also. IAM allows organizations to oversee digital identities and regulate user access to important data within their cloud environments. It plays a crucial role in protecting both information and infrastructure, particularly in multi-tenant, distributed, and scalable cloud platforms such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP). IAM provides the following features for protecting APIs: Security, Compliance, User Convenience, Scalability and Risk Mitigation [11].

Journal of Information Systems Engineering and Management
2025, 10(43s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Feature	IAM	Traditional Security
Access Control Model	Role-Based(RBAC), Attribute-Based(ABAC)	Often Group Based or Static Permission
Authentication	Multi-factor(MFA) , SSO Federal Identity (OAuth)	Username/Password (Often Single-Factor)
Authorization	Fined-Grained Policies (JSON/YAML)	Coarse-Grained(File/Share Permission)
Credential Management	Short-Lived-tokens, Dynamic Secret	Long term password, Hard coded key
Scalability	Auto Scale with Cloud Services	Manual User/ Group Management
Audit & Compliance	Real- Time Logging	Limited Logs, Manual Audit
Security Posture	Zero Trust, Test Privilege by Default	Perimeter-Based (Firewall-Centric)
Tools	AWS, IAM, Azure, GCP	Active Directory LDAP, VPNs

Table 2. Difference between IAM and Traditional Security

-OpenID

OpenID Connect extends the OAuth 2.0 authorization framework by introducing an identity layer, enabling client applications to confirm user identities and retrieve basic profile details. It relies on standardized JSON Web Tokens (JWT), known as ID tokens, to transmit identity information securely. These tokens are digitally signed and can be encrypted, ensuring their integrity and making them well-suited for use in diverse cloud environments, including public, private, and hybrid models. Cloud environments typically consist of various applications, microservices, and third-party integrations, all of which demand strong authentication and authorization. In traditional setups, each service manages its own login credentials, resulting in fragmented identity management, heightened risk of credential breaches, and a subpar user experience [7]. OpenID solves these issues by centralizing identity verification with trusted identity providers (IdPs) like Google, Microsoft, or enterprise solutions such as Okta or Auth0.

6.4 Difference Between Data Security, Network Security and API Security

Aspect	Data Security	Network Security	API Security
Primary Focus	Protecting Data at Rest/ in Transit	Protecting infrastructure (VPCs, firewalls)	Securing Communication Between Services/Apps

Journal of Information Systems Engineering and Management
2025, 10(43s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Key Technologies	Encryption,DLP, Tokenization	Firewalls, VPNs, DDoS Protection	OAuth 2.0, JWT, API Gateway
Threats Mitigated	Data Breaches, Leaks, Unauthorized Access	DDoS, MIMT, IP Spoofing	Broken object-level Auth, Injection Attack
Cloud Service	AWS KMS, Azure Key Vault, GCP Cloud HSM	AWS Shield, Azure NSG, GCP Firewall Rules	AWS API Gateway, Azure, API Management
Implementation	Encryption (TLS 1.3), Access Controls	Segmentation (VPCs), Zero Trust Networking	OAuth,Input Validation
Monitoring	Data Access Logs, SIEM Alerts	Network Flow Logs, IDS/IPS	API Logs, Threat Detection
Example Use Case	Encrypting PII in an S3 bucket	Isolating Workloads in a private Subnet	Securing a payments Gateway API

Table 3. Difference between Data Security, Network Security and API Security

6.5 Performance Comparison Between Data Security, Network Security and API Security

Metric	Data Security	Network Security	API Security
Latency Impact	High	Low	Moderate
Scalability	Variable	Moderate	High
Resource Overhead	High	Low	CPU-heavy
Throughput	Limited by crypto operation (~10-20%) due to encryption	Limited by Network Bandwidth (~5-15 %)	Limited by API Gateway capacity (~15-30 %)
Cloud Optimization	Hardware HSMs, AES-NI acceleration	SD-WAN, global load balance	Auto-scaling API Gateway

Table 4. Performance comparison between different security types

Journal of Information Systems Engineering and Management
2025, 10(43s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

7 Solutions for cloud data security

In today's cloud computing landscape, ensuring the security of data is critically important. Encryption remains one of the primary methods for protecting information, particularly during transmission. The Diffie-Hellman key exchange algorithm plays a vital role in creating secure communication pathways, allowing data to be safely encrypted even over unsecured networks. By using Diffie-Hellman, two entities such as a user and a cloud server can establish a shared secret across a public channel without directly sharing the secret key itself. They first agree on common public parameters, exchange their public keys, and then individually generate the same shared secret, which becomes the basis for encrypting their communication. This method ensures that, even if cyber attackers intercept the transmission, they cannot access the encrypted data without the private keys. Diffie-Hellman is commonly integrated into secure connection protocols, like TLS handshakes, making it a key technology for safeguarding sensitive data in the cloud.

8 Conclusions

Even though cloud computing is a rising technology for nova days, which provides multiple services for their users, and the security is the major issue for protecting data from cloud platform. In this paper we discussed the different security challenges for data loss in cloud computing and also a robust solution to overcome the risk of data loss in cloud computing.

Conflict of Interest - The authors declare that they have no conflict of interest.

Funding Information - There is no funding granted for this research through any external sources

Author Contribution – It is declared by author that all works embodied in this manuscript is written by the researcher himself

Data Availability Statement – N/A

Research Involving Human and / or Animals – This article does not contain any studies with human participants or animals performed by any of the authors.

Informed Consent - The authors affirm that this manuscript is original, has not been published previously, and is not currently under consideration by any other journal.

References

[1] Cloud Computing A Hands-on Approach, Arshdeep Bahga and Vijay Madisetti, Universities Press

[2] Cloud Computing Principles and Paradigms, Rajkumar Buyya, James Broberg and Andrzej Goscinski, Wiley

[3] Cloud Computing Fundamentals, Industry Approach and Trends, Rishabh Sharma, Wiley

[4] Mohamed Al Morsy, John Grundy and Ingo Müller an Analysis of the Cloud Computing Security Problem

[5] Kriti Bhushan and B.B. Gupta Security challenges in cloud computing: state-of-art IEEE Transactions on Dependable and Secure Computing, Vol. 1, No. 4, pp.193–208.

[6] Sonia Bassi 1, Anjali Chaudhary 2 Cloud Computing Data Security-Background & Benefits

[7] L. Ertaul1, S. Singhal2, and G. Saldamli3 Security challenges in cloud computing 1 Mathematics and Computer Science, CSU East Bay, Hayward, CA, USA 2 Mathematics and Computer Science, CSU East Bay, Hayward, CA, USA 3 MIS, Bogazici University, Istanbul, TURKEY

[8] Akhil Behl Emerging Security Challenges in Cloud Computing an insight to Cloud security challenges and their mitigation

[9] R. Velumadhava Raoa, K. Selvamanib Data Security Challenges and Its Solutions in Cloud Computing

[10] Hamed Tabrizchi1 · Marjan Kuchaki Rafsanjani1 A survey on security challenges in cloud computing: issues, threats, and solutions Published online: 28 February 2020 © Springer Science Business Media, LLC, part of Springer Nature 2020

[11]Nalini Subramanian(Research Scholar) , Andrews Jeyaraj Recent security challenges in cloud computing https://doi.org/10.1016/j

[12] Srijita Basu Arjun Bardhan, Koyal Gupta, Payel Saha, Mahasweta Pal, Manjima Bose, Kaushik Basu, Saunak Chaudhury, Pritika Sarkar Cloud Computing Security Challenges & Solutions-A Survey

[13] Muhammad Faheem Mushtaq1, Urooj Akram1, Irfan Khan2, Sundas Naqeeb Khan1, Asim Shahzad1, Arif Ullah1 Cloud Computing Environment and Security Challenges: A Review

[14] Keiko Hashizume1, David G Rosado2, Eduardo Fernandez-Medina2 and Eduardo B Fernandez1 an analysis of security issues for cloud computing

[15] https://bridgeit.com.au/blog/choosing-the-right-cloud-service-model / accessed at 22 January 2025

[16] https://www.geeksforgeeks.org/evolution-of-cloud-computing/ accessed at 22 January 2025

[17] https://cloud.google.com/learn/what-is-cloud-data-security accessed at 22 January 2025

[18]https://www.cisa.gov/news-events/news/understanding-digital-signatures accessed at 23 January 2025

[19] https://www.ibm.com/think/topics/man-in-the-middle accessed at 23 January 2025

[20] https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/ accessed at 23 January 2025

[21] https://www.n-ix.com/cloud-security-best-practices/