International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

The Dark Side of the Cloud: Security Issues in Cloud Computing

Dr. H. Mohana
Assistant Professor
Department of Computer Science
St Anne's Arts and Science College

Abstract - Cloud Computing is an internet-based computing model that delivers services and resources on demand through the internet, either through a private cloud within an organization or via third-party servers. It is mainly defined by features such as scalability, pay-per-use, and self-service access. Industries like banking, healthcare, retail, education, manufacturing, and business widely adopt cloud computing because it allows easy and cost-effective access to networks, storage, servers, applications, and other services without the need to own physical infrastructure. Despite its advantages, limited control over cloud data can lead to several security concerns, including data loss, misuse of cloud services, insecure APIs, malicious insiders, shared technology vulnerabilities, account hijacking, and traffic interception. To improve security and build user trust, continuous research, technological advancements, and new security solutions are being developed. This research paper provides an overview of cloud computing, discusses the major security threats and challenges in the field, highlights its significance in various industries, and explores possible future developments in cloud security.

KEYWORD: Cloud computing, Saas, Paas,Iaas, Security issues, Future Trends

I. INTRODUCTION

The term cloud computing was first influenced by Googles CEO Eric Schmidt in late 2006 [6][7]. The term Cloud refers to something that is present everywhere that can be accessed by anyone from any part of the world like Internet, hence the name Cloud Computing. In other words, we can say that Cloud is something which is present at remote location over network. Cloud Computing refers to manipulating, configuring and accessing the applications o As the name suggests, cloud computing refers to something that is ubiquitous and accessible to anybody, wherever in the globe, such as the Internet. Put another way, we can define the cloud as anything that exists remotely via a network. Using the cloud (via the Internet) to manipulate, configure, and access applications is known as cloud computing. Both hardware resources and software components are used in cloud computing. Depending on the needs and demands of the users, cloud computing offers them all services like storage (SaaS), infrastructure (IaaS), and platform (PaaS). To put it simply, cloud computing is the provision of services, such as servers, storage, databases, networking, and software, via the internet (the "cloud").Pay-as-you-use cloud services offer cost-effective, scalable, and agile solutions. Line through Cloud (over Internet). Cloud Computing has both, the components of software and hardware resources involved in it. Cloud computing provides everything like a service including storage (Saas), infrastructure (Iaas) and platform (Paas) for the users as per their requirements and needs. To make it more elaborate we can simply say that Cloud computing is the delivery of services including servers, storage, databases, networking and software over the internet("Cloud").Cloud provides services on a pay-as-per use basis offering agile, scalable and cost effective service.

II. TYPES OF CLOUD

- Public Cloud -> The public cloud allows systems and services to be easily accessible to the general public on pay-as-per use basis. It allows scalability and resource sharing.Public clouds are owned and operated by thecloud service providers, which deliver their computing resources like servers and storage over the Internet. Microsoft Azure, Amazon Web Services are an example of a public cloud.
- Private Cloud -> The private Cloud on the other hand refers to computing resources used exclusively by a single business or organization. Private Cloud can also be said as an internal cloud for a company that can be used only by its members and no other general public can have access to it. Private cloud is a more secure cloud system and has more control over its system

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

as it is used by a selected group of people.

- Hybrid Cloud ->Hybrid cloud as the name suggests is a combination of both private cloud and public cloud. It creates a single environment to operate both the private cloud resources as well as public cloud resources thereby providing increased flexibility. In simple words we can say that in hybrid cloud, both private and public cloud is integrated providing the features of both in one single frame.
- Community Cloud ->Community cloud computing refers to the one in which a group of several orgnizations or companies share the cloud services. The organizations having the same concerns can share the resources in community cloud. The services can be hosted by a single or group of organizations belonging to the community or by some external third party as well.

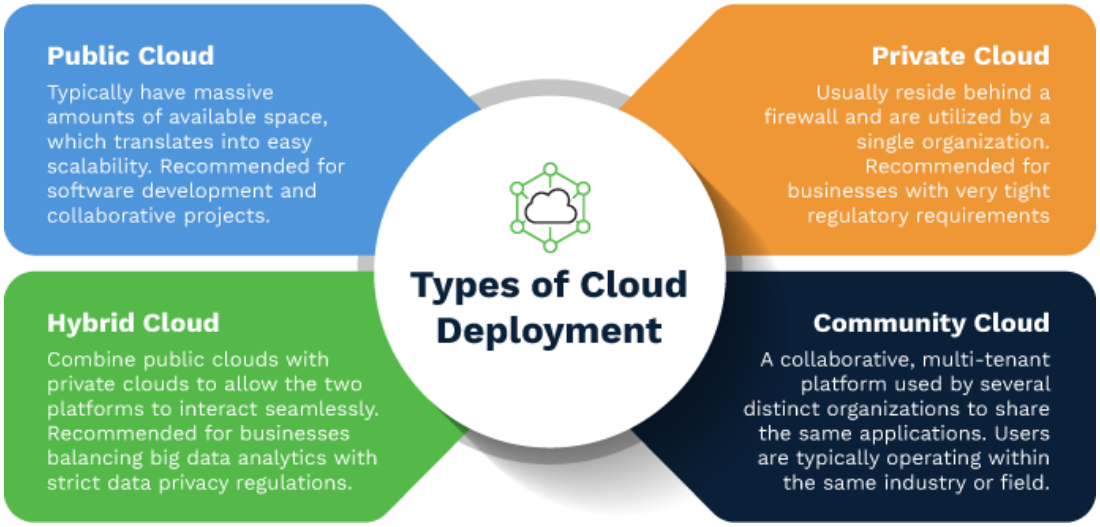


Figure 1: Cloud Deployment

III. LITERATURE REVIEW

The academic discourse on cloud security has evolved significantly since the early conceptualizations of cloud computing. Initial research focused primarily on virtualization vulnerabilities and basic service-level agreements (SLAs) for availability [1]. The shared responsibility model continues to create security gaps, with research indicating that 89% of enterprises misunderstand their security obligations in cloud environments [2].

The past studies on cloud security, especially the ones carried out before 2015, mostly focused on the techniques used in encryption, access control systems, and secure authentication structures as fundamental solutions to safeguard against unauthorized access to data [3].
The theoretical basis of cloud security is rooted in two major paradigms, which are the shared responsibility model and the zero-trust architecture. The shared responsibility model outlines the separation of security responsibility among cloud users and the cloud service providers by focusing on the significance of collective effort towards holistic protection [4].

There have been large research gaps in the improvement of cloud cybersecurity. The existing literature explains that adaptive and real-time defense mechanisms are insufficient and can respond to threats independently of each other to complex and multi-vector threats [5]. Key areas of concern include communication interception, denial-of-service attacks, and the injection of cloud malware, all of which pose significant threats to data integrity and availability within cloud infrastructures [10].

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

IV. CLOUD COMPUTING ARCHITECTURE:

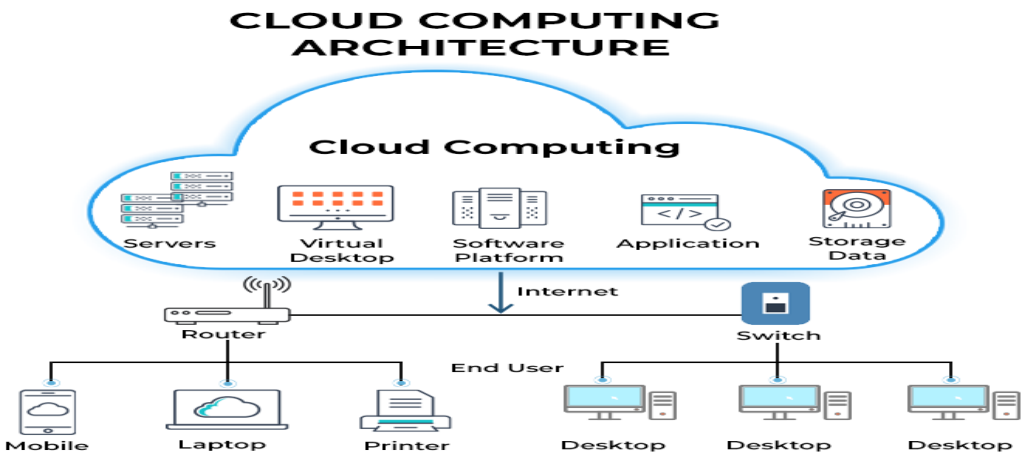


Figure 2: Cloud Architecture

Cloud computing allows users to store files online instead of on physical storage devices, enabling access from anywhere with an internet connection. Cloud services are mainly categorized into Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). Based on deployment, clouds can be public, private, or hybrid.

Cloud computing has two layers: the front end and the back end. The front end is the user-facing layer that allows access to cloud-stored data through applications or software. The back end consists of servers, databases, and hardware that securely store and manage data. Middleware software connects the front end and back end to ensure smooth communication between applications and databases.

V. MODELS FOR CLOUD SERVICE DELIVERY

The Cloud Computing generally contributes three types of services: [8]

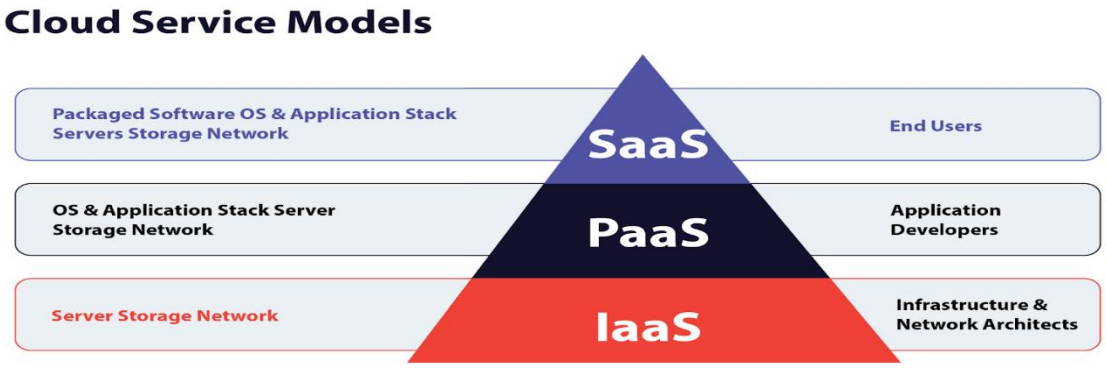


Figure 3: Cloud Services

a) Software that is offered as a service SaaS: SaaS is a cloud service where the entire software is offered as a service via the internet on a pay-per-use basis. To put it simply, this service simplifies our task by enabling us to utilize the software immediately through the internet rather than downloading and then using it. This service can use any software that is available.

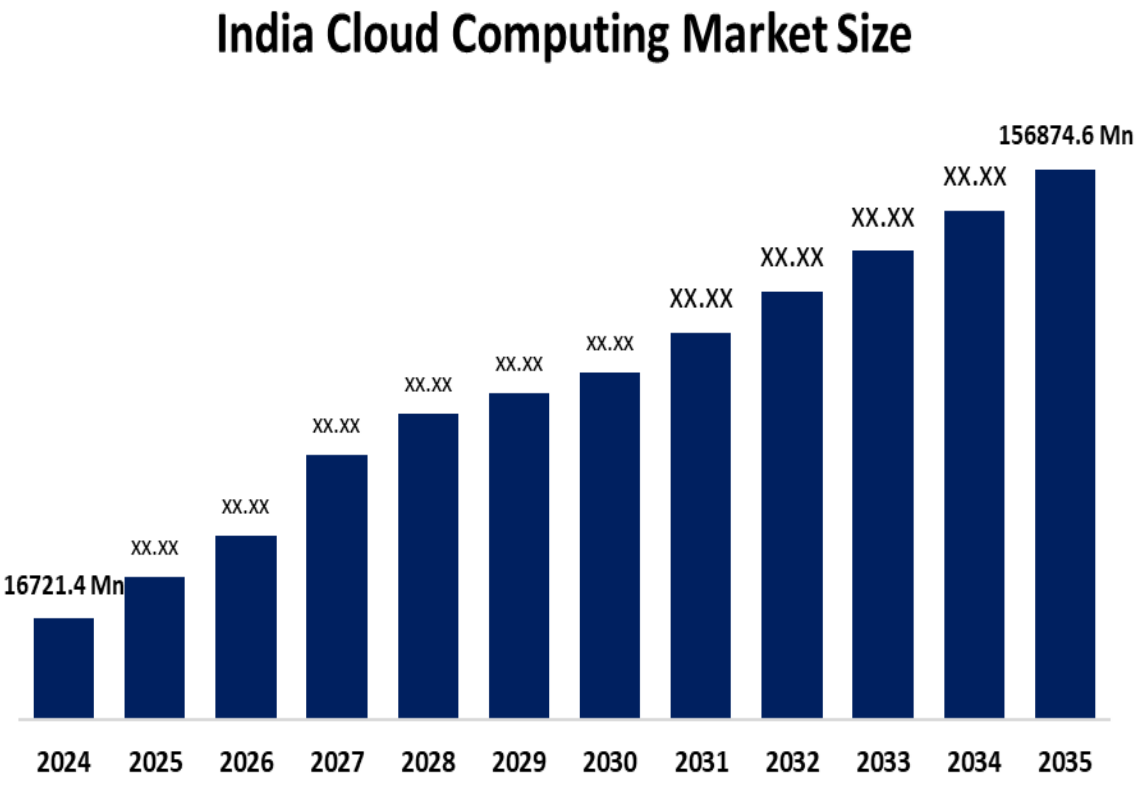
International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

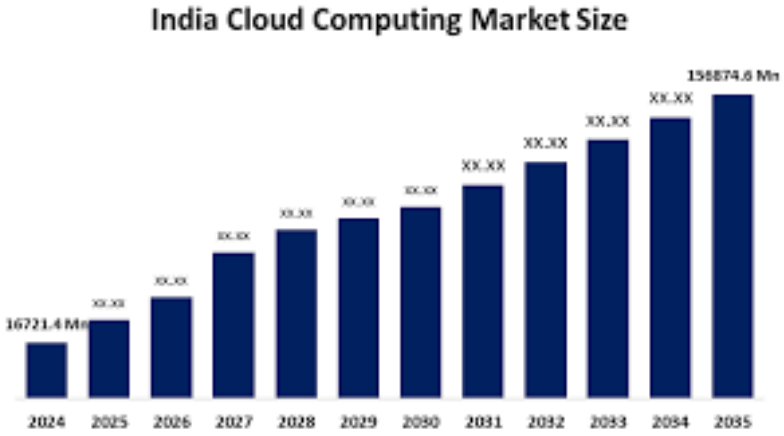
Ex- Google apps, Dropbox

b) Infrastructure as a Service (IaaS): Hardware as a service is another name for IaaS.
Customers can use this service to rent IT infrastructure, including servers, networking, and storage, as needed.The IaaS cl oud computing platform lowers costs by removing the requirement for each firm to maintain its IT infrastructure.
Ex-Google compute engine, Digital Ocean

c) Platform a platform as a service (PaaS): PaaS is a service in which hardware and software tools are delivered online by a third-party source. Customers can run, manage, test, and debug their apps on this platform. The user can run all of the hardware and software resources on a platform provided by a PaaS provider.PaaS makes it possible to avoid the hassle and cost of purchasing or maintaining software. software.
Ex- Windows Azure, Google App Engine.

VI. RAPID GROWTH OF CLOUD COMPUTING [9]





International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

Figure 4: Rapid Growth of Cloud (2024-2035)

VII. RISKS TO CLOUD COMPUTING SECURITY

Figure 3: Security Risk In Cloud Environment

A Similar to how a coin has two sides, every subject has two sides. We have studied and learned about cloud computing's many benefits and how it has emerged as one of the hottest technologies of our time. However, cloud computing also presents a number of difficulties and problems, the most significant of which are related to security. It is thought to be the largest obstacle to cloud computing's success. Cloud computing presents numerous and significant security challenges. Let us take a quick look at some of the main security concerns with cloud computing.

i. UNAUTHORISED ACCESS – Unauthorized system access that results in infiltration and data breaches is the other main security concern with cloud computing. The most common causes of account hijacking are social engineering, password theft, and phishing attempts. Similar to unlawful access, authorized users' access intended to damage the cloud can likewise be risky.Any external user can easily cause a data breach and compromise cloud security thanks to these access points.

ii. MISCONFIGURATION - When cloud security controls are improperly set up or left vulnerable, security misconfiguration occurs, endangering our system and data. To put it simply, misconfiguration occurs when resources on public cloud servers are not set up properly, leaving the system vulnerable to intrusions and attacks. One of the most significant and frequently disregarded security vulnerabilities in cloud computing is misconfiguration. Because of cloud misconfiguration, the majority of businesses are concerned about security.

iii. DATA LEAKAGE– Data sharing has been a simple process since the advent of cloud computing. However, many businesses are also quite concerned about data sharing because of the potential of data leaks, which is particularly high when it comes to sensitive and crucial business data. Since cloud computing is a multi-user environment that also incorporates third-party users, data leakage is a possibility. This means that anyone, anywhere, can view the data.

iv. INSECURE API'S–Application programming interfaces (APIs) facilitate the operation of cloud computing operations; if they are not secured, they might give hackers the chance to compromise the system and take advantage of sensitive personal information. Since every company now makes its interfaces available to the public for business partners to access, cloud APIs have become a prime target for attackers. This means that the data is readily available online and can be exploited in any way.

v. LACK OF VISIBILITY/CONTROL – The organization or user who uses cloud services loses control over the data and has less visibility after they store all of their data there or give the cloud system provider permission to handle or maintain their data. They are no longer able to monitor their data and are unable to confirm their security measures. After utilizing cloud services, a business may encounter a number of additional problems in addition to these. Protecting data and resources from security breaches and cyber threats is made more challenging when there is a lack of transparency and control over them.

vi. DISTRIBUTED DENIAL OF SERVICE ATTACKS – i. A cloud-specific attack that impacts every cloud layer is DDoS. Multiple machines target a single system or user in this type of assault by sending a lot of data packets, filling the network

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

with undesired traffic and preventing the user from using their resources. Both the system and the organizations who use it are impacted by this attack since they are unable to access their data. Because cloud data is shared online, it is vulnerable to virus infestations and cyberattacks.

VIII. FUTURE ADVANCES IN THE FIELD OF CLOUD COMPUTING:

In the coming years, the IT industry is expected to move rapidly toward automation. Technologies such as Artificial Intelligence (AI) and Machine Learning (ML) are likely to play a major role in this transformation. As automation continues to grow, the demand for traditional programming jobs may gradually decrease.

For example, in an automated environment, machines may begin creating and managing logic instead of humans. While this improves efficiency, it can also increase security risks. A human attacker may take considerable time to exploit computer resources, but a machine powered by AI and ML can perform the same task within seconds. In such situations, traditional security systems like Intrusion Detection Systems (IDS) may no longer be sufficient. Therefore, there is a strong need to enhance existing security mechanisms such as firewalls and IDS technologies.

According to cybersecurity reports, the use of internet and cloud-based services is expected to grow significantly in the coming years. As more Internet of Things (IoT) devices connect to cloud platforms, the workload on cloud systems will also increase. This growth may lead to more advanced security threats that current protection methods may not be able to handle effectively.

Hence, continuous research and innovation are necessary to strengthen cloud security, improve protection systems, and develop advanced technologies capable of defending against modern cyberattacks in highly automated environments.

IX. CONCLUSION

In conclusion, cloud computing is one of the most advanced and rapidly growing technologies, offering significant benefits to individuals, businesses, and organizations. However, challenges related to security and privacy still require further research and effective solutions. Although cloud computing has transformed the IT industry, it continues to evolve and improve.

Leading technology companies such as Google and Microsoft are actively working to strengthen cloud security and address existing vulnerabilities. Due to its flexibility, scalability, and cost-effectiveness, cloud computing has already gained widespread popularity and is expected to become an essential technology worldwide.

Despite certain limitations and concerns, cloud computing has introduced a new era in the IT sector. Since the technology is still in its early stages, there remains enormous untapped potential and many opportunities for future advancements and innovation.

REFERENCES

1. C. Stouffer, "23 cloud security risks, threats, and best practices," Norton, 2023. [Online]. Available: https://us.norton.com/blog/privacy/cloud-security-risks https://en.wikipedia.org/wiki/Cloud_computing
2. O. Can et al., "A comprehensive literature of genetics cryptographic algorithms for data security in cloud computing," Cybern. Syst., pp. 1–35, 2023
3. Sunarjo, R. A., Widjaja, A. E., Magdalena, L., Azzudin, M., Effendi, W. W. A., Friandi, S. Z., & Ikhsan, R. Z. (2025, August). Addressing Cybersecurity Risks in Multi Cloud Environments for Digital Transformation. In 2025 4th International Conference on Creative Communication and Innovative Technology (ICCIT) (pp. 1-6). IEEE
4. Al-Muhtadi, J., Shahzad, B., Saleem, K., Jameel, W., & Orgun, M. A. (2019). Cybersecurity and privacy issues for socially integrated mobile healthcare applications operating in a multi-cloud environment. Health informatics journal, 25(2), 315-329.
5. Dey, S., Sarma, W., & Tiwari, S. (2023). Deep learning applications for real-time cybersecurity threat analysis in distributed cloud systems. World Journal of Advanced Research and Reviews, 17(3), 1044-1058.
6. Christina A A, “Proactive measures on account hijacking in cloud computing network” published in Asian Journal of Computer Science and Technology, vol.4, 2015, 31-34. 6.
7. Choubey R, Dubey R and Bhattacharjee J, “A survey on cloud computing security challenges and threats” published in International Journal on Computer Science and Engineering (IJCSE), vol.3, 2011, 1227-1231.
8. Dinesha H A and Agrawal V K, “Multi-level authentication technique for accessing cloud services” published in International Journal on Cloud Computing: Services and Architecture (IJCCSA), vol.2, 2012, 31-39.
9. https://www.grandviewresearch.com/horizon/outlook/cloud-computing-market/india/2026
10. V. Raja, “Exploring Challenges and Solutions in Cloud Computing: A Review of Data Security and Privacy Concerns,” Deleted Journal , vol. 4, no. 1. p. 121, Apr. 30, 2024. doi: 10.60087/jaigs.vol4.issue1.p141.