A review on: security challenges and applications of cloud computing

Francis k. Mupila
PhD Scholar/ Visiting Faculty, Amity University Uttar Pradesh Noida sector 125, India
Dr Himanshu Gupta
Associate Professor, Amity University Uttar Pradesh Noida sector 125, India

Abstract
Cloud computing has become increasingly popular due to its scalability and cost-effectiveness, but its adaptability and flexibility can lead to security challenges when examining failed policies or malicious activities. Using the network, cloud computing has the ability to offer users more adaptable and cheaper services. Cloud computing has expanded dramatically over the past several years thanks to the resources' scalability, giving the impression that this area of the IT industry is growing quickly. Cloud computing has increased the number of security challenges, leading to users losing faith in it due to a lack of security. There are many security concerns with cloud computing, including multi-tenancy, elasticity, security performance, and optimization. This paper provides a thorough analysis of the cloud computing architecture, including deployment tactics, service level agreements, cloud components, and security. It also covers the security issues associated with transferring data to the cloud and provides a practical solution to mitigate any potential risks. It dynamically increases the organization's capacity without spending money on new hardware, personnel, or software licenses. We shall talk about a few clouds computing issues in this paper. It also examines some of the security measures now in use for cloud computing security, educating researchers and professionals about various security risks. This paper seeks to advance our understanding of cloud computing techniques. This paper's main goal is to act as a reference and manual for ongoing research initiatives. In-depth applications that have already benefited from cloud apps are investigated in the paper.
Keywords: 1. Cloud computing, 2.architecture, 3.security challenges, 4.applications.

1. Introduction

One of the numerous benefits of cloud computing is that it is a more adaptable way to get storage and processing resources on demand. It increases information technology capacity and flexibly adds capabilities without requiring additional funding for pricey infrastructure, software licensing, or staffing. Instead of needing to make substantial infrastructure expenditures, businesses are increasingly embracing cloud services to lower their initial operational expenses by investing in the capabilities they really use.For shared resources that can be swiftly built and provisioned with minimum managerial participation, cloud computing [1] offers quick, simple, and on-demand network connectivity, as shown in figure 1. Cloud computing is described by the National Institute of Standards and Technology (NIST). Quick adoption, efficiency improvements, and insufficient funding are the main drivers for cloud service use among enterprises.

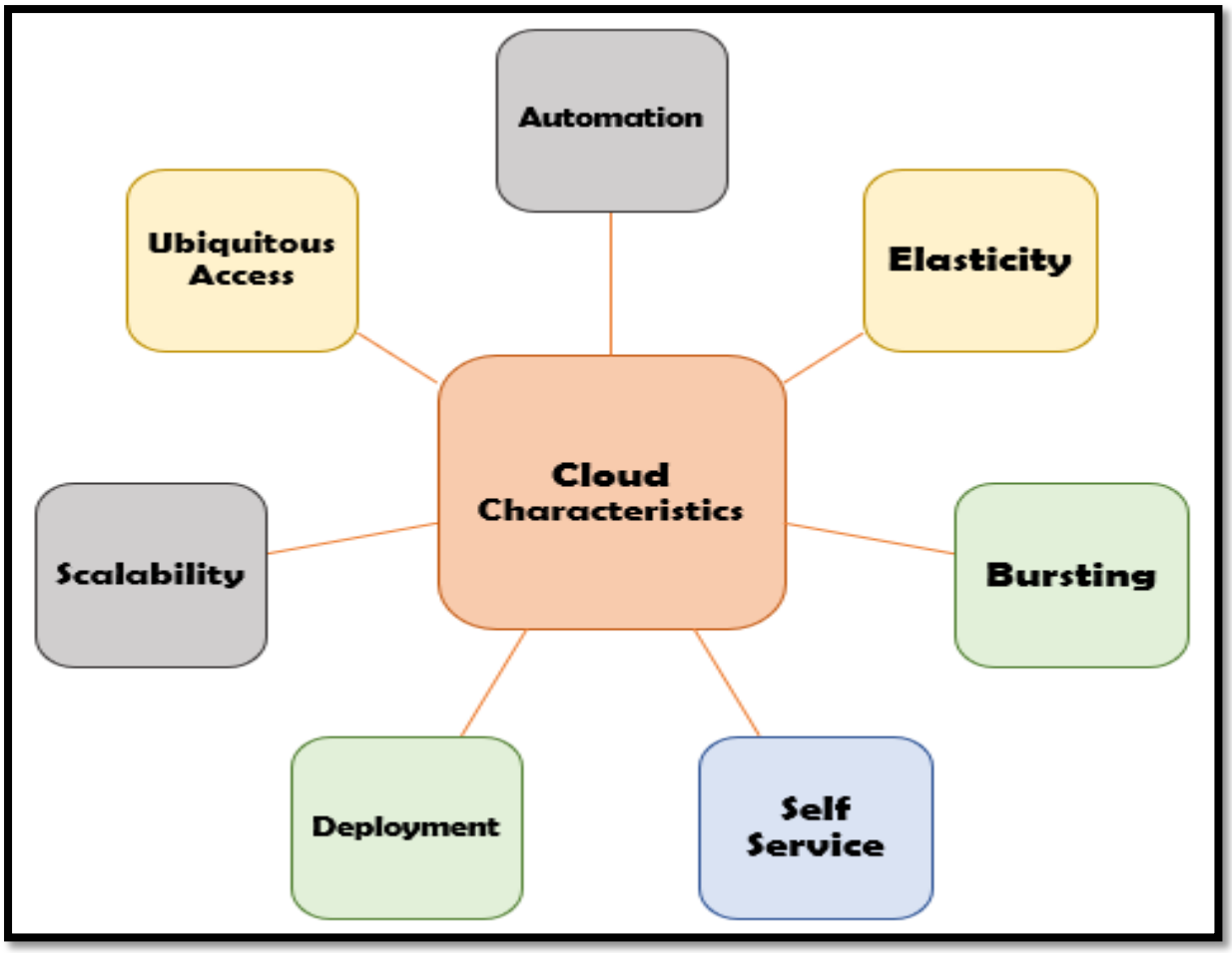

Figure 1: Cloud characteristics

Cloud computing is a network of digitized computers that allows for the dynamic presentation and provisioning of virtual servers in accordance with service level agreements (SLAs) that have been established by the participants in the agreement between customers and service providers. It provides unlimited virtual machines, high efficiency, monitoring systems, virtualization mitigation, quick adaptability, extensibility, and accessible solutions with top-notch performance [2]. Cloud computing is a relatively new computing paradigm with significant obstacles to its adoption, such as security, data safety, regulatory concerns, and constitutional concerns. Companies like Microsoft, Google, Amazon, IBM, and others have built cloud computing platforms to enhance their services, but there is uncertainty regarding safety at all thresholds, including the cloud service, communication network, data given, and application. There are also significant obstacles to its adoption [3]. The comparison features between traditional computing and cloud computing are shown in table 1. The administration of information and its accompanying activities is a significant concern when collected data and software solutions are transferred from the cloud to enormous data centers. The usage of cloud computing may present a number of security difficulties, including those relating to control and privacy, accessibility and virtualization flaws, the administration of credentials and identities, confidentiality, and the integrity of respondent device authentication [4].The market maturity and growth in cloud computing use are both accelerating because network operators guarantee challenging system security, accountability, and compliance standards. The adaptability and increased efficiency that cloud services would offer will contribute to this expansion.

Table 1: Traditional vs cloud computing comparison

Traditional Computing	Cloud Computing
Static	Dynamic
Internal networks	Over the internet
Administrative over head	Reduce admin function
Non-shared	Scalable and elastic
Providing for month	Provisioning for minutes
Dedicated consumption	Shared consumption
Traditional hardware procurement	Self-service
Manual data entry is used	Data are automatically entered
There is no remote system access.	There is remote access to the system.
Loss of transactional time	Transactions don't take much time.
Single tenant	Multi-tenant

Cloud computing has enabled users of on-premises systems to save money on hardware and software upkeep. This research provides an overview of architectural for cloud computing [5], reliability, management, and service models. While there are many benefits to distributed computing, security issues and worries should not be ignored when choosing an innovation model. Researchers and consultants agree that while cloud computing offers many benefits, its security is still vulnerable to attacks and other dangers, especially when it comes to resource sharing and virtualization.There is a growing need for security and trust in business cloud applications due to the lack of security components and controls in distributed computing [6] that can guarantee cloud security and privacy. Additionally, the user's availability weakness was mentioned, and an improved data encryption technique was suggested to address this.In order to promote reliability and trust, this research aims to define the security difficulties and obstacles in cloud computing. When discussing security solutions, it considers the requirements, risks, and requirements. Also, to increase the dependability and trustworthiness of calculations, it is therefore necessary for increasingly efficient components that ensure the rightness and accuracy of results provided by cloud assets.

The rest of this paper is structured as follows: A survey of the cloud computing literature was provided in Section 2, and a detailed study of the cloud architecture is provided in Section 3. The presentation of the security issues with cloud computing is the focus of Section 4. The cloud computing applications were discussed in Section 5. Section 6 offers a conclusion and looks at potential directions for additional research.

2. Literature Review

Over the past few years, the use of internet-based computing platforms, programs, and resources has increased dramatically, offering numerous benefits to businesses and organisations. Yet cybersecurity is a significant issue. This is primarily because this technology offers businesses and organisations a wide range of benefits. Cybersecurity, however, is one of the biggest issues and concerns with the expanding usage of cloud computing [7]. Cloud computing offers numerous benefits to businesses and organisations, but cybersecurity is a major issue. Data security, infiltration threats, data protection, and data security are among the security issues associated with cloud computing. The availability of open-access data, methods, open-source software, tools, technologies, and infrastructure would improve public health's capacity to conduct mapping and spatial analysis quickly for decision-making.Innovations in science and technological, such as artificial intelligence techniques and machine intelligence, and data cubes, are making it easier to find solutions for big data storage and analytics from EO, as well as production of analysis-ready data to speed up risk models. Infrastructures [8] such as cloud environments and high-performance computing systems are also being explored.

In 2018, the author proposed an authentication schemes provide efficient and adaptable security services to cloud tenants, which can be provided by third parties or renters. The provision of this security may be made by third parties, or renters may use it to monitor their virtual machine instances (VMs). In 2019,

reviews focused on the risk and risk factors associated with cloud migration process. Review the cloud computing idea and go over the numerous problems that have come up in the cloud computing ecosystem in 2020. In the study, some typical security risks are covered. Different breaches are described. The study concludes that the data must be protected from breaches by increasing the level of security.

According to some authors, cloud computing has advanced significantly in terms of utilising modern technologies. The practise of integrating cloud services into an organisation appears to be gaining popularity. Organizations [9] need to think about using cloud services as a crucial component of their foundations to save on capital expenses. However, a number of obstacles are preventing widespread adoption and deployment, and implementations of cloud services lack a high level of security, with the key issues being collection protection, information protection, information assurance, interoperability security, and vulnerability scanning. The primary goal is to safely manage and keep the information that doesn't fall under the control of the data owner. The existing cloud service implementations' greatest flaw is their inability to provide a widely acknowledged high level of security. Implementations of cloud services don't generally have a sufficient degree of safety. The company is employing a bottom-up strategy for security, focusing on smaller cloud-related issues [10] in order to address the more significant issue of cloud security. They are also using secure co-processors to improve security and have put Hadoop to use. There are numerous new technologies developing quickly, each with the potential to progress technology and simplify human life. New technologies are developing quickly, but one must be aware of the security dangers and difficulties posed by using them.

The authors investigate several architectural designs in 2021 based on the services they offer. Data centres are centrally located spaces with enormous volumes of data storage where processing and data are kept. On servers, processing and data are kept. Customers must have faith in the provider about data security and availability before transferring data to a public cloud, and difficulties with stability and adaptability requirements must be resolved. A reliable monitor that can audit the cloud server's operations has been installed there. Cloud computing has both positive and negative effects on information security, so it is important to have a reliable monitor and guarantee a specific cloud computing [11] service level to reduce potential security trust issues and adhere to governance challenges. Some authors focus on a new technology that is predicted to lower the cost of old technologies.

The use of the cloud [12] Industry influences information security in both a beneficial and detrimental way. Whether we can maximise its advantages while minimising its drawbacks will determine the outcome. Only in this way can the cloud become a platform for increased productivity, actual cost savings, and security. Cloud computing security is important for the safety of information, whether it is at rest or in transit. To protect data from external attacks, a secure cloud framework is recommended. The confidentiality of data, no matter if it's at rest or in transit, is one of the main security issues with regard to cloud infrastructure. In order for a cloud's content to be secure, this paper discusses cloud computing security challenges and recommends a completely secure cloud framework. The most important security [13] concerns relating to cloud infrastructure are covered in this paper. There are several security concerns. The topic of cloud computing security issues is then covered, which are essential for a cloud's data to be secure. To protect the data from outside threats, the next secure cloud architecture is suggested. The paper discusses the benefits and drawbacks of cloud computing, security threats and mitigation strategies, and a proposal for cloud computing in a smart power grid. The study of network security technology will benefit greatly from the paper's significant implications for the mechanization of communications and the popularization of the national economic information network.

3. Architecture for Cloud Computing

Four deployment models make up the cloud computing architecture: commercial, corporate, collaborative, and mixed. The deployment models demonstrate how cloud computing services can be employed by the computer infrastructure to offer services [14]. The user gets access to the three cloud service models: infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS). There are different layers of security needed for these service models in the cloud environment. The architecture of cloud computing is shown in Figure 2.

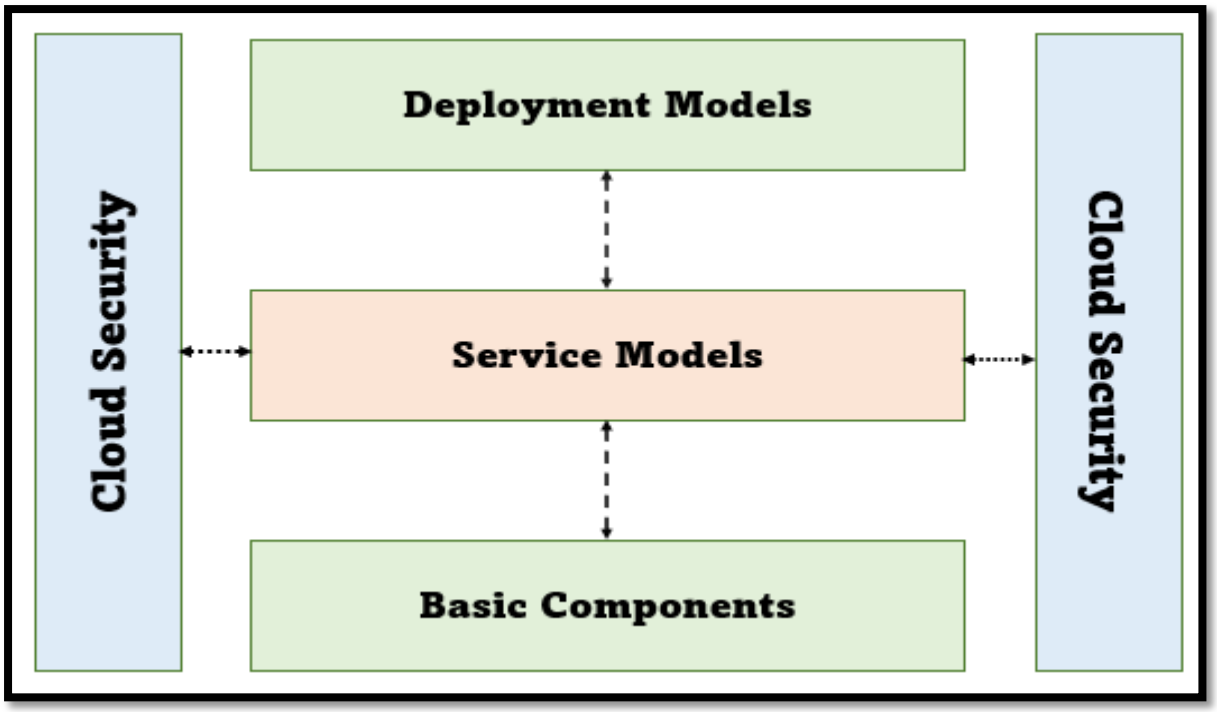

Figure2: Architecture for cloud computing

A variety of services are offered by the cloud and are accessed online. The management of resource allocation, the delivery of services, and the upkeep of security are the objectives of the cloud service provider. The five main components of cloud services are listed in Table 2. Cloud security is a necessary and difficult task when shared resources or data are transported to the cloud using a client-server architecture.

Table 2: Full analysis of the cloud computing architecture

Cloud deployment models	
Public Cloud	A service level agreement (SLA) between the consumer and the empowerment strategy in a public cloud, which is managed by the service provider, is known as a SLA.
Private Cloud	The cloud infrastructure is managed and maintained by a lone business that caters to several clients.
Hybrid Cloud	Two or more cloud deployment strategies—public, private, or community clouds—can be combined to create a hybrid cloud. These clouds continue to exist as separate, distinct entities even though they are connected.
Community Cloud	When a company shares its network infrastructure with customers who have a similar interest or set of concerns, such as those pertaining to policy, security requirements, mission, and compliance, the practise is known as community cloud.
Cloud Service Models	
Infrastructure as a Service (IaaS)	IaaS maintains physical servers, including server farms, storage, microprocessors, network infrastructure, routers, and a variety of those other

	infrastructure services, and offers standardized computing resources via the internet. Any software can be launched and deployed by the user as they see fit.
Platform as a service (PaaS)	PaaS serves as the middleware for the service model, providing amenities in the shape of packages, programs, IDEs, and development platforms maintained by the supply functions.
Software as a Service (SaaS)	The SaaS model refers to a group of remotely hosted apps that the service provider makes available to consumers on demand via the internet. Instead of giving the ability to develop software or applications, the SaaS model provides enterprise users with the capability of business software at a comparatively low cost.
Cloud Basic Component	
Hypervisor	The Virtual Machine Monitor (VMM) or manager, often known as the hypervisor, is a piece of hardware or firmware and software that enables the running and creation of many virtual machines on a single hardware host.
Virtualization	Several customers or organisations can share the resources of a physical instance thanks to virtualization. Making one physical resource identical to numerous virtual resources is helpful.
Storage	Clients utilise cloud storage across a network so that data may be remotely backed up, managed, and maintained. The service provider's main objective is to allay client worries about the security features built into their services, such as encryption and authentication.
Multi-tenancy	In a multi-tenancy system, there is a particular instance of corporate software that can accommodate numerous clients.
Cloud Network	The term cloud networking refers to the use of the internet to access network resources from a centralised service provider. Customers can share network and compute resources in this cloud.
Cloud Security	
Cloud Storage Security	Cloud storage adoption and popularity present security challenges, and IT professionals caution that file-sharing programmes and cloud storage come with inherent risks, whether they are virtual or physical.
Cloud Infrastructure Security	A distributed workforce can be made possible by cloud computing, but users must comprehend the basics of operating the cloud infrastructure to ensure secure deployment, data processing, collaboration, and safety procedures.
Software Security	Throughout all phases of development and production, the cloud provider was required to protect its software or apps against threats from

	both inside and outside.
Cloud Network Security	It is the duty of a cloud service provider to only permit legitimate network communication and to prevent all unauthorised traffic. Cloud providers do not share the access devices, such as switches and routers, that connect cloud virtual machine instances to the network of providers.

4. Challenges with privacy and security in cloud computing

Applications for cloud services are running on internal or external networks within cloud computing infrastructures. Cloud services are running on internal or external networks, and customers' assurances of the organization's capabilities to deliver services are used to illustrate the idea of trust in the company. The chosen cloud deployment methods, where the ownership is in possession of the applications and they are outsourced, are the foundation for credibility in the cloud computing environment [15].

In the conventional design, trust requires an effective security strategy that addresses operational restrictions and flows between them. External systems gain access to the restrictions that target the software that controls or affects access to consumer data. In cloud deployment methods, the entity that controls the cloud infrastructure [16] is given control by the community or public cloud. When a public cloud is established, the ability of the infrastructure owner to enforce an effective security policy ensures that the necessary security measures are taken to reduce risks and threats. In essence, cloud security refers to confidence in the computers and services used by the infrastructure owner.

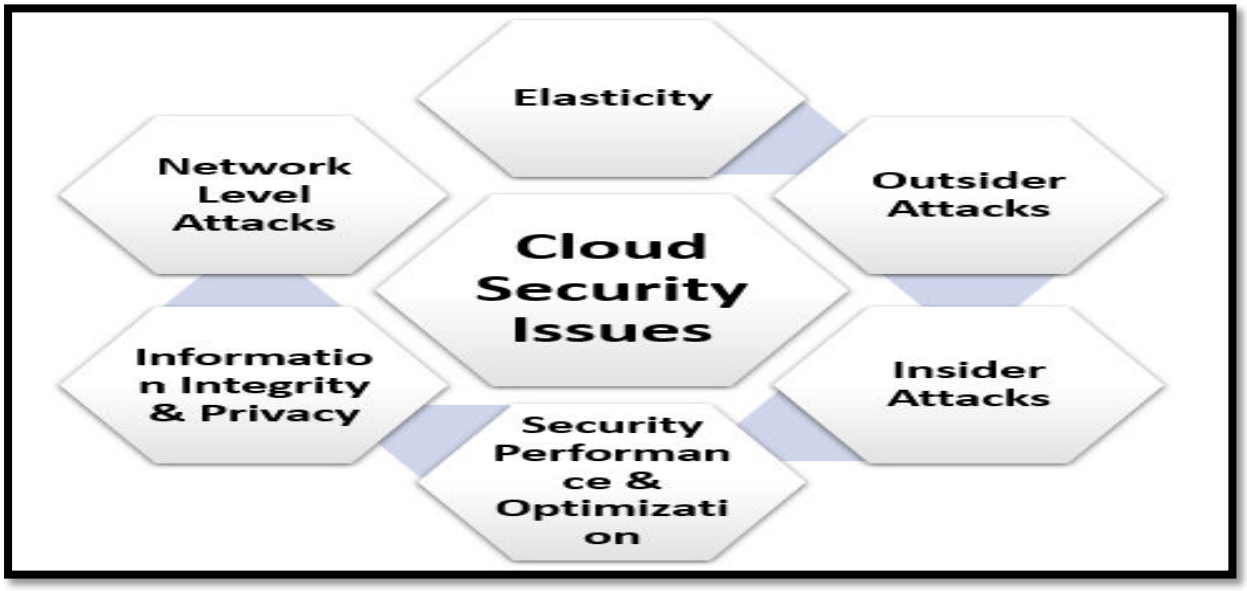

Figure 3:Cloud computing Security Issues

Cloud computing [15] presents security concerns due to the any correlation or exchange of information of organisations or systems to an outside organisation, which could allow someone to access information resources without authorization. However, the confidence of the company remains due to the fact that the private cloud infrastructure is controlled and operated by a private company, where no new security risks were presented. Figure 3 depicts the security concerns with cloud computing. The following are some specific cloud computing infrastructure security problems to be taken into consideration:

A. Authenticity

In cloud computing, data integrity is the upkeep of data kept on cloud servers to ensure it is neither destroyed nor altered by outside parties. Companies can boost customer confidence in their ability to safeguard data privacy and system integrity by providing more obvious ways to identify what or who might alter the information or data in the system. The system uses an authorization [17] method to decide

what kind of access, if any, a specifically authorised client should have to resources that are controlled by the system.The three primary entities involved in ensuring data integrity are the owner of the data, the cloud services provider to which the data was outsourced, and the auditor. The following are some design issues in the cloud that are addressed by the data integrity scheme:

- **Computation efficiency:**Before outsourcing to a cloud storage server, data might be pre-processed according to a data integrity scheme.
- **Communication efficiency:**Three key aspects of a data integrity scheme can be used to describe communication efficiency: the data owner's task proposal, the cloud storage server's challenge response, and the overhead associated with the initial transmission of information.
- **Reduced disk I/O:**The efficiency of disc I/O in the data integrity scheme is determined by the inefficiency of metadata accessibility, which prevents access for verification on the server storing data in the cloud.
- **Security:**Because data integrity systems are susceptible to various attacks, there are considerations while constructing them.

B. Confidentiality

Confidentiality is the process of keeping customer data private so that only authorised users or systems can access it. In regard to the services that cloud computing [6] offers (such as apps and associated infrastructures), cloud technologies have even more accessible systems and applications than ever before than private data centres do.

- **Multi-Tenancy:** The term "multi-tenancy" describes the shared nature of cloud resources such as data, memory, networks, and software.
- **Data Remanence:** Data is represented in residue that can be mistakenly erased or wiped because of an absence of equipment partitioning among diversity, a major, and the virtual partitioning of the server components on a single public cloud. This could lead to the unintentional disclosure of sensitive data.
- **Application safety and confidentiality:** User authentication is related to data confidentiality. Regulating access to many things, such as application, hardware, and recollection, is a significant difficulty for preventing hackers from accessing the customer's account.
-

C. Availability

Applications and infrastructure in the cloud are made available to ensure that authorised users can always access system resources on demand. Users can use the cloud computing models (IaaS, PaaS, and SaaS) to access applications and other services from any place at any moment.

D. Trusted Third Party (TTP)

TTP is a trusted third party that facilitates interaction between two parties and examines all transactions between them [18]. It provides a trusted security domain that explicitly takes into account the disappearance or loss of the conventional security barrier. It is an unbiased organisation that gives businesses confidence in electronic transactions through technological and commercial security aspects. The environment of cloud computing [2] [3] demanded TTP services, which demonstrate how to build the necessary level of trust and provide the best way to preserve the sincerity, authenticity, and informational and telecommunication confidentiality.

1) **Client-Server Authentication:** Certification is essential for ecosystem applications, network gadgets, virtualization software, and administration cloud services, which must all be certified by the certification authority in order to communicate with the cloud computing environment.

2) **High or low levels of confidentiality:** Data interruption or alteration risks are increasing, making it difficult to transmit data across a network. The complexity of the cloud computing environment

grows as a result of the lack of a traditional physical connection, necessitating protection not just for cloud traffic but also for communication among cloud hosts.

3) Data separation using encryption: Confidential information must be protected in the environment for cloud computing, which has become critical to the adoption of SaaS models. Data confidentiality, integrity, and privacy are maintained through the cryptographic separation of the data, calculations, and processes using an encryption mechanism that looks intangible to outsiders.

5. Applications of Cloud Computing

Cloud computing has essentially limitless applications. With the necessary middleware, a cloud-based computing system could execute all the services that a desktop computer could [12]. A cloud computing system might be able to run anything, from common word processors to specially made computer programmes for a particular business. Why would someone wish to run programmes and save data on a different computer system? Answer is the customers are able to access their data and give instructions from any Internet-connected computer at any moment and from anywhere in the world, with data not restricted to a single user's computer or business network. Costs for hardware may decline as a result. Systems for cloud computing would lessen the demand for sophisticated client hardware. Since the cloud system would meet your demands, you wouldn't have to buy the computer with the fastest processor and most memory. As an alternative, you might purchase a cheap computer terminal that comes with a monitor, just enough computer capacity to run the middleware required for connecting to the cloud environment, a keyboard, and a mouse. Since you would keep all your data on a distant computer, you wouldn't require a sizable hard disc.Businesses can save money on IT assistance by using cloud computing technology, which allows them to access computer applications across the entire firm without requiring a package of software or a licence for each employee. They can also pay a metered cost for cloud computing services [19]. Companies are not required to purchase a package of software or a licence for each employee. In theory, Hardware with fewer moving parts would be easier to manage than a network of uncoordinated devices and operating systems. Computer-using businesses need to make sure they have the right application in order to achieve their goals.Cloud computing [10] allows businesses to store data on another person's equipment, eliminating the need for physical space. Digital storage devices and servers require room. Because they are lacking it locally, several businesses rent physical space to house servers and databases.

6. Conclusion and Future Work:

Cloud computing is a modernized innovation that is predicted to dramatically lower the cost of existing technologies, which is the current development trend in the IT sector, but it has both advantages and disadvantages for information security [20]. The use of thecloud has many security risks, in addition to its benefits. We discussed the architecture of cloud computing in depth.This paper revealed security flaws, difficulties, hazards, and vulnerabilities in cloud-based systems and data transfers., which will encourage firms to move to the cloud. Further research is needed to improve service accessibility and quality, entice customers to use cloud computing, and boost confidence in TTP. Mitigation strategies for cyber threats will be used to support cost-benefit analysis and motivate companies to shift operations to the cloud. A component of cloud computing [9] services that meets security requirements is the development of a framework for an all-encompassing security and privacy trust evaluation management system to protect data from outside threats. To protect the data from outside threats, the next secure cloud architecture is suggested. The topic of cloud computing security issues is covered to ensure data is secure.

References

[1] Bennasar, H., Essaaidi, M., Bendahmane, A., & Ben-othman, J. (2021). A Systematic Literature Review of Cloud Computing Cybersecurity. Advances in Dynamical Systems and Applications, 16(2), 1883-1919.

[2] Mushtaq, M. F., Akram, U., Khan, I., Khan, S. N., Shahzad, A., & Ullah, A. (2017). Cloud computing environment and security challenges: A review. International Journal

of Advanced Computer Science and Applications, 8(10).

[3] Sharma, R., & Trivedi, R. K. (2014). Literature review: Cloud computing-security issues, solution and technologies. International Journal of Engineering Research, 3(4), 221-225.

[4] Kannan, T. V., &Arvindhan, M. A nAnalysis of cloud computing security challenges-a conceptual framework for cloud computing early adopters as a technology model.

[5] Ahsan, M. M., Gupta, K. D., Nag, A. K., Poudyal, S., Kouzani, A. Z., & Mahmud, M. P. (2020). Applications and evaluations of bio-inspired approaches in cloud security: A review. IEEE Access, 8, 180799-180814.

[6] Abdulsalam, Y. S., &Hedabou, M. (2022). Security and privacy in cloud computing: technical review. Future Internet, 14(1), 11.

[7] Popović, K., &Hocenski, Ž. (2010, May). Cloud computing security issues and challenges. In The 33rd international convention mipro (pp. 344-349). IEEE.

[8] Gupta, N., Maashi, M. S., Tanwar, S., Badotra, S., Aljebreen, M., &Bharany, S. (2022). A Comparative Study of Software Defined Networking Controllers Using Mininet. Electronics, 11(17), 2715.

[9] Soofi, A. A., Khan, M. I., & Amin, F. E. (2017). A review on data security in cloud computing. International Journal of Computer Applications, 96(2), 95-96.

[10] Aljawarneh, S. A., &Yassein, M. O. B. (2016). A conceptual security framework for cloud computing issues. International Journal of Intelligent Information Technologies (IJIIT), 12(2), 12-24.

[11] Alouffi, B., Hasnain, M., Alharbi, A., Alosaimi, W., Alyami, H., & Ayaz, M. (2021). A systematic literature review on cloud computing security: threats and mitigation strategies. IEEE Access, 9, 57792-57807.

[12] Sharma, M. A., & Sinha, G. (2021). An Efficient Approach on Data Security with Cloud Computing Environment: A Comprehensive Research. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 12(14), 1372-1382.

[13] Sen, J. Security and Security and Privacy PrivacyPrivacy Issues in Cloud Computing Computing. Innovation Labs, Tata Consultancy Services Ltd., Kolkata, INDIA.

[14] Gupta, N., Tanwar, S., Badotra, S., &Behal, S. (2022). Performance Analysis of SDN Controller. International Journal of Performability Engineering, 18(8).

[15] Soewito, B., Gaol, F. L., &Abdurachman, E. (2022). A systematic literature Review: Risk analysis in cloud migration. Journal of King Saud University-Computer and Information Sciences, 34(6), 3111-3120.

[16] Che, J., Duan, Y., Zhang, T., & Fan, J. (2011). Study on the security models and strategies of cloud computing. Procedia Engineering, 23, 586-593.

[17] Anuradha, M., Jayasankar, T., Prakash, N. B., Sikkandar, M. Y., Hemalakshmi, G. R., Bharatiraja, C., & Britto, A. S. F. (2021). IoT enabled cancer prediction system to enhance the authentication and security using cloud computing. Microprocessors and Microsystems, 80, 103301.

[18] Karmakar, A., Raghuthaman, A., Kote, O. S., &Jayapandian, N. (2022, April). Cloud computing application: Research challenges and opportunity. In 2022 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS) (pp. 1284-1289). IEEE.

[19] Tanwar, S., Gupta, N., Iwendi, C., Kumar, K., &Alenezi, M. (2022). Next Generation IoT and Blockchain Integration. Journal of Sensors, 2022.

[20] Zhang, Q., Cheng, L., &Boutaba, R. (2010). Cloud computing: state-of-the-art and research challenges. Journal of internet services and applications, 1, 7-18.