iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** X **Month of publication:** October 2022

DOI: https://doi.org/10.22214/ijraset.2022.46980

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue X Oct 2022- Available at www.ijraset.com

Fundamentals and Research Issues on Cloud Computing

Saloni Mahesh Kargutkar[1], Shraddha Manoj Borkar[2]
[1]*M.E. Scholar, VIT, Mumbai University*
[2]*M.Com. Scholar, Mumbai University*

Abstract: ***Access control and data security are now two of the biggest issues with cloud computing. Users can access data from the cloud server through a process known as access control. There are numerous issues that arise while accessing data, including data security, lengthy access times, data loss, overhead, redundant data, etc. An overview of cloud computing basics is given in the first section of this paper. Additionally, this document also covers all cloud computing-related topics. Finally, future development directions for the cloud computing environment have been determined.***
Keywords: Storage, virtual machines, cloud service provided, client server, encryption, decryption

I. INTRODUCTION

Using parallel computing, virtualization, utility computing, and service-oriented architecture, cloud computing is a novel technology. When used to supply a service, the term "cloud" can refer to a combination of networks, hardware, storage, and interfaces. Users can now access cloud services from a variety of information technology (IT) organisations, including Google, Yahoo, Amazon, and others [1].

Users of cloud computing don't have to worry about any hardware, software, or other devices. Users in this case are unaware of the true location of their data on cloud servers. Users of cloud computing can share data using an infrastructure that is made available to them. Users, Cloud Service Providers (CSPs), and Data Owners (DOs) are the three stakeholders involved in cloud computing. Every user's profile is saved by the CSP, which also manages all tasks [2]. The CSP enables DOs to store their information or files on a cloud server, and users can retrieve these files as needed via the cloud server. There are only a few conditions for using cloud services:

1) The CSP must establish the access control policies before any data or services may be accessed.
2) A mapping of access policies between the CSP and organisations with the accessible resources is required in order to provide the user with the requested resource. The mapping of policies is always open to violation. In order to ensure secure access to resources, the business should enforce more access policies.
3) The DO is required to provide customers with all available data services.

The internet is the sole foundation for cloud services. We are aware that there are a lot of malicious individuals or hackers online. Therefore, security vulnerabilities with cloud services were common [3]. The most important privacy and security concern is access control. Traditional access control approaches cannot be used in a cloud setting due to their static nature. The development of any access control model must take into account a number of key aspects of cloud services, including a sizable number of dynamic users, a sizable quantity of resource, etc. For cloud computing, numerous access control strategies have already been put out [4–12]. The following are this paper's main contributions:

a) The principles of cloud computing are discussed in the first section of this essay.
b) Each concern or issue related to cloud computing is covered in detail in this document.
c) The cloud computing environment has also been given many future work directions.

The remainder of the essay is divided into sections. The principles of cloud computing are presented in Section 2. All of the cloud computing's concerns have been thoroughly covered in section 3. The future work directions are highlighted in Section 4. In section 5, the paper's conclusions are presented.

II. FUNDAMENTALS OF CLOUD COMPUTING

A. Definitions of Cloud Computing

In cloud computing, customers are provided with an infrastructure to utilise as a working space. There are numerous ways to define cloud computing. Following is a list of some of them: • "Cloud computing is a novel kind of IT outsourcing that doesn't yet adhere to enterprise IT standards and isn't backed by the majority of the major corporate vendors." Staten J, among others [13]. • "A Cloud is a type of parallel and distributed system made up of an assortment of connected, virtualized computers that are dynamically provisioned and presented as one or more unified computing resources based on service-level agreements established through negotiation between the service provider and consumers." - Buyya R et al.

B. Cloud computing history

There were huge mainframe computers in the 1950s. Users could not afford to purchase such a computer for personal use due to its high cost. They had established a technique known as "time sharing" as a result. A single computer could be used by several people thanks to "time sharing". J.C.R. Licklider attempted to connect all of the computers, which were dispersed throughout the world, in 1969 [15]. John McCarthy, a scientist, received input on the "cloud" notion from other specialists before he first proposed the idea of providing compute as a public service. When IBM introduced the VM operating system in the 1970s, IT businesses began to utilise virtual machines in practise. Multiple computers operate in the same processing environment in this infrastructure. Virtualization is the term for this kind of connection. In the middle of the 1980s, IBM introduced a user-friendly computer. Microsoft also donated its operating system at that time. The internet began to provide enough bandwidth in 1990, and businesses connected their employees' computers to one another. Salesforce.com was the primary cloud computing milestone in 1999 [16]. Delivering apps was its main objective. The following step of development was carried out by Amazon Web Services in 2002. Through Amazon Mechanical Turk, Amazon offered services such as compute, storage, and applications. Elastic Compute Cloud (EC2) by Amazon was made available for business use in 2006 [17]. Companies and individual users can host their own apps in the cloud thanks to EC2. When Google and IBM collaborated, cloud computing significantly increased in popularity in 2007. Web 2.0 debuts on the market in 2009. Google and other businesses began to provide browser-based applications through "Google Apps." Many IT organisations today are aware of the advantages of the cloud computing environment. Cloud computing provides users with a new working environment and expands storage capacity in the IT sector.

C. Cloud Computing Features

Cloud computing has a variety of features, including:

1) *Agility:* During a transaction, a system's environment may occasionally alter. The term "agility" refers to a system's capacity to react quickly to its dynamic surroundings.
2) *Reliability:* Reliability is improved when many sites are used. Additionally, it enables cloud computing for better disaster recovery and business continuity.
3) *Scalability:* Cloud computing can expand or contract its cloud services in response to customer demand.
4) *Pay-per-use:* In cloud computing, customers can make payments based on how frequently they utilise the services.
5) *On-demand Service:* Since users can access cloud services at any time, they are not a permanent fixture of the IT system.
6) *Resilience:* A CSP's "resiliency" enables it to ignore cloud server and persistent data storage failures.
7) *Performance:* Web services are used in cloud computing to monitor performance. The CSP has access to the cloud server's activity.
8) *Security:* Cloud services are now widely used by IT firms. Therefore, the CSP offers a reliable encryption method for users' sensitive data.
9) *Resource Pooling:* A cloud server can accommodate millions of users. Consider the 27 million users of "Skype."

D. Cloud Computing Benefits

Cloud computing has a number of advantages:

1) *Lower IT Costs:* Cloud computing has made managing and maintaining IT systems less expensive. Users utilise the resources of the cloud service provider in a cloud environment. There is no requirement to purchase pricey systems.
2) *Scalability:* In cloud computing, the system may swiftly scale up or down depending on the circumstance.
3) *Business Continuity:* The protection of data and systems is the most crucial component of business continuity planning. Data may occasionally experience numerous natural calamities. Data must therefore be stored on the cloud server for backup purposes.

4) Work practises can be more flexible thanks to cloud computing, which also enables customers to access data from their homes.
5) Storage is almost limitless thanks to cloud computing, so users don't have to worry about running out of room. Cloud computing offers practically limitless storage capacity.
6) *Speed:* If users are enrolled on the cloud server, they can access data from any location.

E. Cloud Computing Drawbacks

Cloud computing's drawbacks There are a number of drawbacks to cloud computing, which are described below:

1) *Security and Privacy:* The cloud servers are frequently accessed by hackers or other unauthorised users. They consistently attempt to hack into data or change their profile to one of the approved users. Cloud data must therefore be protected [18].
2) *Transferability:* If customers wish to switch from one cloud to another, the CSP must transfer all user data to the new cloud. Therefore, moving users from one cloud to another is rather challenging.
3) *Downtime:* On occasion, the website falls offline, making it impossible for users to access data stored on a cloud server.
4) *Comprehension:* It is really challenging to comprehend what is happening on the cloud server. The CSP keeps track of all kinds of information and keeps it private.
5) *Limited Control:* Because cloud computing apps and services are run from remote locations, by companies, or by other parties, users have limited control over them.

F. Service Delivery Model

Three services, namely Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS), are typically used to supply cloud computing [19].

1) *Software as a Service (SaaS):* In the SaaS model, the cloud provider offers a licenced version of a software programme. This programme is available for demand purchase by any business or consumer. On-demand software is another name for SaaS. Users of SaaS can make payments as needed, such as annually, monthly, weekly, or hourly. Salesforce.com, Google Mail, MuxCLoud, and other services are examples of SaaS providers.

Advantages of Saas Providers:

- One user can use several services from many SaaS providers when using SaaS, which eliminates the complexity of software installation.

2) *Platform as a Service (PaaS):* In PaaS, CSPs offer an environment complete with operating systems, databases, environments for running programming languages, and web servers. PaaS provides a cloud setting in which users can develop, execute, and deploy applications. Aneka, Azure, and other suppliers of PaaS are examples. PaaS has the following benefits:

- It gives users a comprehensive platform to develop software;
- Users don't have to worry about how much memory is required to execute the software.

3) *Infrastructure as a Service (IaaS):* IaaS is currently the most widely used in IT firms. The customer can typically access the cloud provider's infrastructure when using the IaaS approach. This infrastructure may include firewalls, storage, and networks. IaaS offers a variety of resources, including IP addresses, load balancers, virtual local area networks, raw storage, and software packages. IaaS suppliers include Amazon EC2, GoGrid, and others.

IaaS has the following benefits:

- It offers a way to control the SaaS and PaaS service models.
- IaaS can enhance network efficiency.

G. Model of Deployment

Private cloud, public cloud, community cloud, and hybrid cloud are the four basic types of clouds.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue X Oct 2022- Available at www.ijraset.com

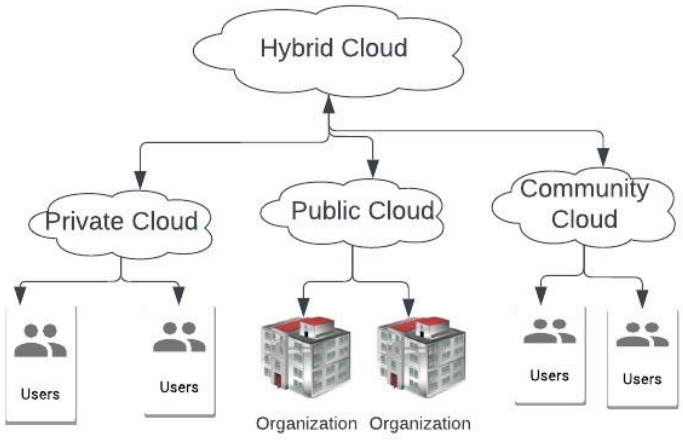


Fig. 1 Deployment model of cloud computing

1) *Private Cloud:* Cloud infrastructure that is completely managed by one company is referred to as a private cloud. Either an organisation or a third party may handle it. Resources are only accessible to an organization's clients in a private cloud, enhancing the security and privacy policy of that company. The cloud computing deployment model is shown in Fig. 1.
2) *Public Cloud:* The CSP offers the resources, including the network, server, etc. on the public cloud [20]. Here, customers can make payments based on how much of the public cloud they have used. In the public cloud, users or clients from many businesses collaborate and share the same network or cloud. There may be numerous attackers because there are numerous users from various corporations. Therefore, security issues are significant in the public cloud.
3) *Community Cloud:* In a community cloud, a number of companies that share common objectives share infrastructure or a cloud environment. All of these companies or a third party maintain the community cloud. The public cloud is occasionally used for purposes related to national security.
4) *Hybrid Cloud:* This type of cloud combines public and private clouds. The central administrator is in charge of running it [21]. The hybrid cloud provides safe access control between users and cloud providers and offers IT solutions by combining public, private, and community clouds.

III. CLOUD COMPUTING PROBLEMS

The CSP in cloud computing must make sure consumers don't run into issues with security or data loss. The following is a list of some cloud computing issues:

A. Accessibility

A major issue with all forms of clouds is availability. The purpose of using the cloud environment is to give users access to services from anywhere at any time. The majority of the infrastructure and platforms offered by CSPs today are built on virtual machines. Here, traffic directed to IP addresses can be blocked by virtual computers. The virtual machines are added alongside these security measures to increase system availability in the cloud.

B. Security of Information

To maintain user data privacy in a cloud environment is to maintain the confidentiality of the cloud environment. The management of user data, which is housed across many data centres, depends heavily on confidentiality. To safeguard sensitive user data, the CSP must enforce confidentiality at several stages of cloud applications.

C. Access Management

Only people who are authorised to access the data on the cloud server can do so thanks to access control. The CSP monitors all access requests made by clients or users of the Public Cloud, Community Cloud, Hybrid Cloud, Organization User Private Cloud, through access control. There are numerous procedures to follow when accessing data or a file, including authentication, authorization, and accountability.

Cloud computing makes sensitive data or files more vulnerable. Because of government surveillance of databases, there may initially be a lot of concerns. Any country, where data were not previously preserved, can store data in a cloud environment. It is permissible for the government of that nation to view the information [22]. Customers may receive no indication that a foreign authority has accessed their data. Second, any IT company employee with permission may give hostile users access to their database. Following that, malevolent people could access data or files on the cloud server.

D. Issues Associated

With Data the following list of data-related difficulties is provided:

1) *Data Integrity:* Maintaining information integrity in a cloud environment enables for the protection of user data from being altered by unauthorised users or CSPs. Data can occasionally be changed by hackers. The CSP is in charge of supplying the data integrity.
2) *Data Loss:* There may be data loss if the cloud provider suspends operations owing to a financial crisis or for other reasons. Users won't be able to access data in the future because the servers don't have any data.
3) *Data Leaking:* Data leakage occurs when data is obtained by unauthorised parties, such as hackers or malicious individuals.
4) *Data Locations:* Users have no idea where data is located. Users are unaware of the true storage location for the data. It could be kept within or outside of their nation.
5) *Unwanted Access:* Maintaining the secrecy of data or files in the cloud is fraught with risk. As an illustration, the government of a country can examine actual data if user information is housed there.
6) *Data Segregation:* In cloud computing, insufficient data isolation progressively raises the risk. Giving complete segregation of client data storage in the cloud server will solve this issue.
7) *Vendor lock-in:* This strategy enables customers to rely on the vendor's services. By developing IT solutions, vendor lock-in can be established. It's seen as one of the primary problems with cloud computing. When a vendor cease providing a service, the CSP tries to provide it from a different vendor, who may be located on a different cloud server.
8) *Data Deletion:* How can users be aware that their files or data have been completely destroyed from the server and cannot be recovered again? is another major problem with cloud servers. There are currently no methods to determine whether a user's data has been totally wiped.
9) *Data Analysis:* There are many distributed systems in a cloud computing environment. Information finding is therefore exceedingly challenging. The CSP takes a long time to examine the data when users request it. Consequently, providing data requires additional time.

E. Storage Related Issues

With the use of a cloud computing environment, data can be managed by a CSP or other party and saved on a cloud server. The data is divided into several tiny parts by the CSP. The CSP divides the data and then stores it in several data storage facilities. The data can be recovered from another piece of the data if any portion of the data crashes. There are numerous concerns regarding data storage, some of which are listed below:

1) *Security Company:* Many users are concerned about the resources' security because the CSP manages every aspect of a cloud environment and is unreliable.
2) *Ownership:* Some users worry about losing their own rights when data aren't used for a while. This issue is addressed by several CSPs through a robust agreement.
3) *Multiplatform Support:* In cloud computing, how services are integrated with various operating systems, such as Linux, OS X, Windows, etc., is a problem for IT departments.
4) *Data Recovery:* A cloud server mishap is possible. Data can thus be lost. The CSP is in charge of establishing the data backup.
5) *Data Portability and Conversion:* The CSP is primarily responsible for partitioning and transforming files or data. Following conversion, the CSP must retain the data's format so that it cannot be revealed to hostile users.

F. Policy Issues

Policy Concerns Depending on the cloud situation, a cloud environment's privacy varies. Some clouds pose modest privacy dangers, while others pose significant privacy risks. On the basis of the calendar, social networks, people's locations, and preferences, services are occasionally tailored. The cloud server has a lot of policy difficulties.

Following is a list of some of them:

1) *Insufficient user Control:* Data visibility and control are restricted in a SaaS cloud environment from the user's perspective. Therefore, the key query is how data are stored on the cloud server and how users have access to data. These are the obligations users have under the law.
2) *Unauthorized Secondary Use:* In the cloud context, unauthorised uses of data pose a significant risk. The CSP in cloud computing always seeks to make money off the usage of user data. Secondary data usage are frequently rejected by the CSP.
3) *Data Proliferation:* The potential of a cloud server to involve numerous parties when DOs do not have data control is referred to as "data proliferation." Transferring data from one cloud to another requires a legal 10 jurisdiction. Risk and legal complexity are so increased [23]. Dynamic provisioning: In cloud computing, it is unclear who entity is in charge of keeping track of private information or who establishes guidelines for how data should be handled.

G. Security Issues

There was a self-control system for managing data in the conventional model. Because sensitive information may be stored outside the user's own domain, cloud security becomes a delicate topic. The public cloud raises more than just privacy concerns. According to a recent survey [24], the biggest concern facing the cloud environment is security. In cloud computing, the main problems are related to determining who is in charge of what kind of security. There is no standardised API, which causes this division of security concern. The cloud security alliance claims that account theft, malevolent insiders, unsecured interfaces, and problems with shared technology are the key problems with cloud computing [25].

1) *Identity Management and Authentication:* The CSP uses the Identity Management (IDM) mechanism to identify users and deliver services. The interoperability of IDM is a significant issue. IDM is still not well understood in multitenant cloud servers.
2) *Backup:* It is exceedingly challenging to ensure proper availability and backup in a cloud computing environment. In the event of a breakdown, a backup of the data is essential.
3) *Lack of Standardisation:* The majority of problems are brought on by cloud computing's lack of standards. By providing better standards, Service Oriented Architecture (SOA) seeks to resolve numerous problems.
4) *Multi-tenancy* is a feature that allows one piece of software to run on a SaaS server and be used by a number of different businesses. A work scheduling technique is used by several CSPs to increase hardware efficiency. However, the majority of CSPs use virtualization to get the most out of their hardware.
5) Audit: From an audit standpoint, a lot of new difficulties have been developing in a cloud computing environment. To guarantee data integrity, the cloud server's transaction details require a proper record.

H. Trust Issues

The concept of trust is challenging with the cloud server. The intention to tolerate vulnerability based on optimistic expectations about another person's intentions or actions is known as trust [26]. One method of building trust online is security. Another element of trust is reputation, which is something that businesses value highly.

Many customers only consider a company's reputation. Persistent trust and dynamic trust are the two basic types of trust used in cloud computing. "Persistent trust" is related to a foundation with a long history. "Dynamic trust" addresses information that is transient or mutable.

1) *Weak Trust Connections:* The user is not always aware of all the details of a transaction as it is taking place. People used to become irritated about the data security in that situation rather than finding solutions. They may not always agree to use the CSP in the future.
2) *A Lack of Customer Trust:* The CSP occasionally requests customers to submit their personal data. However, this supply network breeds mistrust among consumers. The extent to which data on the cloud are protected is also in doubt [27]. As a result, users who are unaware of the risk refuse to use cloud servers.

I. Legal Aspects

Legal frameworks are a vital factor in the safeguarding of users' sensitive or confidential data. Such frameworks exist in every single nation. Sometimes it is uncertain which path a transaction will take to completion. Multiple nations may process a single transaction. Consequently, the judicial system in that nation compromises security.

Users of cloud computing are unaware of the precise location of the data storage. It might be kept anywhere in the world. So, depending on where the data is stored, a separate legislation may apply to the data.

Data and files are saved on the server in several copies. These copies are also controlled by various organisations. The location of data affects privacy legislation. Place restrictions also apply when sensitive data, such as financial or health information, is transferred [28].

J. Attacks on the Cloud Environment

Malicious users carry out a variety of attacks, which are crucial in a cloud setting.

1) *Denial of Service (DoS) Attack:* This happens when a user repeatedly sends the server erroneous requests. Unauthorized users frequently request access to sensitive cloud data on the cloud server.
2) *Cookie Poisoning:* Unauthorized users may attempt to alter cookies in order to access data. Cookie poisoning is the term for this ailment.
3) *Distributed Denial of Service (DDoS) Attack:* In a DDoS, attackers have control over data accessibility [29].
4) *Virtual Machine Checkout:* A lot of businesses today employ virtual machines. On their own personal computers, that company's employees frequently upgrade virtual machines. As a result, any employee may assault.
5) *Attack Involving Migration:* This happens when virtual computers are moved from one location to another.
6) *An Encryption attack is* used to gain access to private data on a cloud server by jeopardising security.
7) *DNS Attack:* Cloud hackers can quickly login to a network when a server is called by name. Therefore, if the data are not secured, unauthorised people may access the user's sensitive information.
8) *Sniffer Attack:* Occasionally, attackers can read the data's content with ease. Sniffer software may monitor all data travelling across a cloud network.
9) *Cloud Malware Injection:* In this attack, the attacker uploads a false copy of the data to the cloud server.

IV. FUTURE WORK DIRECTIONS

The following future opportunities are provided in this section based on the conversations above:

1) How security is provided for the user's sensitive data is still unclear. To safeguard the data, a solid standard (agreement) should be created.
2) In the conventional system, the CSP is constantly exposed to the access structure. Therefore, anyone with malevolent intent can quickly get into a user's data. As a result, a new model that offers great security can be created.
3) It is possible to create a suitable method that provides user data in a shorter amount of time. Therefore, users can use cloud services for less money.
4) It is possible to create a new technology that lowers the overhead in relation to the user base.
5) International data leaking is always a possibility with cloud computing. The data can be safeguarded against data leakage using a fresh technique.
6) Users will be able to detect and handle errors effectively with the introduction of a new scheme.
7) A new model could be created to stop the loss of data.

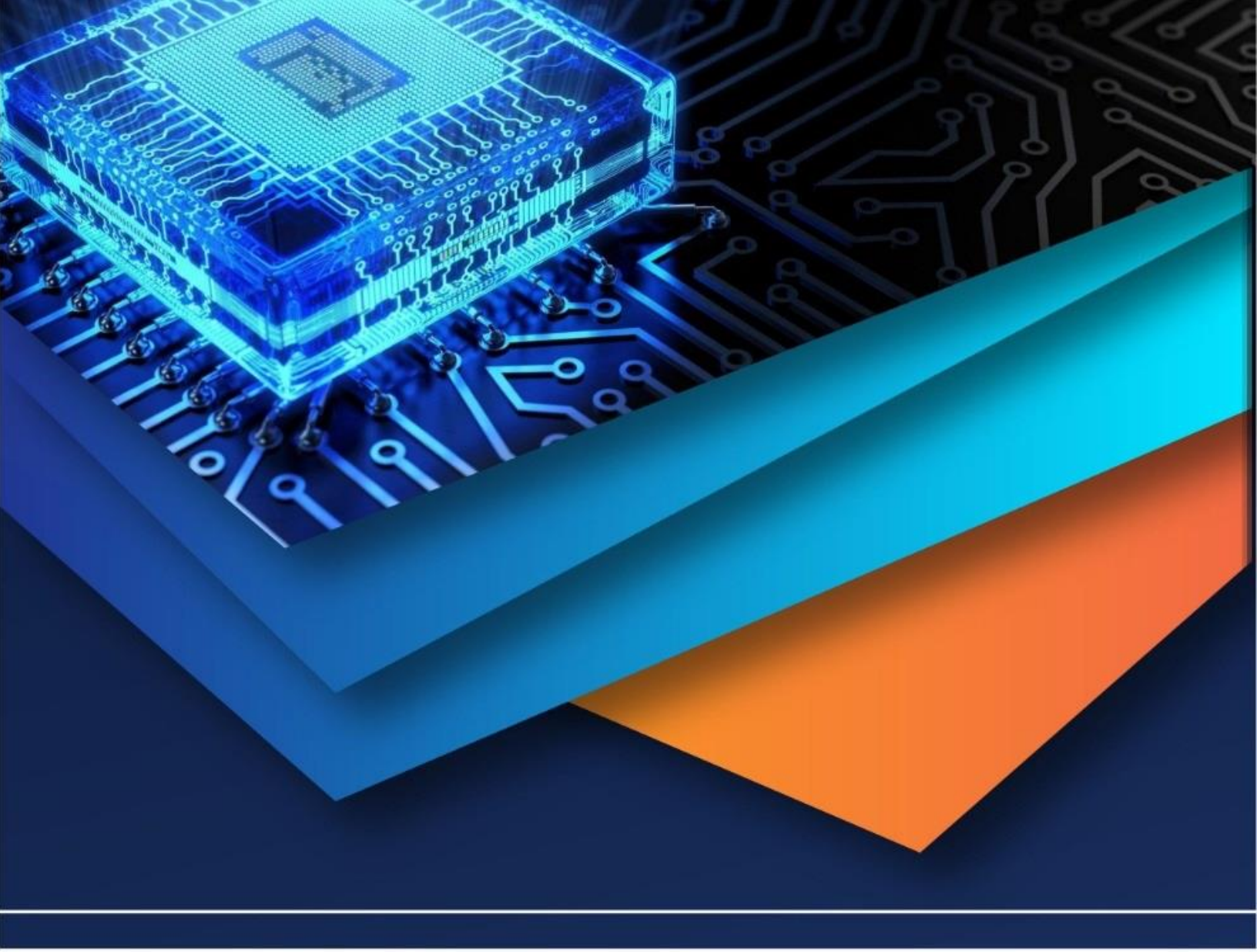
V. CONCLUSIONS

These days, cloud computing is quite well-liked due to its adaptability and affordability. In the first section of this essay, the basics of cloud computing are covered. This paper discusses a number of cloud computing security challenges, including availability, confidentiality, access control, data-related, storage-related, policy-related, security-related, trust-related, legal-related, and attacks on the cloud environment. Future research directions are also discussed in this paper. In the future, a new access control paradigm for effective data access can be created.

REFERENCES

[1] Q. Zhang, L. Cheng, and R. Boutaba, “Cloud computing: state-of-theart and research challenges,” Journal of Internet Services and Applications, vol. 1, no. 1, pp. 7-18, 2010.
[2] S. Namasudra, S. Nath, and A. Majumder, “Profile based access control model in cloud computing environment,” Proc. of the International Conference on Green Computing, Communication and Electrical Engineering, IEEE, Coimbatore, India, pp. 1-5, 2014.
[3] G. Anthes, “Security in the cloud,” Communications of the ACM, vol. 53, no. 11, pp. 16-18, 2010.
[4] B. Balamurugan, P.V. Krishna, N.S. Kumar, and G.V. Rajyalakshmi, “An efficient framework for health system based on hybrid cloud with ABE-outsourced decryption,” in Artificial Intelligence and Evolutionary Algorithms in Engineering Systems, L.P. Suresh, S.S. Dash, and B.K. Panigrahi, Eds., Springer, India, pp. 41-49, 2014.

[5] S. Namasudra and P. Roy, "Secure and efficient data access control in cloud computing environment: a survey," Multiagent and Grid Systems-An International Journal, vol. 12, no. 2, pp. 69-90, 2016
[6] B. Balamurugan and P.V. Krishna, "Extensive survey on usage of attribute based encryption in cloud," Journal of Emerging Technologies in Web Intelligence, vol. 6, no. 3, pp. 263-272, 2014.
[7] A. Majumder, S. Namasudra, and S. Nath, "Taxonomy and classification of access control models for cloud environments," in Continued Rise of the Cloud, Z. Mahmood, Ed., Springer, London, pp. 23-53, 2014.
[8] S. Sarkar, K. Saha, S. Namasudra, and P. Roy, "An efficient and time saving web service based android application," SSRG International Journal of Computer Science and Engineering (SSRG-IJCSE), vol. 2, no. 8, pp. 18-21, 2015.
[9] S. Namasudra and P. Roy, "A new table based protocol for data accessing in cloud computing," Journal of Information Science and Engineering, in press.
[10] B. Balamurugan and P.V. Krishna, "Enhanced role-based access control for cloud security," in Artificial Intelligence and Evolutionary Algorithms in Engineering Systems, L.P. Suresh, S.S. Dash, and B.K. Panigrahi, Eds., Springer, India, pp. 837-852, 2014.
[11] S. Namasudra and P. Roy, "A new secure authentication scheme for cloud computing environment," Concurrency and Computation: Practice and Exercise, 2016. DOI: 10.1002/cpe.3864
[12] S. Namasudra and P. Roy, "Size based access control model in cloud computing," Proc. of the International Conference on Electrical, Electronics, Signals, Communication and Optimization, IEEE, Visakhapatnam, India, pp. 1-4, 2015.
[13] J. Staten, "Is cloud computing ready for the enterprise?," Forrester, 2008.
[14] R. Buyya, C.S. Yeo, and S. Venugopal, "Market-oriented cloud computing: vision, hype, and reality for delivering IT services as computing utilities," Proc. of the 10th IEEE International Conference on High Performance Computing and Communications, Washington, DC, USA, pp. 5-13, 2008.
[15] B.R. Kandukuri, R.P. V, and A. Rakshit, "Cloud security issues," Proc. of the International Conference on Services Computing, IEEE, pp. 517-520, 2009.
[16] N.D. Naik and K.J. Modi, "Evolution of IT industry towards cloud computing: a new paradigm," IJRIT International Journal of Research in Information Technology, vol. 1, no. 5, pp. 236-242, 2013.
[17] J. Harauz, L.M. Kaufman, and B. Potter, "Data security in the world of cloud computing," IEEE Computer and Reliability Societies, pp. 61-64, 2009.
[18] I. Tsagklis, "Advantages and disadvantages of cloud computing-cloud computing pros and cons," 2013. Available: http://www.javacodegeeks.com/2013/04/advantages-anddisadvantages-of-cloud-computing-cloud-computing-pros-andcons.html
[19] E. Savolainen, "Cloud service models," in Seminar-Cloud Computing and Web Services, University of Helsinki, Department of CS, 2012.
[20] M.A. Morsy, J. Grundy, and I. Müller, "An analysis of the cloud computing security problem," Proc. of APSEC Cloud Workshop, Sydney, Australia, 2010.
[21] Global Netoptex. Demystifying the cloud-Important opportunities, crucial choices, 2009.
[22] Regulation of Investigatory Powers Act 2000, Part II, UK. Available: http://www.legislation.gov.uk/ukpga/2000/23/part/II
[23] I. Rastogi, A. Chandra, V.K. Gupta, and A. Vaish, "Privacy issues and measurement in cloud computing: a review," International Journal of Advanced Research in Computer Science, vol. 4, no. 2, pp. 81-86, 2013.
[24] P.K. Mckinley, F.A. Samimi, J.K. Shapiro, and C. Tang, "Service clouds: a distributed infrastructure for constructing autonomic communication services," Proc. of the 2nd International Symposium on Dependable, Autonomic and Secure Computing, IEEE, Indianapolis, IN, pp. 341-348, 2006.
[25] Top threats to cloud computing v1.0. Cloud security alliance, 2010.
[26] D.M. Rousseau, S.B. Sitkin, R.S. Burt, and C. Camerer, "Not so different after all: a cross-discipline view of trust," Academy of Management Review, vol. 23, no. 3, pp. 393-404, 1998.
[27] L. Mearian, No, your data isn't secure in the cloud, 2013. Available: http://www.computerworld.com/article/2483552/cloud-security/no-- your-data-isn-t-secure-in-the-cloud.html
[28] Guidelines governing the protection of privacy and transborder flow of personal data. Organization for Economic Co-operation and Development (OECD), Geneva.
[29] R. Bhadauria, R. Chaki, N. Chaki, and S. Sanyal, "A survey on security issues in cloud computing," Cornell University Library, Ithaca, NY, USA, 2013.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY