Nawaz et al. LGURJCSIT 2023

LGU Research Journal of Computer Science & IT

ISSN: 2521-0122 (Online)
ISSN: 2519-7991 (Print)

doi: 10.54692/lgurjcsit.2023.0702459

Vol. 7 Issue 2, April – June 2023

Cloud Computing Services and Security Challenges: A Review

Sabreena Nawaz, Ahmed Naeem Akhtar, Hafiz Burhan Ul Haq
Departement of Information technology, Lahore Garrison University, Lahore, Pakistan

Email: sabreena.nawaz@lgu.edu.pk

ABSTRACT:

An architecture of computing that provides services over the Internet on the demand and desires of users that pay for the accessible resources that are shared is referred to as cloud computing. These resources are shared over the cloud, and users do not have to acquire them physically. Some shared resources are software, hardware, networks, services, applications and servers. Almost every industry, from hospitals to education, is moving towards the cloud to store data because of managing the effective cost and time of organizing the resources physically in their space. Storage of data over the data centers provided in the form of clouds is the key service of cloud computing. Users store their desired data on publicly available clouds over the Internet and away from their boundaries cost-effectively. Therefore, encryption is used to obscure the user's information before uploading or storing it to the shared cloud devices. The main aim of the techniques is to provide security to user's data from unauthorized and malicious intrusions.

KEYWORDS: Cloud Computing, Cloud Services, Security, Challenges

1. INTRODUCTION

With the evolution of new technologies, cloud computing has seen fast advancement from a couple of recent decades. This technology provides an inclusive solution to meet the desires and needs of individual users. Cloud computing can be described as the advanced level of network and modern paradigm in computing. Cloud computing will provide a foundation for business and a considerable measure of other administration work by providing an independent physical area. It provides the services to users to store their data remotely and power raw hardware infrastructure to develop any tool like web applications [8].

Additionally, cloud computing is the most evolving and rising technology nowadays. To understand what cloud computing is, this can be the best example: If a person needs milk, there is no need to buy a cow; he can get it from the dairy shop as much as required, only pay for the required milk. Cloud computing serves the same purpose. Users can store their important data on servers remotely accessible online [1]. There are ample data centers to provide facilities over the Internet to leverage the storage of data not on the hard drive of users but over the Internet.

Cloud computing is the next stage in the evolution of the Internet which can provide almost everything including network infrastructure, business applications and many other services. Although cloud computing provides commercial use and technological benefits to the users for storing essential data, some security challenges must be explored and addressed. One of the main issues for the users is a threat to the security and malicious access of their data stored over the Internet on a public cloud.

The paper is organized as under; section II explores various services offered in a cloud computing environment, section III describes deployment models for cloud computing, and sections IV & V mention Security attributes

and security challenges for cloud computing. Section VI concludes the paper.

2. SERVICES OFFERED BY CLOUD COMPUTING

Different services provided by cloud computing (CC):

2.1. Managed CC IaaS (Infrastructure as a Service)

This infrastructure is an instant computing infrastructure, stored and managed through the Internet. It means you pay for what you use. It helps to avoid or reduce the expenses of managing our servers. You only have to pay for what you are using, just like renting the resources as long as you use them. Cloud computing service provider manages this whole infrastructure.

2.2. Managed CC SaaS (Software as a Service)

Like IaaS, this infrastructure also is an instant computing infrastructure, stored and managed through the Internet. However, some more services are provided in this infrastructure, such as development tools, database management systems, BI services (Business Intelligence Services), middleware, etc. PaaS is designed to support the web application lifecycle: Managing, deploying, testing, building and updating.

2.3. Managed CC PaaS (Platform as a Service)

This service allows the user to utilize apps based on the cloud over the Internet, such as office tools and email. This service is a complete software solution. We can utilize software through cloud service providers on a pay-as-go basis. This service is the complete solution; it provides services that are provided by IaaS and PaaS also, such as hardware middleware. You can rent an app for the company, and users can utilize it through the internet browser. It allows the organization to use apps with minimal upfront costs. Table 1. discusses the cloud service metric, while Table 2 shows the security threats that affect the IaaS, PaaS, and SaaS.

Table 1: Cloud Service Metric

Services	**Properties**	**Applications**	**Benefits**
CC IaaS	Centralized IT management infrastructure, Scalable infrastructure on user demand, No single point of data failure	Microsoft Azure, Rackspace, Google compute engine,	Lower infrastructure cost, Faster growth to the market, Scalability, Flexibility,
CC PaaS	The integrated environment with tools for development and hosting any application, Provide security, server software and backups, Facilitate collaborative work with remotely dispersed teams	Google App Engine, Apache Stratos, AWS Elastic Beanstalk, Windows Azure services, Heroku, "Master data management (MDM)",	Minimal Development, Scalability Opportunity, Future Proofing, Rapid Time to the market, cost-effective, Developed or multiple platforms,
CC SaaS	Provides subscription model of applications and software, Remotely accessible applications	Microsoft Office 365, Google Apps, Amazon web services, Zendesk, Dropbox, Slack	Scalability, Lower Cost, Integration, Easy to Use, Reduced Time, Integration

Table 2: Security threats related to IaaS, PaaS and SaaS

Attack Name	Explanation	Targeted Layer
Zombie	It affects the availability of the service by corrupting genuine virtual machines (VMs) via direct or indirect flooding of host machines.	IaaS, PaaS and SaaS
Man in the Middle [11]	Obtaining data, transferring data, or communicating with users compromise the sincerity and secrecy of the communication.	IaaS, PaaS and SaaS
Phishing	It is coercing users to visit phoney or illegal websites by using link manipulation. This may compromise the confidentiality of critical user data.	IaaS, PaaS and SaaS
Authentication Attack	They are using loopholes in the authentication protocol as a vector for attack.	IaaS, PaaS and SaaS
Side Channel Attack	Compromises the integrity of the data. Through side-channel information, hackers can decrypt encrypted data and extract either the plain or ciphertext. These may be carried out in one of two ways: either via extracting target VNs or by manually inserting affected text on users' VMs.	PaaS and SaaS

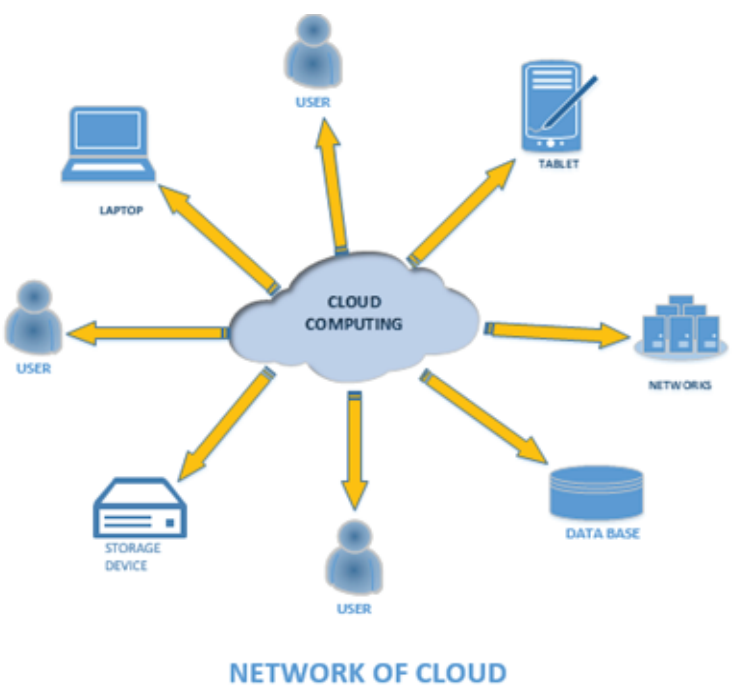

Figure 1: Cloud Network

3. DEPLOYMENT MODELS OF CLOUD COMPUTING

Many cloud services are available to users in their demand. Cloud deployment models describe the control of the infrastructure. Every deployment model of the cloud fulfils the user's or organization's needs at different levels according to their requirement. Each model has a different implementation cost and value proposition. Users need to be well aware of the properties and characteristics of each deployment model before choosing it.

Following are the deployment models of cloud computing.

3.1. Community Cloud

This cloud is used by small, known consumers who all share the same requirements: cost, performance and security. Usually these purchasers are drained from similar business verticals (e.g., services of finance). Even though this need not to be the situation. Amazon's GovCloud and NYSE Capital Markets Community platform are the examples.

3.2. Hybrid Cloud

Hybrid cloud service combines private and public clouds to allow that application and data to be interchangeable between them. This cloud gives more flexibility and deployment options as applications data move between public and private clouds.

3.3. Private Cloud

A single organization owns this cloud, and its resources are only used by that organization. The physical location of the private cloud can be the company site data center. Third-party service providers manage some of the organization's private cloud and get paid for it. A private network maintains the information that is present on the private cloud.

3.4. Public Cloud

Cloud service provider third-party owns and manages this public cloud. Over the Internet, these computer resources are delivered, such as storage and server. The best example of a public cloud is Microsoft Azure. The cloud service provider owns and manages hardware and software. We can access these resources through a web browser by owning an account.

4. GIANT SERVICE PROVIDERS

Cloud computing has evolved into the go-to paradigm for information technology in 2021 [9], as businesses prioritize as-a-service providers above conventional suppliers, expedite digital transformation initiatives, and support the new standard of work in the aftermath of the COVID-19 pandemic.

Nevertheless, IT expenditures progressively shift to cloud behemoths as organizations implement more multi-cloud setups. Following a recent Flexera study on IT expenditures for 2021, funds are being channelled toward Microsoft Azure, its software-as-a-service offerings, and Amazon Web Services. Google Cloud Platform is also gaining traction for big data and analytics workloads. However, major data center and hybrid cloud providers such as IBM, Dell Technologies, Hewlett-Packard Enterprise, and VMware also contribute.

4.1. Amazon Web Services

With its approach of supplying customized databases tailored to workloads, AWS can capture database share. The development of AI and machine learning services and if AWS becomes the preferred model training platform. Use cases for 5G, cloud, and edge computing are being developed. More AWS clients can be moved to its processors. The popularity of AWS serverless instances. AWS's approach to multi-cloud installations. Vertical market competition with Azure and Google Cloud. Although all three strive for health care, merchants choose Azure and Google Cloud.

4.2. Microsoft Azure

Azure is the Microsoft cloud provider that most closely mimics AWS but is hidden in the private cloud. The Microsoft commercial cloud is a mash-up of several services. Businesses will undoubtedly purchase a special buffet that includes Azure but not only focuses on it. Despite this, Microsoft's cloud's commercial run rate is approaching $10 billion annually. Microsoft Azure takes advantage of its architecture for software as a service. The irony is that because the bulk of Microsoft's revenue comes from cloud services that are software-based over infrastructure, like Office 365 and Dynamics, we could easily switch Microsoft from IaaS to SaaS. However, Azure is a strong participant because to its AI, machine learning, and business background. Microsoft is pursuing edge computing.

4.3. Google Cloud Platform

The database, data analytics, and Looker divisions are integrated by Google Cloud, which hires Kazmaier, a former SAP employee. In contrast to Microsoft Azure, which is still under preview, Google Cloud Anthos for AWS is already widely available [9]. Google helps users cut their Google Cloud costs. Google Meet now provides unlimited meetings and live captioning in four additional languages. Google keeps growing. Microsoft Office-related functionalities are now

available in the workspace. To provide backup and disaster recovery services via Google Cloud, Google purchased Actifio. The Database Migration Service from Google is now publicly accessible. Google Cloud recruits several leaders as it broadens its sector and vertical knowledge. With its no-code approach, Google Cloud's Corporate Application Platform aims to draw corporate and citizen developers. Improvements for identity, Kubernetes clusters, and app modernization tools have been made with Anthos by Google Cloud. Google has introduced Cloud Premium Support for customers in the corporate world. Google Cloud has integrated Kaggle and BigQuery. Security Health Analytics is now available via Google Cloud in beta. VMware workloads will start being managed by Google Cloud. The BigQuery Reservations feature on the Google Cloud Platform is aimed towards businesses.

5. SECURITY ATTRIBUTES OF CLOUD COMPUTING

The attributes of cloud computing are described below.

5.1. Data confidentiality

It refers to the security and protection of essential data from illegal and unauthorized users. Data confidentiality is a major aspect while talking about cloud computing. Many security models and protection techniques have been there for the protection of data, with some pros and cons. Rongzhi [1] gives the general sketch of a data encryption algorithm where each time user wants to download a file from the cloud server, he will enter the memory password and a boost password. After that, a hash function will encrypt the password and decrypt the file. Another security model for the protection of data mostly used is the cryptograph algorithm. Furthermore, aldossary and William Allen [2] went deep to investigate the problems and solutions. They found the main issue was the multi-tenancy and hostile insider within a computing environment.

5.2. Data integrity

It mentions the guarantee that data is not modified intentionally or unintentionally by anyone, stored on the cloud storage device while travelling between two entities. For the sake of correct results, data integrity is a crucial aspect. Data stored on the cloud storage must not be transit or altered purposely or maliciously. Kiruthika and Sree, in [3], presented a data integrity confirmation scheme by involving a mediator party as a reliable and dependable verifier. The suggested scheme allows the users to authenticate the integrity and correctness of their data without downloading or moving it to their personal computers. But this technique also has some shortcomings and limitations like the scheme could not stop the user from altering data at cloud storage.

5.3. Data availability

It denotes the trusted and authorized accessibility of data on time over the Internet from the cloud storage. As contrasted with the integrity and privacy of data, the data accessibility attribute of cloud computing has not pulled much attraction and consideration from the researchers yet. Qadir et al. [4] suggested that data availability depends on network, software and hardware, but achieving continuous and smooth data availability over the cloud is hard and challenging.

Another researcher, Mehta, stated that "Distributed Denial of Service (DDoS)" attacks are challenging to measure and avoid, but following a firm mechanism of defense that must properly employed will reduce the effects of DDoS attacks. The mitigative fortifications that can positively decrease the impacts contain "service of filtering routers, load balancing, disabling IP broadcasts", applying security fixes as and when accessible, disabling the services that are idle and mostly unnecessary and execution the active discoveries for any intrusion.

6. SECURITY CHALLENGES

Some major security challenges of cloud computing:

- ***Data breaches and downtime***

While enterprise-grade services provided by the cloud are typically more reliable and secure than old-style infrastructure, there are potential expenses in data fissures and downtime. Resolving these issues for public and private clouds involves the deals of providers i.e. outsiders as third parties. Therefore, The company has a slight say about the approximated time period for the vital business method to last.

- ***Denial of service attacks***

DoS attacks aim to overload a system and prevent users from accessing its services. These attacks are destructive to cloud computing platforms

because they may cause widespread user pain by overwhelming a single cloud server. When there is a high workload, cloud systems provide additional virtual machines and service instances, increasing processing capacity. The cloud infrastructure makes a cyber attack more deadly while striving to prevent one. And last, legitimate users cannot access their cloud services since the cloud infrastructure is slow. If hackers use more zombie machines to target many systems, DDoS attacks might be far more dangerous in the cloud. To decrease them, it's essential to be conscious of them.

Injections of malware into the cloud Attacks using malware injection seize control of a user's cloud data. This is done by hackers inserting a virtual machine instance into an IaaS solution or a SaaS or PaaS system, or a service implementation module. If the cloud system is successfully tricked, requests from cloud users will be sent to the hacker's component or instantiation, which will lead to the execution of malicious code. After that, the intrusive party might start damaging activities like data modification, theft, or espionage.

The two most common malware injection attacks are cross-site scripting and SQL injection. Hackers may introduce harmful software (such as Flash, JavaScript, etc.) into a vulnerable web page as part of cross-site scripting assaults. German researchers planned an XSS attack against the cloud computing infrastructure of Amazon Web Services in 2011. SQL injection happens when hackers use unsecure database applications to target SQL servers. A SQL injection attack was launched against the Sony PlayStation website in 2008.

- ***Cloud service abuse***

Hackers may run DoS and brute-force attacks against particular people, companies, and even other cloud providers using inexpensive cloud services. For instance, utilizing the EC2 cloud architecture from Amazon, security experts Bryan and Anderson executed a DoS attack in 2010. They could make their consumer unavailable online for $6 due to hiring virtual services. At the 2011 Black Hat Technical Security Conference, Thomas Roth engaged in a brute force attack. By renting servers from cloud providers, hackers may exploit the enormous cloud capacity to send thousands of possible passwords to a target user's account.

- ***Wrapping attacks***

A wrapping assault in cloud computing would be a man-in-the-middle attack. Even though web browsers are often used by cloud users to access services, wrapping attacks may still occur. An XML signature does not secure the document's attributes, but it safeguards user's credentials fromunaccredited access. Attackers may change an XML document due to XML signature element wrapping. For instance, Amazon Elastic Cloud Computing's (EC2) SOAP interface was shown to have a vulnerability in 2009. Attackers could alter an intercepted notification due to a successful signature-wrapping assault.

- ***Man-in-the-middle attacks***

In this attack, hackers use holes in the synchronization token system to intercept and modify cloud services. As a result, the synchronization token is replaced with a new one that gives the attackers control over during the following synchronization with the cloud. Consumers may be unaware that their credentials have been hacked since an attacker can always recreate the original synchronization tokens. Additionally, it's possible that compromised accounts won't ever be recovered.

- ***Insider threats***

This type of attack is launched by a legitimate user intending to violate the security protocols deliberately. An assailant in a cloud environment might be someone providing administration to cloud or a client corporate representative with significant rights. Cloud providers should create secure structures with distinct degrees of contact to cloud services to avoid this type of criminal conduct.

- ***Hijacking a service or account***

Account or service hijacking happens when access is gained to a user's personal information. There are several ways to do this, including fishing, spyware, and cookie infection. Once a cloud account has been hijacked, hackers may access the user's personal or professional data and jeopardize cloud computing services. For instance, a 2007 phishing attempt victimized a Salesforce employee, revealing all of the company's client accounts.

- ***Avanced persistent threats (APTs)***

APT attacks enable hackers to steal private information kept in the cloud or abuse various

cloud services indefinitely without being detected by normal users. The short duration of these vulnerable attacks permits hackers to revamp to security measures and solutions. Once illegal access is granted, hackers can roam around the data centre networks and exploit network traffic for harmful purposes .

- ***Meltdown and Specter attacks***

These two aspects of cyber attacks first arose this year and have quickly become a new menace to cloud computing. Potential enemies can access encrypted data from memory using malicious JavaScript code by leveraging a design flaw in supreme current CPUs. Both Spectre and Meltdown compromise the separation of programs and operating system modules, allowing invaders to retrieve data from the kernel. This is a major issue for cloud providers since not all cloud users apply the most recent security fixes.

- ***Accessibility to Servers & Applications***

In the case of traditional data centers, there are restricted and reliable connections that are fully controlled by administrative access to the data servers but not in the situation of cloud data servers and data centers. In distributed computing, the admittance to the data is conducted and controlled over the Internet, leading to risk exposure. Additionally, it is imperative to prevent data accessibility to unauthorized users by the controlled administrative access by monitoring the change in the system's control.

- ***Lack of visibility and control***

Suppose you are managing the open/public or hybrid cloud conditions. In that case, the absence of data in the cloud can mean a loss of control and power over numerous IT management and data protection aspects. As the client ultimately manages the legacy technology style that is in control, the cloud services offered by outside providers do not provide the same degree of administration and management. The third-party performs a major role in providing control over the services. A lack of awareness of potential safety vulnerabilities can contribute to an organization failing to recognize possible risks.

- ***A Lack of Transparency***

Suppose a company purchases a public or hybrid cloud solution as a third-party provider. In that case, it is conceivable that it won't provide a complete overview of services, describing precisely the guidelines of how the product operates and the vendor's security procedures. The absence of consistency in operation restricts the consumers to smartly determine if their information is still being saved and handled safely.

- ***Vulnerabilities for Shared Technology***

A company may expose to security weaknesses and vulnerabilities while using the hybrid or publicly available clouds for similar cloud services users. The cloud provider has to ensure this doesn't happen, but no provider is fine. Likewise, every service user may experience security weaknesses and vulnerabilities that other users in a similar cloud may cause. Table 3 provides an overview of security attacks that existed in cloud computing.

Table 3: Classification of attacks

Classification of attacks	Explanation	Attacks
Denial of Service	The attacker generates a lot of data traffic to prevent services from being available.	SMURF is an ICMP command that generates an echo request and sends it to an intended IP address. LAND: the process of transmitting fake SYN packets with the same IP address as their source and destination. SYN Flood is a technique that reduces storage efficiency by sending faked IP packets. Teardrop is an exploit that uses flaws in TCP/IP stacks.
Remote to Local	The system's integrity has been compromised due to the attacker's execution of instructions that provide access to the system.	SPY is an acronym for installations that operate a computer for phishing. Attempt to Guess the Password IMAP: locating a mail server that uses IMAP that is vulnerable.

Distributed Denial of Service	A distributed denial-of-service attack (DDoS) involves flooding the system dispersedly.	Exploiting legal HTTP POST or GET requests is one example of HTTP flooding. Zero Day Attacks are when security flaws that are unknown to CSPs are exploited.
Probing	They compromised the victim's identity by gaining access to sensitive information.	Ports are being swept. Scanning for open ports using NMAP
User to Root	The attacker compromises the system when they execute instructions that provide them access to the system.	Rootkits are software programs providing privileged access while concealing the fact that they exist. Buffer Overflowing

7. THE PROTECTION OF INDIVIDUAL PRIVACY BY CONTROLLED ACCESS AND DESIGN

Modelling privacy concerns accurately is a key goal of the Privacy Process Patterns. They may be thought of as patterns applied to privacy-related processes, and they detail how such concerns might be realized through observable procedures, linking flows, and activities. They are supplemental tools that teach programmers to implement certain privacy features more accurately. When it comes to protecting users' privacy while still allowing cloud services to function, Privacy Process Patterns (PPP) are seen as the most effective solution. Some of the privacy patterns are:

7.1. Anonymity

is the ability to remain untraceable in any way, either directly or indirectly. The problems of Accountability and a huge anonymity set might occur when a person is anonymous. The advantages include unrestricted location monitoring, user anonymity, and little effort on the user's part. The Tor network, Onion routing and distributed-control networks may all be used to realize this quality.

7.2. Pseudonymity

is using a fake name or other identifying information to avoid detection. An issue that may emerge is the question of integrity. Positive effects let users access services without having to reveal their true identities. However, some users still follow the procedure to ensure its continued existence. Administrative procedures might be used to accomplish this identity management. Smart cards and biometrics are all examples of technologies that may be used for this purpose.

7.3. Unlinkability

is utilizing a service or resource without third-party connectivity between the user and the service. The issue is one of integrity and Accountability. The advantage is that it protects user privacy by not enabling harmful surveillance of user experience.

7.4. Undetectability

is third-party monitoring among a pool of potential consumers. Problems: the effectiveness of being undetectable relies heavily on the extent to which the set is undetectable. Users' privacy is protected, and the service is undetectable to potential attackers. Second, using techniques like steganography and watermarking makes it difficult for attackers to determine whether or not a certain IOI exists. Applications: mail and transaction encryption, smart card-based authorization management

7.5. Unobservability

is the inability to detect the presence of a user among a group of possible users. Problem: it depends on the amount of integrity and anonymity specified. Benefits include complete anonymity and undetectability while using resources and second, guaranteeing a positive user experience apart from the connection with and the opportunity to observe a third party. Smart cards and a permission management system will be used in the implementation. Services that protect users' anonymity, such as Tor, Hordes, and GAP.

8. CONCLUSION

One of the evolutionary technologies, cloud computing, provides users with commercial and economic advancements. With the many of its advancements and benefits, some issues need to be addressed. Security is the major concern and

issue that attracts researchers' attention and prevents users from accepting the emerging cloud computing technology for the share of resources and data. Due to the complexity, achieving the security that provides end-to-end connection and conduct of service is challenging. This paper presented a review of cloud computing attributes concerning security concerns and future security challenges that can arise in data storage in the cloud. In future, these challenges can be explored for the solution of computational security issues for the strength and vulnerability of each service provided by cloud computing.

REFERENCES

[1] Rongzhi Wang, "Research on data security technology based on cloud storage", Procedia Engineering, 174, 1340 – 1355, 2017.

[2] S. Aldossary and W. Allen, "Data security, privacy, availability and integrity in cloud computing: Issues and current solutions," International Journal of Advanced Computer Science and Applications, vol. 7, no. 4, pp. 485–498, 2016.

[3] V. Kiruthika and B. R. L. Sree, "A survey and a data integrity proofs in cloud storage," International Journal of Computer Science and Network Security, vol. 15, no. 11, pp. 39–11, 2015.

[4] S. Qadir and S. M. K. Quadri, "Information availability: An insight into the most important attribute of information security," Journal of Information Security, vol. 7, pp. 185–194, 2016.

[5] V. Krishna Reddy, B. Thirumal Rao, Dr. L.S.S. Reddy, P.Sai Kiran "Research Issues in Cloud Computing "Global Journal of Computer Science and Technology, Volume 11, Issue 11, July. 2011.

[6] R. Mehta, "Distributed denial of service attacks on cloud environment," InternationalJournalofAdvancedResearchinComputerScience, vol.8, no. 5, pp. 2204–2206, 2017.

[7] A. Kundu, C. D. Banerjee, P. Saha, "Introducing New Services in Cloud Computing Environment", International Journal of Digital Content Technology and its Applications, AICIT, Vol. 4, No. 5, pp. 143-152, 2010.

[8] Priyanshu, Rizwan, "A Review Paper on Cloud Computing", International Journals of Advanced Research in Computer Science and Software Engineering, ISSN: 2277-128X (Volume-8, Issue-6), 2018.

[9] Dignan, Larry. "Top Cloud Providers in 2021: AWS, Microsoft Azure, and Google Cloud, Hybrid, SaaS Players." ZDNet, 11 Jan. 2021.

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

[11] W. Akram, K. Mahmood, X. Li, M. Sadiq, Z. Lv and S.A. Chaudhry. An energy-efficient and secure identity based RFID authentication scheme for vehicular cloud computing. Computer Networks, 217, 109335. 2022.