A Review on Chronicle of Cloud Computing Security and Storage Environment Models

Shrinivasa
Senior Assistant Professor, Department of Computer Science & Engineering, SMVITM Bantakal, Udupi, Shrinivasa.cs@sode-edu.in

Dr. Chandrakala B. M
Associate Professor, Department of Information Science & Engineering Dayananda Sagar College of Engineering, Bangalore, Chandrakalabm, ise@dayanandasagar.edu

Abstract

Cloud computing is a rapidly evolving and expanding technology that is now being used in a wide range of applications all over the world. It offers on-demand and pay-per-use computing services through the internet, allowing users to use a pool of resource sharing without having to buy them. The key benefit of this model is that it eliminates the need for the user to worry about the deployment of expensive computing platform, which saves money and time for any organisation. Because of its services' scale and dependability.Despite its many benefits, the transition from a localized computing platform to a virtual computing platform poses a number of security concerns and issues to both user and the service provider. The objective of this research is to offer a quick overview of cloud computing technology, including current and future developments, what services the CC provides, security difficulties and obstacles, and Cloud Computing Attacks.

Keywords: *Cloud Computing, Cloud Computing Architecture, Cloud Security, Cloud Storage, Challenges and Issues in Cloud Computing, Security Measure in Cloud.*

I. Introduction

Cloud computing is the most latest internet-based computer machine that enables users with accessible and adaptable options for gaining access to and the use of various cloud apps. The internet is the driving pressure behind the diverse technologies that've been created. One of those that has lately been resolved is cloud computing. it's miles a defined preferred [1] for connecting a big quantity of shared or personal structures as a way to provide customizable capability, data, figures, and data garage infrastructure.Cloud computing is a realistic manner to obtain unambiguous value savings, and it has the capacity to convert a facts centre from a massive placing to a variable-price surroundings [2]. Cloud computing has emerged as a singular innovation that has advanced during the last several years and is expected to emerge as the following essential situation inside the coming years. because it's far a brand new generation, it necessitates new safety issues and faces a selection of challenges [3].

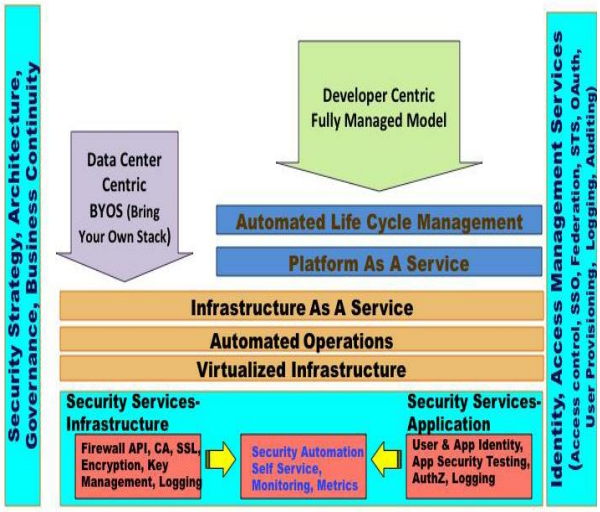
The cloud computing paradigm has advanced dramatically and enormously, and it has established a leap forward phenomenon in information technology because it provides huge price financial savings and new business options to its users and companies. customers that use the cloud offerings as requested, who use shared talents as a provider which could speedy and dynamically develop get right of

entry to services over a networked infrastructure constitute cloud computing. The traditional IT delivery paradigm is being disrupted through cloud infrastructure.price savings, scalability, performance, asset utilisation, more desirable efficiencies, and mobility are a few of the organisation and IT outcomes. the security and performance of cloud computing services have been hailed by using companies, however the normal delivery of cloud computing services wasn't as handy and robust as they declare [4].

By way of connecting the cloud app to the net, cloud computing lets in cloud records to be stored and viewed remotely. with the aid of choosing cloud offerings, users are able to keep the Meta statistics within the cloud facts server. Cloud service companies can access or take care of data remotely stored information centre [5].

To make certain protection, statistics within the cloud calls for itself a safety, together with information segregation within the cloud service.Encryption, virtualization, and authentication can be used to split statistics at numerous tiers. This improves records safety by stopping undesirable access. it's essential in a joint occupancy cloud context with several customers or clients who do not see or share statistics with every different however can pool duties or software in an execution putting, even if they do not belong to the equal company. authorities at the moment are trying accessibility of laptop device features, usually records storage and computational electricity, with out direct customer manipulate algorithm is known as cloud computing [6].

Figure 1. Architecture of Cloud Computing Security [7]



For cloud users, information safety is a prime challenge. to relieve consumer worries, this era desires sizable safeguards and approaches. most people of cloud carrier customers are worried approximately their non-public information being viewed or shared with other cloud carrier providers: (i) consumption facts; computer tool specifics collected (ii) delicate information, knowledge about health, banking statistics, and different private facts (iii) data that may be used to categorise the individual personal statistics (iv) specific computer person identities;IP addresses, precise hardware identifiers, and different traits which are only visible to the human eye [8].

The use of cloud carrier suppliers' offerings, cloud information is processed and retrieved on an internet server. As a result, the usefulness of cloud services is growing, making it a growing market that is attracting a variety of hobby from the educational and enterprise fields. Many problems plagued the cloud garage device, inclusive of inaccessibility and protection troubles. due to the fact the cloud garage service is targeted on two-manner information sharing amongst provider provider and user,

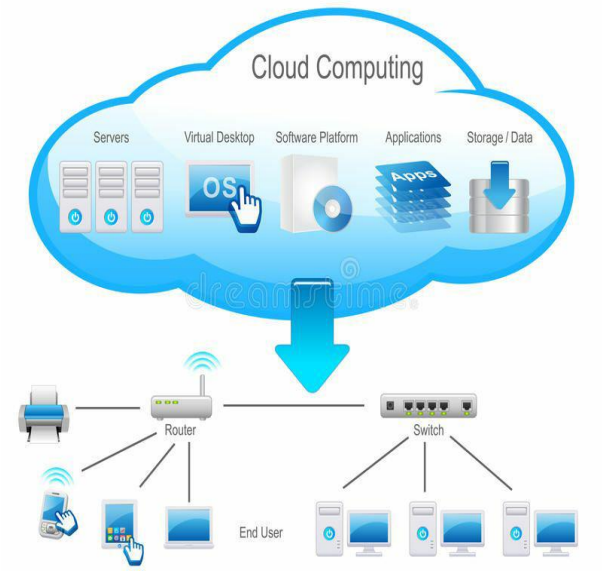
cloud computing safety concerns encompass integrity, verification, confidentiality, honesty, availabilityand permission.As a result, the threat of information compromise is increasing, and it may be divided into two categories: important records and archive cloth. crucial records is statistics that an person requires at any given time and might be irritated by way of any halt or disappearance. furthermore, archival statistics is facts that is extraordinarily uncommon in its entirety, and normally in a non-vital second. As a result, a ruin in it'll not be appeared a first-rate problem [9].

The following is the structure of this paper: Section 1 provides an overview of cloud computing, while Section 2 examines the foundation of cloud computing.Furthermore, in Section 3, the associated work is presented, and in Section 4, the research problems are examined. In addition, Section 5 discusses cloud computing strategies, and Section 6 portrays security difficulties. The answer to data security concerns is discussed in Section 7. Section 8 discusses the benefits and drawbacks. Then, in Section 9, there is a discussion, and finally, in Section 10, there is a conclusion.

II. BACKGROUND OF CLOUD COMPUTING

For networking systems, middleware and web development frameworks, and commercial applications, cloud computing provides a resource-sharing environment. Cloud operating models include free infrastructure services that respect various services, paid infrastructure services, and consumers' lucrative complimentary marketing services. Researchers, scholars, businesspeople, and IT companies all use the phrase cloud computing in different ways. Clouds are a large collection of virtualized technologies that are readily accessible and useable. These services can be dynamically adjusted to comply to a changeable fee (scale), allowing for the most efficient use of resources [10].

Figure 2. Cloud Computing [11]



Beyond a question, cloud computing is the most interesting approach in the IT sector. Competing online service organisations have hinted to a cloud computing approach, with the less expensive cloud infrastructure becoming the focus of the market [12].

This success was preceded by its adaptable computing web service, which launched in 2006 and allows clients to rent equipment and run their own programmes. That year, Google debuted the Google Docs functionality.Google Docs was founded on two various ingredients: Google bought Writely, a service that allows renters to copy, change, and move papers using blogging platforms. Developed in 2005 from two web breakthroughs is a web-based application that enables users to make, update, alter, and share data online. It is utilised Ajax-based applications that are compatible with Microsoft Excel. The spreadsheets should be saved in HTML format [13]. When USinter-networking was required, AT&T entered the

cloud-computing industry in 2006. USI was a software platform with over 30 states' worth of applications.In 2008, AT&T unveiled synapse, a cloud-based service that integrated the five USi internet data centres in the United States, Europe, and Asia to act as a worldwide portal. In order to aid with speedier cloud, IBM created the IBM cognitive cloud platform in 2011. The ICloud was later released by Apple, with the goal of storing additional personally identifiable information. This year, Microsoft began pushing the cloud on media, informing the general public about the cloud's ability to store photographs and videos with easy access. In 2012, Oracle released the Oracle cloud, which has three key business components (IaaS, PaaS and SaaS).Contemporary cloud technology is now since cloud computing has grown as a viable and easily obtainable tool. This climate requires an inherent level of consciousness to ensure efficiency [14].

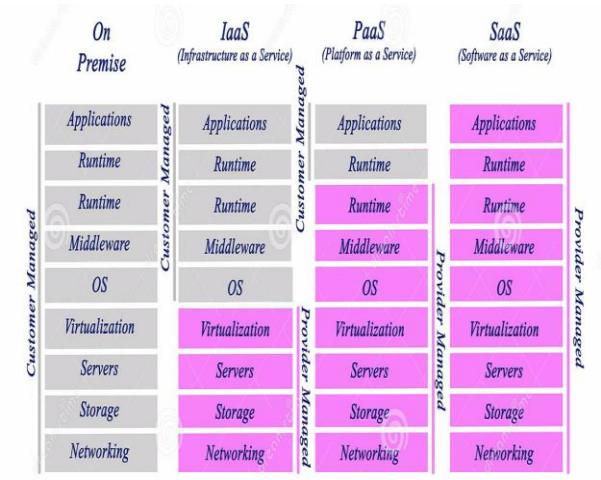
III. RELATED WORK

Cloud data security is a major worry, and several approaches have been offered, as well as improving data security risk evaluation in cloud computing, as well as growing worries about data storage issues related to privacy, such as the example of intercepted email accounts data security. The studies listed below are those in which various researchers explored [15].

[16] discussed the concerns about safety, standards, and challenges that cloud service providers must meet in cloud engineering. It covered defence strategies designed to mitigate well-known dangers.The focus is on exceptional case approaches that are best suited for current security systems rather than intrusion sensors. Developments in the pattern can be seen. According to [17], cloud technology is able to reduce service costs while improving corporate performance. However, there's many security concerns that must be addressed in order to encourage include a subject for cyberattacks and unlawful activities because these networks store data from a variety of corporations and people in their databases.The researcher applied a cloud-computing survey to detect vulnerabilities and security difficulties, as well as to outline five types of attacks that are on the rise. 1: Refusal to provide service 2: Encounters by a malevolent intruder 3: A network attack on the workstation Phishing assaults are number four. Target attacks on shared memory are number five. They proposed a methodology to categorise such risks automatically, and they tested its effectiveness by visualising vulnerabilities in specific cloud scenarios[18].

A paper published in [19] combines data from eleven publications on susceptible security risks. The researchers calculated their findings, which included the topic they looked into and the methods they employed to tackle the problem in their document.It discusses a number of key security concerns about cloud computing, as well as techniques for mitigating the risk. According to the study, cloud computing will become more popular, potentially resulting in large groups of attackers. He frequently believes that future collaboration and data lock-in issues can be avoided by employing application.

Figure 3. Types of Cloud Computing [20]



[21] mentioned CC characteristics such as low maintenance costs, market divergence and scalability. They feel that cloud computing minimises complexity and allows consumers to create services more quickly and easily. Virtualization is a way for interacting with quality of service. This also tackles the advantages of using a specific indicated that in CC, some regulations are required. It built certain cloud frameworks and investigated cloud computing security problems and its approach in accordance with cloud computing principles. Depending on a cloud architecture research, also developed technologies to improve the cloud-computing work.

3.1 Advantages of Cloud Computing:

The few benefits are listed below,

• Endurance

• Information Technology Diversity

• Expand Memory

• Superb Mobility

• Lower Cost

Cloud computing's advantages pique the curiosity of the information and technology industry. According to ITC surveys from 2008-2009, numerous companies and individuals are discovering that cloud computing provides benefits over traditional computing approaches. [22]

IV. PROBLEM STATEMENTS

Cloud computing delivers services to organisations so that they can use them, and the information is stored in vendors' physical locations outside of the organization 's authority. As a result, security is playing an increasingly important role, or this functionality of cloud computing has raised a variety of issues in security, such as integrity, privacy and data confidentiality, where every organization required or demanded a secure cloud computing environment wherein the system or providers establish confidentiality.To create that level of confidence in cloud services, a platform that can handle authentication, verification and encrypted data transmission is necessary, as well as one that can ensure data secrecy [23].

In relation to the cryptographic principles of CC security Confidentiality, Integrity, and Availability [24], there are three essential challenges to be faced.

A. Availability

Given the critical impact on cloud-based corporate operations, prompt accessibility of sensitive information. Consider a scenario in which a cloud service provider (CSP) or a cloud server fails to deliver data to an end user or a business organisation on time. In this case, the end user or business organisation is completely cut off from cloud services and is unable to continue or function correctly.

B. Integrity

Data integrity ensures that data in transmission is not tampered with and may only be read or

modified by those who are authorised to do so. To further defend, it must not be deformed in route and safeguards must be in place to ensured information cloud not be altered by an entity.

C. Confidentiality

Confidentiality refers to avoiding unauthorized data access and, as a result, ensuring that only the users with authority have access to the data.

V. TECHNIQUES IN CLOUD COMPUTING

5.1 Data Encryption

You'll need to use data encryption approaches if you wish to store important data on a large data store. Although passwords and firewalls are suitable, individuals may be able to get around them to access your data. Data gets fragmented when it is placed in a pattern that cannot be read without the use of an encryption key. The insight is completely ineffective to the gate crasher. The method of transforming facts into a secret code is known as encoding. You'll need the enigmatic secret or hidden phrase, that is also known as the encryption key [25], to decode the jumbled data.

5.2 Authentication and Identity

Customers and even transmitting devices are verified using a variety of methods, although cryptography is the most well-known. Server authentication can be accomplished in a number of methods, including utilising unique passwords, having a security token, or using a measurable number like a distinctive mark in the architecture. There is an issue with employing standard personality approaches in a cloud context when the project involves several cloud specialist co-ops (CSPs). In this use situation, personal data synchronisation with the enterprise is not adaptive. Traditional character procedures have a number of challenges when moving basis to a cloud-based arrangement [26].

5.3 Availability of Information (SLA)

Data or information that is not attainable is a big issue in distributed computing enterprises. The Administration Level Comprehension is used to tell clients about whether the institution's resources are available to them. It's a trusting relationship among the customer and the supplier. One method to assure asset availability is to have a contingency strategy in place for nearby properties, just as you would for your most important data. Although the resources are unavailable, the client has exposure to asset data [27].

5.4 Information uprightness and Privacy

Distributed computing is used to transfer information and resources to lawful clients. Assets can be accessed by Browsers, as well as by malicious aggressors. The challenge of data integrity can be solved by fostering data stream is exposed to many layers of verification to maintain adequate consumes. Certain accessing instruments should be provided, likewise RSA certifications aswell as SSH passageways [28].

5.5 Malware-infusion assault arrangement

This configuration produces a lot of customer virtual machines and saves them all in a single location. It takes advantage of the FAT virtual working environment (File Allocation Table). The software that is handled by a consumer is stored in the FAT table. Every one of the events will be overseen and planned by Hypervisor. The IDT (Interrupt Descriptor Table) is utilised for integrity checking [29].

5.6 Flooding Attack Solution

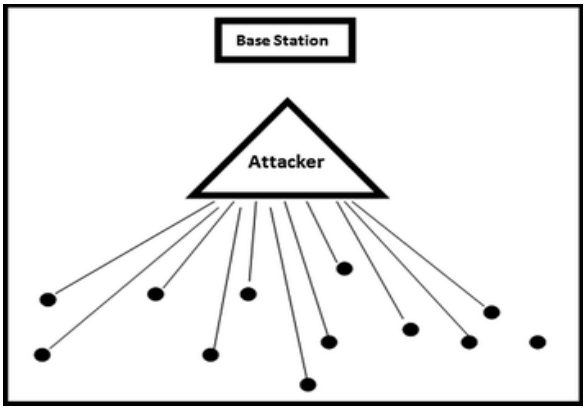
An armada is a term used to describe a group of cloud workers. One group of workers is

regarded for framework style requirements, one for memory the panel, and the last one for centre calculation associated responsibilities. The armada's workforce is able to speak with one another. When one of the employees gets overworked, a new worker, known as the name employee, is called in to take his or her place. This new worker has all the current worker positions and can be used to alter concerns and states. Work can be supervised using Hypervisor.Job approval and confirmation are likewise handled by Hypervisor. An authorised customer's PID can be used to identify a request. RSA can also be used to scramble the PID [30].

5.7 Secure Information Management

It is a data security process for storing a wide range of data in a single location. It consists of experts who work on systems that must be inspected and then send data to a worker known as the "Security Console." An admin is in charge of the security system, who evaluates the data and answers to every alarms. Cloud security is becoming increasingly challenging across the board as the cloud client base, dependence stack, and cloud defence solutions to resolve security threats evolve. The term "log management" is occasionally used to describe it. Cloud companies also provide security standards such as PCI DSS and SAS.Data Security Management Maturity [31] is another paradigm of Information Security Management System. This is depicted in Figure 4.

Figure 4. Flooding Attack arrangement [32]



VI. SECURITY ISSUES

The cloud computing framework's tremendous scalability eliminates the need for cloud providers to plan ahead for system supply, allowing them to provide limitless computing services on demand. Many companies, expanding consumer service. We explore the security issue with a variety of corporations' existing cloud computing platforms in this study [33]. The implementation of cloud computing systems due to the existing investigative protection challenge encountered by enterprises. This normally implies that the operating system is delivered to the cloud user. The OS is ultimately responsible for the cloud service provider [34].

6.1 Infrastructure as a Services (IaaS)

This technique offers you get entry to to essential assets which includes virtual computer systems, actual machines, and digital garage. Infrastructure as a service (IaaS) is a standardised provider that supplies virtual computers and different primary storage and computing abilities thru the net or network. although the patron does now not administer or oversee the essential cloud infrastructure, he or she does have manage over working structures, storing, and installed applications, in addition to perhaps limited control over a few

networking components (e.g., host firewalls). The customer or user completely outsources the resources and storage, such as hardware and software, that they require on this approach. they may be all controlled using an API carrier.It covers offerings together with Terremark organisation Cloud, Amazon EC2, home windows stay SkyDrive, and others [35].

Advantage of IaaS Solutions

- The services are pay-per-use, so users may choose which ones they want to utilise.
- Cost savings due to the lower infrastructure costs associated with the IaaS approach.
- Flexible and efficient resources that can be swiftly scaled up and down based on user needs at any moment.
- High availability and accessibility to a group of resources or infrastructure.
- Beneficial for business expansion.

6.2 Platform as a Services (PaaS)

It allows users to create new programs making use of APIs which might be completely established and programmable, in addition to the creation, layout, and hosting of recent apps. customers can proportion get right of entry to to the platform, which allows them to install their very own cloud-based totally applications and services. development equipment, configuration control, and deployment systems are a few of the systems to be had. Microsoft Azure, pressure, and Google App Engine are amongst examples [6]. The Platform as a provider issuer presents the person or subscriber factor degree get entry to on this approach, permitting them to assemble and execute cloud programs as wanted over the net or community.both the cloud user and the cloud issuer should be aware of the security dangers posed with the aid of statistics sharing and multi-tenancy [36].

Advantage of PaaS Solutions

- Corporations may easily focus on their development without having to worry about the underlying infrastructure.
- The infrastructure software does not require any updates or upgrades. The PaaS provider is responsible for all updates, upgrades, and routine maintenance.
- Lower prices: PaaS decreases organisational costs by eliminating the need for enterprises to invest in hardware and software. The platform as a service (PaaS) provides tools for developing, testing, and hosting applications.

6.3 Software as a Service (SaaS)

SaaS refers to software program that is made reachable by using a provider on a pay-in keeping with-use foundation over the internet or a pc network and may be configured remotely. It allows us to provide software program programmes to stop consumers as a service. for example, Google programmes (e mail, video games, Google doctors) are available on a variety of gadgets, such as computer systems, laptops, and smartphones. any other instance of SaaS is Microsoft's workplace 365, which affords on line framework that consists of word, PowerPoint, and Excel, all of which might be available via web and cellular programs.in this model, the company gives the authority to the person or subscriber for gaining access to each assets and programs. it affords the ability to the consumer to put in all the essential software on cloud as a way to access the software program through all styles of their non-public devices through the

net connection or community. The SaaS presents a popular included improvement environment (IDE) to its client to get entry to the programs and switch the data and programs to a far off garage server through software program services.It reduces the time and power required to install and preserve sophisticated software program with the aid of allowing customers to down load it directly from the internet. It additionally frees the user from time-consuming programming and equipment administration [37].

Advantage of SaaS Solutions

- Programs can be accessed from anywhere using a variety of internet-connected devices.
- Rapid resource scaling in response to customer inquiries.
- Eliminate infrastructure issues: SaaS users do not need to be concerned about the provider's infrastructure.
- Data is protected, and it comes with a repair and training package.

Table 1. Comparison of Private, Public and Hybrid cloud [38]

Attribute	Private Cloud	Public Cloud	Hybrid Cloud
Space Required	Very large	Very low	Medium
Workload	Mission-critical workload with security concerns	Normal workload	Highly dynamic or changeable
Security	High	Low	Moderate
Data & Application Integration	Easy	Easy	Changing cloud systems is a difficult task.
Reliability	High	Medium	Medium to high
Scalability	Limited	Very high	Very high

VII. SOLUTION TO DATA SECURITY AND STORAGE CHALLENGES

Encryption is advocated as a safer technique to protect documents. Until you need to encrypt information should issue authorization to certain members of the community in order for them to have easy access to information. Multicultural data authentication should be utilised to incorporate data accessibility control. To protect privacy and data confidentiality, data encryption will be used as a solution.Add encryption to information to determine it completely unusable and to prevent other users from accessing it. Standard encryption can make availability more difficult. If the files stay unaltered, users should review before transferring to the cloud. Calculating the file's hash ensures that the data isn't modified until it's transferred to cloud servers. It is conceivable to utilise this hash computation for record integrity, however it is extremely challenging to maintain.By combining identity-based and RSA Signature cryptography, it is possible to test the integrity of RSA-based data. By means to separate data from diverse users, physical level, and device level, SaaS ensures that all limits must be evident at the stage of the. It's possible that [39] will be used to design a distributed access control framework.

It will be used for accessibility controls in cloud computing. Regulations that are centred on the use of passwords or attribution to recognise

unauthorised users are better. Authorization approach enables the owner to delegate the majority of computer-intensive operations to the cloud without disclosing data or servers. A data-driven architecture can be created for stable data collecting and exchange among cloud users. A network-based intrusion protection system is utilised to track attack patterns [40, 41].

VIII. MERITS AND DEMERITS OF CLOUD COMPUTING SECURITY AND STORAGE

Cloud computing is the most current net computing community that gives users with reachable and customizable alternatives for having access to and the usage of numerous cloud apps. by way of connecting the cloud app to the internet, cloud computing permits cloud statistics to be saved and retrieved remotely [4]. with the aid of choosing cloud services, users may be able to shop their Meta facts inside the cloud records center [5]. Cloud provider providers can retrieve or communicate information saved in the cloud data centre. As a result, statistics collection for records processing in a cloud facts centre ought to be done with the utmost information.Cloud computing offers lots of flexibility, performance, usefulness, and value savings, all of which can be exceptionally attractive. it's miles the maximum recent new era that provides consumers with numerous benefits even as additionally posing severa risks. As a result, the significance of cloud computing is growing, and it is attracting loads of awareness from the instructional and training sectors [42].

However, when it comes to cloud computing, we've got numerous problems to deal with. in this segment, we've got diagnosed some of troubles relating to facts security in addition, facts isolation and privacy have a 92 percentage effect on safety troubles. statistics protection, dependability, integrity, accessibility, identity, and secrecy, as well as a lack of assets and abilities, are most of the maximum severe protection demanding situations in cloud computing. There are six levels to the statistics lie cycle. Create an inventories, use, transmit, archive and kill it [43].

IX. DISCUSSION

Technology is a promising concept that is gaining traction nowadays, as well as an ongoing search zone with promising results. Users of this technology can manage their resources at any time and from anywhere. Cloud is regarded as a conscientious and important firm that has entered the IT market. As a result, the software industry must move to CC, which necessitates the assessment of numerous crucial issues such as security. CC must also be incorporated by creatives in order to save expenses and increase performance. We've discussed the present issues here. Solutions must be appropriately re-evaluated in terms of their cloud applicability.Our problems are succinctly summarised in the table, along with their restrictions and potential models. We can use encryption to secure our data from unscrupulous people. This also applies to different types of encryption. We can keep our personal information safe by encrypting it. Furthermore, in our article, we analyse many examples of cloud security and offer solutions to them. Information, software, and other sorts of safety must all be considered. Furthermore, we construct a cloud computing architecture that includes several services such as IaaS, PaaS, and IaaS, each with its own set of features and duties, and we illustrate these with appropriate examples.This research demonstrates that CC provides the ability to employ assets from a resource pool, which aids in the reduction of E-Waste. In our paper, we

discuss some of the advantages of cloud computing and how they may be highly beneficial. Several issues in CC, including as guarantee, privacy, accomplishment, acquisition, and other non-technical issues, must be investigated in the future research. As a result, researchers are confronted with several issues and are required to identify solutions to both scientific and non-technical issues.

X. CONCLUSION

Cloud computing offers a whole lot of flexibility, productiveness, usefulness, and price savings, all of which might be surprisingly appealing. it is the most recent new era that provides purchasers with numerous benefits at the same time as additionally posing numerous risks. to address the vulnerabilities involved with CC, information protection challenges and strategies to such troubles are described right here. we've mentioned a number of the programs of cloud computing in this paper. This observe demonstrates that using this technology in an employer after addressing data protection risks can bring about a diractic change. we have long past thru a number of the most important facts security demanding situations in cloud computing, a way to resolve them, and the advantages and downsides of cloud computing.This observe demonstrates that CC presents the capability to rent sources from useful resource sharing, which aids within the discount of E-Waste. Many troubles approximately cloud need to be tested in future research, along with protection, privateness, effectiveness, rights, profitability, and different non-technical aspects. As a result, research groups encounter severa challenges and should look at answers to both technological and non-technical troubles. the safety issues have to be very well investigated.

Reference

[1] H. Karajeh, M. Maqableh, and R. Masa'deh, "Privacy and Security Issues of Cloud Computing Environment," in Proceedings of the 23rd IBIMA Conference Vision, 2020, pp. 1-15.

[2] Aldossary, Sultan, and William Allen. "Data security, privacy, availability and integrity in cloud computing: issues and current solutions." International Journal of Advanced Computer Science and Applications 7.4 (2016): 485-498.

[3] N. Khan and A. Al-Yasiri, ''Cloud security threats and techniques to strengthen cloud computing adoption framework,'' in Cyber Security and Threats: Concepts, Methodologies, Tools, and Applications. Hershey, PA, USA: IGI Global, 2018, pp. 268–285.

[4] J.-Y. Park, S.-H. Na, and E.-N. Huh, ''An optimal investment scheme based on ATM considering cloud security environment,'' in Proc. 11th Int. Conf. Ubiquitous Inf. Manage. Commun., Jan. 2017, pp. 1–7.

[5] M. K. Hussein, M. H. Mousa, and M. A. Alqarni, ''A placement architecture for a container as a service (CaaS) in a cloud environment,'' J. Cloud Comput., vol. 8, no. 1, p. 7, Dec. 2019

[6] A. Sharma, B. Keshwani, and P. Dadheech, "Authentication Issues and Techniques in Cloud Computing Security: A Review," Available at SSRN 3362164, 2019.

[7] K.-L. Tsai, F.-Y. Leu, and J.-S. Tan, ''An ECC-based secure EMR transmission system with data leakage prevention scheme,'' Int. J. Comput. Math., vol. 93, no. 2, pp. 367–383, Feb. 2016.

[8] C. Rong, S. T. Nguyen, and M. G. Jaatun, "Beyond lightning: A survey on security challenges in cloud computing,"

Computers & Electrical Engineering, vol. 39, pp. 47-54, 2013.

[9] J. Cheng, S. Qi, W. Wang, Y. Yang, and Y. Qi, ‘‘Fast consistency auditing for massive industrial data in untrusted cloud services,’’ in Proc. Great Lakes Symp. VLSI, Sep. 2020, pp. 381–386.

[10] S. S. Rizvi, T. A. Bolish, and J. R. Pfeffer, ‘‘Security evaluation of cloud service providers using third party auditors,’’ in Proc. 2nd Int. Conf. Internet things, Data Cloud Comput., Mar. 2017, pp. 1–6.

[11] E. Turban, J. Outland, D. King, J. K. Lee, T.-P. Liang, and D. C. Turban, Electronic commerce 2018: a managerial and social networks perspective: Springer, 2017.

[12] H. Dey, R. Islam, and H. Arif, "An Integrated Model To Make Cloud Authentication And Multi-Tenancy More Secure," in 2019 International Conference on Robotics, Electrical and Signal Processing Techniques (ICREST), 2019, pp. 502-506.

[13] K. Kaviya, K. Shanthini, and M. Sujithra, "Evolving Cryptographic Approach for Enhancing Security of Resource Constrained Mobile Device Outsourced Data in Cloud Computing," 2019.

[14] Z. Yan, X. Li, M. Wang, and A. V. Vasilakos, "Flexible data access control based on trust and reputation in cloud computing," IEEE transactions on cloud Computing, vol. 5, pp. 485-498, 2015.

[15] Y. Sharma, H. Gupta, and S. K. Khatri, "A Security Model for the Enhancement of Data Privacy in Cloud Computing," in 2019 Amity International Conference on Artificial Intelligence (AICAI), 2019, pp. 898-902.

[16] S. Namasudra, "An improved attribute‐based encryption technique towards the data security in cloud computing," Concurrency and Computation: Practice and Experience, vol. 31, p. e4364, 2019.

[17] G. Somani, M. S. Gaur, D. Sanghi, M. Conti, and R. Buyya, "DDoS attacks in cloud computing: Issues, taxonomy, and future directions," Computer Communications, vol. 107, pp. 30-48, 2017.

[18] L. Alhenaki, A. Alwatban, B. Alamri, and N. Alarifi, "A Survey on the Security of Cloud Computing," in 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS), 2019, pp. 1-7.

[19] P. Deshpande, S. Sharma, S. K. Peddoju, and A. Abraham, "Security and service assurance issues in Cloud environment," International Journal of System Assurance Engineering and Management, vol. 9, pp. 194- 207, 2018.

[20] A. Singh and K. Chatterjee, "Cloud security issues and challenges: A survey," Journal of Network and Computer Applications, vol. 79, pp. 88-115, 2017.

[21] N. Almasalmeh, F. Saidi, and Z. Trabelsi, "A Dendritic Cell Algorithm Based Approach for Malicious TCP Port Scanning Detection," in 2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC), 2019, pp. 877-882.

[22] R. Anitha, P. Pradeepan, P. Yogesh, and S. Mukherjee, "Data storage security in cloud using metadata," in 2nd International Conference on Machine Learning and Computer Science (IMLCS'2013), Kuala Lumpur (Malaysia), 2013, pp. 26-30.

[23] A. Mallik, A. Ahsan, M. Shahadat, and J. Tsou, "Man-in-the-middle-attack: Understanding in simple words," International Journal of Data and Network Science, vol. 3, pp. 77-92, 2019.

[24] V. S. P. P. C. Kumar and S. P. Rao, "Phishing attack detection," ed: Google Patents, 2019.

[25] S. Anwar, Z. Inayat, M. F. Zolkipli, J. M. Zain, A. Gani, N. B. Anuar, et al., "Cross-VM cache-based side channel attacks and proposed prevention mechanisms: A survey," Journal of Network and Computer Applications, vol. 93, pp. 259-279, 2017.

[26] P. Mishra, E. S. Pilli, V. Varadharajan, and U. Tupakula, "Intrusion detection techniques in cloud environment: A survey," Journal of Network and Computer Applications, vol. 77, pp. 18-47, 2017.

[27] N. Garcia, T. Alcaniz, A. González-Vidal, J. B. Bernabe, D. Rivera, and A. Skarmeta, ‘‘Distributed real-time SlowDoS attacks detection over encrypted traffic using artificial intelligence,’’ J. Netw. Comput. Appl., vol. 173, Jan. 2021, Art. no. 102871.

[28] J. Vinnarasi and N. Sudha, "Security Solution for SDN Using Host-Based IDSs Over DDoS Attack," Available at SSRN 3449613, 2019.

[29] D. E. Simos, J. Zivanovic, and M. Leithner, "Automated combinatorial testing for detecting SQL vulnerabilities in web applications," in Proceedings of the 14th International Workshop on Automation of Software Test, 2019, pp. 55-61.

[30] F. Mohammed and D. Uliyan, "A New Password Authentication Scheme Resistant against Shoulder Surfing Attack," 技術學刊, vol. 34, 2019.

[31] H. H. Neuvirth, R. H. Pliskin, T. Koren, J. Weizman, K. W. Reinsch, and E. Hudis, "Detecting attacks on web applications using server logs," ed: Google Patents, 2019.

[32] C. Busch, "Standards for Biometric Presentation Attack Detection," in Handbook of Biometric AntiSpoofing, ed: Springer, 2019, pp. 503-514.

[33] J. Natarajan, "Cyber Secure Man-in-the-Middle Attack Intrusion Detection Using Machine Learning Algorithms," in AI and Big Data’s Potential for Disruptive Innovation, ed: IGI Global, 2020, pp. 291-316.

[34] S. Chhabra and D. M. Durham, "Cross-domain security in cryptographically partitioned cloud," ed: Google Patents, 2019.

[35] L. Joseph and R. Mukesh, "Securing and Self recovery of Virtual Machines in cloud with an Autonomic Approach using Snapshots," Mobile Networks and Applications, pp. 1-9, 2019.

[36] K. Prabhakar, K. Dutta, R. Jain, M. Sharma, and S. K. Khatri, "Securing Virtual Machines on Cloud through Game Theory Approach," in 2019 Amity International Conference on Artificial Intelligence (AICAI), 2019, pp. 859-863.

[37]. Singh, Parbhakar, Parveen Kumar, and TanweerAlam. "Generating Different Mobility Scenarios in Ad Hoc Networks.", International Journal of Electronics Communication and Computer Technology, 4(2), 2014

[38]. K. Janjua, M. A. Shah, A. Almogren, H. A. Khattak, C. Maple, and I. U. Din, ‘‘Proactive forensics in IoT: Privacy-aware log-preservation architecture in fog-enabled-cloud using holochain and containerization technologies,’’ Electronics, vol. 9, no. 7, p. 1172, Jul. 2020.

[39]. Alam, Tanweer. "Tactile Internet and its Contribution in the Development of Smart Cities." arXiv preprint arXiv:1906.08554 (2019).

[40]. TanweerAlam, “5G-Enabled Tactile Internet for smart cities: vision, recent developments, and challenges”, JURNALINFORMATIKA, Vol. 13, No 2, July 2019, pp. 1-10.

[41]. Alam, Tanweer, Abdulrahman A. Salem, Ahmad O. Alsharif, and Abdulaziz M. Alhejaili. "Smart Home Automation Towards the Development of Smart Cities." APTIKOM Journal on Computer Science and Information Technologies 5, no. 1 (2020).

[42]. TanweerAlam, “Efficient and Secure Data Transmission Approach in Cloud-MANET-IoT Integrated Framework”, Journal of Telecommunication, Electronic and Computer Engineering, Vol 12(1), 2020.

[43]. Novais, Luciano, Juan Manuel Maqueira, and Ángel Ortiz-Bas. "A systematic literature review of cloud computing use in supply chain integration." Computers & Industrial Engineering 129 (2019): 296-314.