Journal of Advances and Scholarly Researches in Allied Education
Vol. 18, Issue No. 3, April-2021, ISSN 2230-7540

A Review on Data Center Networking and Security Aspects in Cloud

Rajiv Garg[1]* Prof. (Dr.) N. K. Joshi[2] Prof. (Dr.) Mahaveer K. Sain[3]

[1] Department of Computer Science, CPU, Kota, India

[2] Department of Computer Science, CPU, Kota, India

[3] Department of Computer Science and Applications, MAISM, Jaipur, India

Abstract – Cloud computing is an evolving paradigm of technology that translates existing technical and computing ideas into utilities comparable to water and electricity systems. Data Center Networks (DCN) is the most important infrastructure for cloud computing's success. In the creation and management of a reliable cloud service, a scalable & efficient data center (DC) is essential. During the last several years, the increasing significance of networking data centers has highlighted associated problems such as conjunctive simplicity and service reliability. The agility needed for multi-tenant cloud requirements is lacking in existing DCNs, leading to poor responsively and reduced scalability. Several security & privacy issues need to be addressed in the cloud computing environment. In this work, we provide an overview of Cloud Computing (CC) also its classification. DCN for CC& evaluate construction prototypes depends upon these issues. This paper summarizes an outline of the data center network for CC, DCN for service models, and deployment models for cloud data centers (DCs) to decrease server power consumption. This comprehensive study also develops and analyses the many unsolved problems impeding the adoption and spread of cloud computing by the different stakeholders involved.

Keywords — Cloud Computing, Data Center Network, Cloud Storage, Data Security

----------X----------

1. INTRODUCTION

In the world of today, innovation is evolving fast and provides clients with different services, such as e-charging, e-mailing, messages, e-transactions, etc., that are paper-free and online. All these affordable administrations need an online exchange of information. This information, which may be private or delicate data such as information for business secrecy, Master Card details, management of an expansion into an account, etc., may be unsafe as a revelation of this information may be necessary to any unapproved customer. Capacity and cloud access are the biggest advances in computer science, but there are many. Many creators reveal that the benefits of cloud computing (CC) are somewhat different from their disadvantages. This however found that information security is becoming a huge issue as a partnership is building, even though we need to find a way to do everything you need with certain management. The most recent innovations in the cloud computing industry have been taken into accounts, such as hardware virtualization and distributed computations. The cloud model has six key characteristics, 3 service models &4 cloud-based models. Various models like SaaS, PaaS & IaaS can be found in the Cloud. It is available in several models, including public, private, and hybrid clouds in Fig.1 [1].

Virtualization technology spans the IT architecture of cloud computing and virtualizes the entire system. This includes servers, storage, networks, applications, etc. It has unified management and control over all resources to enhance the efficiency & flexibility of the system as a whole. Virtualization is also an essential technology for solving and making resource planning flexible, a problem of unified device management. The Cloud storage model can be built into a storage layer of all storage units with the same storage structure and provides single, transparent, and well-encapsulated limits for the user of the Storage Area. [2]. Cloud computing only implies the storage and access to data and applications over the Internet, instead of computer hardware. It provides environment development, resources management capability, cloud application software [3].

Recently, data centers were given considerable attention as hosting broad-scale service Applications as a cost-efficient data storage infrastructure. Regular uses of large data centers, web exploration,

and large scope computing are big companies like Google, Amazon, Yahoo & Facebook. Datacenter service hosting has developed as a multi-billion-dollar company in the future IT industries with the development of cloud computing. The industries are seeking scalable IT solutions, such as in-house or third-person hosted data centers, with the advancement of virtualization technologies and the benefits of economies of scale. A DC is an interface comprising storage devices, network devices, and servers (physical machines) (e.g. switches, routers, and cables). The key infrastructure to support the ever-growing cloud-based services is large data centers. The scalability and reliability of such services in data centers will therefore be a key contact. To respond rapidly to changing requests & service needs, the data center network (DCN) in particular should be agile and reconfigurable. Important research has been performed on the development of DCN topologies to acquire improved data center arrangements [4]. The data center consists of servers, storage, networks, power systems, refrigeration systems, etc. Data centers, including online companies, smart grids, and scientific computing, are dedicated to large-scale services. The DCN network consists of DC& provides network topology, routing devices, & protocols description data center connections DCN. [5,6].

Stocking is one of the most popular functions of the cloud. To avoid a breach of user data by security mechanisms, user records are saved on a remote server. Cloud storage is one of the most popular cloud computing features. Data is maintained in many servers managed by the cloud provider. The users do not know the physical location of a server. Only a forename that stores data can be found in a precise location, but information can be stored at various locations on one or more servers. It is one of the main aspects of CC. Cloud systems should therefore be highly reliable, accessible, and data-secure. Virtualization is the backbone of CC, but it has several advantages such as multi-tendance, resource distribution, and flexibility. The acceptance of cloud services by this set of customers is affected by this vulnerability.

Cloud storage [7] has evolved into 3 classes, one which ensures a secure and cost-effective solution for the fusion of two classes. Public cloud storage companies, which offer a lease-able commodity storage infrastructure (The network bandwidth used in the infrastructure both in terms of short or long-term storage). Private clouds use public cloud storage concepts, but they can be securely incorporated into a firewall of the user. Finally, both models allow hybrid cloud storage to merge, which data should be kept and secured privately in public clouds. The new device of cloud-based storage comes mutually using cloud computing, usually having two meanings: virtualized and high-scalability cloud-based storage resources. This new concept of cloud storage is not well defined. Furthermore, the relationship between cloud storage, storage cloud [8][9], service stockpiling, and cloud storage must be clarified.

Cloud-specific security solutions can attract companies and government agencies to join the cloud for confidentiality, integrity, and privacy of verified information. Several data confidentiality mechanisms are used, although this mechanism mainly targets external attacks and Provides little cloud-provider protection (Insider Attacks). Some mechanisms should therefore be developed to allow users to monitor their data. Data security concerns stand against users and prevent them from taking benefits of a cloud computing system. Many types of research papers have been published in the discussion of the security problems that could face cloud computing and violate user's data [10, 11].

2. CLOUD COMPUTING (CC)

CC [12] is also referred to as 'internet computing,' which materializes any organization or device on a server with its services such as storage, use, and the Internet. In cloud computing, the term was introduced by Google CEO Eric Schmidt during the conference of the industry in 2006 years. Cloud computing was mainly used. Cloud computing is also referred to as the storage and storage of data, programs, or applications on the internet rather than pc. No data is lost when data is saved in the cloud because it is generated in a cloud when data is saved or a server distributes cloud to replicate our data. The risk factor for cloud use is that a person unauthorized to access the information will switch to safety. Cloud is a model development and deployment model that has two main models.

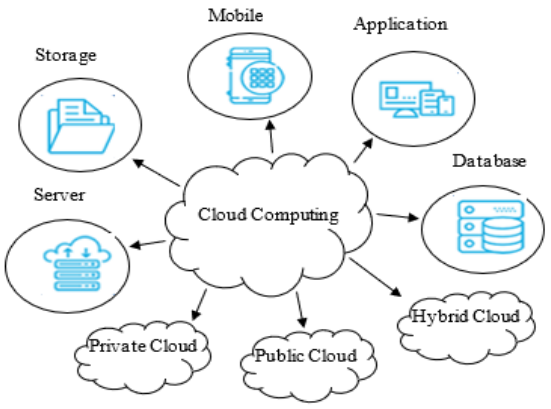

Fig.1. Cloud Computing

The deployment model includes the service's infrastructure, software &platform for service. Modeling includes a private-public cloud & hybrid cloud. Four hardware layers, infrastructure layers, platform layers as well as applications are included. Many of the business organizations were also attracted by using all these cloud services. Cloud

contributes to maintaining and developing a healthy business through its services.

A. Classification of Cloud Computing

CC's key attributes are Multi-tenancy, massive scalability, flexibility, payment, and autonomy. The cloud model is spilled into 3 groups as follows:

- PaaS (Platform as a Service), in its various programming languages, provides application development platforms;
- SaaS (Software as a Service) allows the use of online applications and software that are hosted by a user through the use of various software languages.
- IaaS offers users access to online applications and software hosting the Service Infrastructure user.

The cloud computing implementation model includes

- Public cloud is owned & sold by the service provider to the public.
- A company's private cloud is owned or rented, like a private cloud, however, cloud resources are shared between closed communities.
- Hybrid cloud, which displays two or more models of deployment [13].

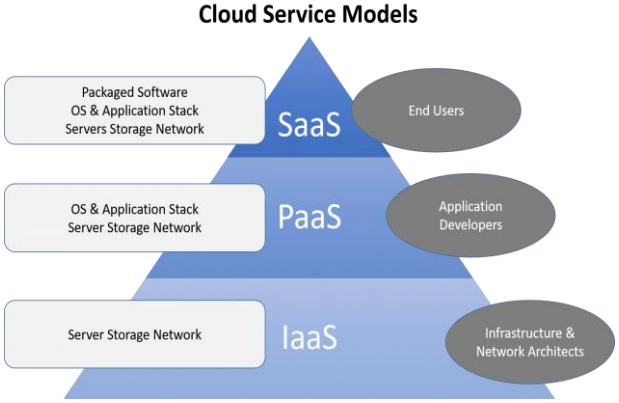

Fig. 2: Service Models of Cloud Computing

Table 1. Techniques of cloud computing & its benefit and drawback

S. No.	Technique name	Advantages	Disadvantages
1	Trust & Security (2015)	Confidence management has been presented	It only takes into account customer input. No consideration has been given to different parameters.
2	Control Data Access (2015)	A different algorithm has been used to secure cloud computing. Defaults can be secured in cloud administrations because the encryption keys have been manufactured using trust models.	Sometimes cryptographically saved data creates a problem as other usual applications access it
3	Multi Authority (2014)	The team interacts independently with each other. Failure or procedure of one influence, therefore, doesn't affect the function of each authority	Overhead occurs in an organization with competent authorities.
4	Trust-based Reputation model (2015)	Some attack detection methods were established	Very few exact results were obtained
5	A trust service scheduling (2014	Results shown were efficient and viable and customers can select workflow services of various cloud services	Dynamic changes in CC status were difficult to manage
6	Attribute-based encryption (2013)	Overhead decrease in the press release. Provide a fine grain to the access control. Resistance to collusion is a highlight of protection, depending on the encryption attribute (ABE)	To encrypt information from any approved customer, the information owner must use the public key.
7	Hierarchical Attribute-set based encryption (2013)	Low continuation costs & operating costs. Fast adversity Recovery	Data proprietors are resistant to domain control
8	CP-ABE (2012)	The CP-ABE resolves the assigned base encryption and supports real-life access control.	The customer consolidates all characteristics into a single set of solutions [14]

B. Security in Cloud Computing

According to the review conducted by preceding reports, data security is measured as an essential research issue in CC. Important data security issues include integrity of information, availability of data, information discretion, data clarity & data control. Data security can be achieved through different features, like access reins & encryption. Service suppliers should ensure that their provisioning communications are safe and that customer data is secured. On the customer's side, they should investigate Data Security (DS) measures that cloud provider is providing security techniques. Cloud provider selection is provided with techniques.

Techniques include a variety of encryption methods, for example, AES, RSA, etc. Since information is saved in the cloud, the data of unauthorized users is endangered. Mechanisms must not be ignored to stop this right of entry management. In arrange to prevent the warning to critical data, a cloud provider should provide authentication to check user authenticity. Different authentication schemes such as SSL, CHAP, &PKI are available to monitor user authenticity. After authentication, an authorization may be given which limits access to users.

3. DATA CENTER NETWORK (DCN)

Recently, the design of DC infrastructure has been receiving major study interest both from industry & academia, in no little component because of the increasing significance of DCs in supporting & sustaining fast-expanding Internet-based applications such as search (for example, Google,Bing), video content hosting and distribution (for example, YouTube, Netflix), social networking (for example, Twitter, Facebook), as well as large scale computations (for example, bioinformatics, indexing, data mining). For instance: A Chicago-based data center, one of the biggest ever DCs with a surface size of over 700,000 feet, supported the Microsoft Live online services. In particular, CC is a culmination in integrating computing & data infrastructure to offer scalable, agile & cost-effective methods to meet increasingly important IT requirements of both businesses & the general public (computing, storage, and applications). [15,16].

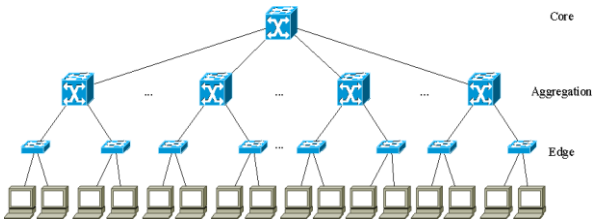

Fig. 3. Data Center Network

The data center [17] is A set of servers, network devices, storage systems, refresh systems, power systems, etc. DCs are designed for large-scale applications for services like online companies, Smart Grid & scientific computing. DCN consists of the data center that also offers data center connections that are outlined in its topology, switching or routing devices & protocols used. For the following reasons, DCN offers numerous functions to organize cloud computing:

DCN enables thousands of data center servers to be connected efficiently so that the DCN system can expand its service.

- For massive machine-to-machine communications, DCN offers travel reliability and efficiency in which cloud activities emerge as work charges on data center servers.
- The DCN supports different techniques for virtualizing which help to create Virtual Machines (VM). DCN should have the capacity to isolate and migrate to a huge variety of virtual instances.
- Previous DCN research has produced solutions for several applications, including data center backup, green computing, of which some may also address cloud consider service issues [18-21].

A. Cloud Computing & DCN

The architecture of CC depicts cloud computing, physical & virtual layer separation. The physical layer is primarily accountable for providing hardware resources of DCN in real-world DCN like CPU, memory, and bandwidth. Activities from the two other layers are transformed into workloads where high-level activities include transmission & transmission of information through different physical agents such as server, middle box, or switch. The virtual layer provides cloud users with virtual instances, like VM and virtual networks. A virtual resource in this layer is allocated by different policies that serve the cloud service model. The final layer is CC that defines the virtual layer primarily for cloud services. Cloud activities include mainly cloud services, Cloud deployment, Big Data, & distributed cloud systems in this work. The other layers of DCN in terms of traffic efficiency, on-demand, & reliability are highly demanded by all these activities [22].

B. DCN for Cloud Service Model

DCNs for CC are crucial use case because they provide cloud computing service model infrastructure. Different cloud computing model services are described via US NIST (National Institute of Standards & Technology). SaaS, PaaS, & IaaS are the three most well-known service models, already deployed in today's corporate DCs. [23-25].

1) **DCN for SaaS Model:** This model doesn't need every user, because all of these tasks are accomplished by the CC system, to manually download, install, configure, run, or using software applications in their computational environment. Because every DCN server performs multiple computational tasks for huge user space services, SaaS needs scalable DCN to support large parallel computing applications, like big data systems.

2) **DCN for PaaS Model:** Tools& libraries of virtual machines are being abstracted from the application on a DCN server as virtual instances for this model. DCN also performs platform maintenance, load balance & extension.

3) **DCN for IaaS Model:** DCN must first virtualize appropriate cloud infrastructure resources to serve the IaaS model. Second, all IaaS VMs should be mapped to DCN servers such that each server uses all infrastructure services. DCNs are also responsible for virtual infrastructure services maintenance, recompense, and migration in all VM systems[22].

B. DCN for Cloud Deployment Model

CC provides a range of cloud service deployment models. Three common business cloud models exist private, public, and hybrid [23]. The details of the requirement are described below.

1) **DCN for private cloud:** This model gives cloud users the greatest level of performance control, reliability & security. DCN must establish VPN (a virtual private network) to install each user's private cloud model. A network must be extremely reliable & user disc space & permissions should be isolated.

2) **DCN for the public cloud:** In this model of deployment SLA is used by all public users. The coordination of security, load balances, and routing in DCN is not a strict requirement, but the QoS is based on the model for a cloud service. As cloud services frequently vary with customer's requirements, DCN needs to ensure that its service deliveries are flexible.

3) **DCN for hybrid cloud:** This model combines private and public clouds. Users maintain sensitive information in the private cloud in a hybrid model while outsourcing critical information & processing to a public cloud. DCN aims at establishing the optimum boundary among private &public cloud components for Hybrid clouds. For example, if a user outsources insensitive data to a public cloud, DCN should avoid data loss while preserving the reliability of every private cloud [26].

4. CLOUD STORAGE

As storage is one of the key infrastructures of clouds, storage data security is the main issue for all systems of CC, especially cloud storage services. Consequences for both service providers and users of a security breach of cloud storage might be extremely damaging. The service provider could lose its customers without users' confidence. In contrast, users with lost or hacked valuable data could suffer irrecoverable damage or loss. Many cases have been stated as cloud security threats. Many leading service providers, such as Google, Amazon & Windows, had disconnection of their web-based cloud services for various reasons, like power failure, hardware, & software failures. E.g., lightning hit Amazon Web Service's server, which caused the power generator to be damaged. While Amazon transferred data successfully into a backup server, the service stopped after its uninterruptible power supply (UPS) was discontinued. In 2006 mass e-mail deletions occurred in Gmail; many users found that without further notice by Google they lost their e-mails & contact information. After users answered the problem, Google was unable to recover accounts. Recently in July 2012, another incident occurred. Drop box, a general cloud storage service, was attacked by hackers due to a security breakdown in the access control. Some users have reported receiving tones of spam emails and even leaked user passwords.

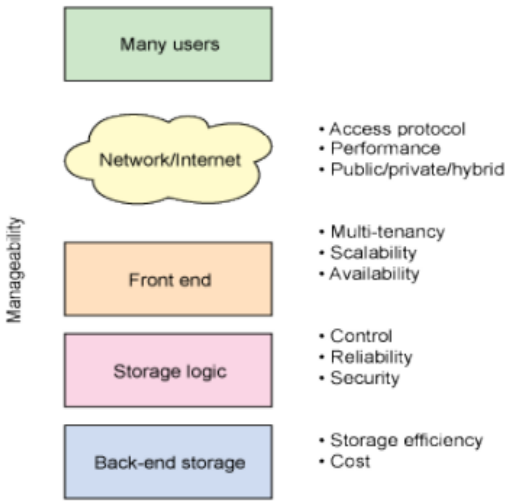

Fig. 4. Cloud Storage Architecture

Cloud storage architectures primarily deal in extremely scalable & multifunctional ways with the supply of storage on request. Architectures of cloud storage generally comprise the front end (see Figure 3 that exports an API for storage access. This API is a SCSI protocol in traditional storage systems; however, these protocols evolve in the cloud. The front ends of the web server, the file front ends and even more, conventional front ends can be found (like Internet SCSI, or iSCSI). There is a layer of middleware behind the front end I call logic of storage I've been calling storage logic. This layer implements different functions, like reproduction & data reduction, through standard data placement methods (with consideration for geographic placement). Lastly, background physical data storage is performed. It may be an internal protocol that has those characteristics or a standard physical disc background.

Table 2. Analysis of Storage Techniques

Reviewed papers	Explanations & Major Issues Handled	Advantages
Bhatia et al. [27]	Using HDFS for cloud storage architecture, compression algorithm, and MongoDB database.	Improved reliability of storage by saving the resulting bandwidth and storage space.

Pratiba et al. [28]	Top-n multi-keyword retrieval over encrypted cloud data.	Compared to other ranked keyword quests, it is secure, scalable, and reliable.
Guo et al. [29]	Interval index, hybrid model view query processing & improved search intersection method for cloud sensor model view results.	It provides an optimized query reaction time and better index updating effectiveness.
Leesakul et al. [30]	Balance among storage reliability & fault-tolerance needs & restrict static deduplication method, which cannot withstand changing behavior of the user.	It uses to handle scalability problems.
Liu et al. [31]	A private cloud storage data deduplication scheme with a CDMI standard depends upon the basic DFS.	It lowers costs and improves the effectiveness of storage. The interoperability of storage nodes is also increased.

5. DATA SECURITY

It is considered an important subject of research in CC. Data accessibility; data integrity, data trustworthiness, data transparency [32], & data control where data resides are key issues relating to data safety. There are different aspects to data security, like access control & encryption. Service providers should ensure that their infrastructure & customer data remain secure [33]. On the customer's side, it should examine data security measures, which cloud providers provide security techniques. A cloud supplier selection is provided with techniques. There are different techniques of encryption, likeRSA,AES [34], etc. There are different algorithms available. Since data is saved in the cloud, the data of unauthorized users is threatened. Controls must not be ignored [35] to stop this approach. To prevent threats to critical data, the cloud provides an authentication method that checks the user's authenticity. Different authentications such as SSL, PKI and CHAP are available to validate the user's authenticity [36]. Authorization may be provided after authentication that restricts the user's access.

A. Issues of Data Security

Data security as a right for the tenant is an important requirement. Secure services draw users into a cloud to store their data. Cloud storage companies are looking for technology that may control and improve access to cloud data. Data attacks and interceptions are also increasing with the size of the data. CC offers storage services as a vital environment in which the user has no data control. In such a situation, a user may wonder "what happens if I delete my data?" & "what happens if I remove it?". The literature contains many solutions for cloud data security. Security solutions were subdivided into 4 layers in [37] (that is authentication, availability, trustworthiness, & integrity). They supposed that trustworthiness automatically guarantees integrity when confidentiality is achieved. This section, however, is devoted to a more in-depth study of data security issues. A current study on cloud-based data privacy & security [38] pointed out the three key reasons for cloud computing's features, independent of server technology. It includes multi-purpose outsourcing.

1) Confidentiality Issues

2) Issues concerning integrity

3) Data Access Issues

4) Authentication and Authorization Issues

5) Data Breaches

B. Data Security Challenges

Since we move into the cloud model, data security and privacy must be highly emphasized. Data leakage or data loss may have an essential effect on an organization's corporation, brand, & trust. In the picture. 2. Prevention of data leaks with 88% vital & very major tasks is considered as a most significant aspect. Likewise, the segregation & security of data has a safety impact of 92%.

a) **Security:** Data could be misused if many organizations share resources. To evade risk, data repositories and data involving storage, transit, or processing need to be secure. The most significant issues in CC are data protection. Moreover, authentication, authorization & access management for data saved in the cloud is important for enhancing security in cloud computing. Data security's three key areas are confidentiality, Integrity, and Availability.

b) **Locality:** Data is distributed across the region numbers and the data is difficult to locate in cloud computing. When data are transferred to various geographical locations, rules governing such data can also be changed. Thus, compliance with cloud computing and privacy laws is a problem. It should be known to customers where they are and informed by the service provider.

c) **Integrity:** The system needs to be protected to enable the data to be modified only by the authorized person. To prevent lost data, data integrity needs to be correctly maintained in a cloud-based environment. Generally, ACID properties should be used to preserve the data truthfulness of all cloud transactions. Many transaction management problems are encountered in most Web

services as they use HTTP services. HTTP doesn't support or warrant transaction delivery. API itself can be used for transaction management.

d) **Access:** The right to data entry refers primarily to data security policies. Organization employees are provided with access to the data section depends upon their company safety policies. Other staff working in a similar organization cannot access the same information. Different encryption methods and key management mechanisms ensure that only legitimate users share the data. Only by various key distribution mechanisms is the key given to approve parties. If data from unauthorized users are to be protected, data security protocols should be enforced strictly. Since the Internet is available to all cloud users, privileged access is needed. Data encryption & security measures can be used by users to avoid risk security

e) **Confidentiality:** Data confidentiality is one of the key necessities when stored in a remote server. Users should know that data is saved in the cloud and that data understanding and classification can be kept confidential.

f) **Breaches Data:** An additional key protection concern that needs designate focused on the cloud is violations. Since big data is kept in the cloud by different users, malicious users are likely to enter the cloud to cause a high-value attack in the whole of the cloud environment. Various accidental difficulties or an insider attack may cause an inappropriate violation.

g) **Segregation:** One of the main aspects of CC is multi-tenancy. Data can be intruded on by multi-tenancy since different users can save data on cloud servers. Through injecting or using a client code, data may be intruded. Data from the other customer data must therefore be stored unconnected. Vulnerabilities in data separation can be detected or detected by testing such as inoculation, data validation, and uncertain storage.

h) **Storage:** Virtual machine storage data has many problems One such problem is data storage reliability. In a physical infrastructure that could cause a security risk, virtual machines must be stored.

i) **Data Center:** Surgery For disaster and data transmission bottlenecks, cloud-based organizations must safeguard their data without loss. Data storage and admittance are problematic if data is not properly managed. Data defeat in case of adversity is caused by cloud providers [39].

6. LITERATURE SURVEY

From the literature, it is evident that various researches have been done in the field of CC using cloud storage, secure data centers, and various data securities approaches. Some of the research work which guides me in the way of completing my paper is discussed below in this section.

W. Li et al. (2021) DCN has gained lots of interest from industry & academia in current years to overcome these difficulties, & many innovative mechanisms at various layers are suggested to increase the transmission efficiency of DCNs. In meantime, numerous surveys have appeared to represent contemporary data center network research. Past DCN surveys, on the other hand, have mostly focused on a single network layer, making it impossible for readers to learn about important studies on a holistic level. They use a multi-layered top-down taxonomy to categorize literature & offer various possible aspects for future research in DCNs to assist readers in quickly understand present research efforts in this area [40].

F. Wang et al. (2021) This study gives an overview of large data cloud computing ideas, features, and advanced technologies. Data access, data integrity, data isolation, data transfer, data destruction, & data exchange are all covered in terms of protection problem data security & privacy control. Finally, a virtualization structure & associated tactics are provided to combat risks & improve data security in a large data cloud environment [41].

V. Sharma and R. Mishra (2020) In this day & age, as storage & computing solutions migrate from workstations to a cloud, DCNs are reaching new heights for large data transactions between combined servers. Because of the exponent rise in cloud services, modern DCNs face some issues, including scalability, energy efficiency, congestion, & cost, all of which are directly influenced via the architectural creation of DCNs. As a result, the purpose of this letter is to give an orderly descriptive review of different DCN topologies, as well as a comparison of these constructions to DCN efficiency matrices. Lastly, the letter summarizes potential future improvements in DCN designs & functions [42].

P. Singh and S. K. Saroj (2020) The objective of this study is to give a safe public auditing method that uses 3rd-person auditors to validate the privacy, reliability, & integrity of cloud-based data. Cloud computing is a rapidly expanding technology that offers low-cost data storage & extremely quick computer capabilities. The cloud service provider or a cloud caretaker is responsible for all data kept in a cloud. As data owners, they are concerned about the authenticity & trustworthiness of data kept on a cloud. Any unauthorized user or individual can misappropriate or manipulate data. The AES-256

technique is used for encryption, SHA-512 for integrity checks, & RSA-15360 for public-key encryption in this suggested auditing approach. Also, execute data dynamics operations like addition, deletion, & alteration of information [43].

A. Bin Rosle et al. (2019) The effects of using optical switches & spreading server racks & moves in DCNs are investigated in this study. The placement formulations are then tested against various network topologies, & total network efficiency is analyzed [44].

J. Lin and L. Liu(2019) Dependent on domain information modelling & large data analysis of industrial data, this study develops an industrial large data analysis method library. This work evaluates a process of choosing traffic features of activities in a commercial Internet by evaluating the behavior features of commercial internet network traffic data; creates a propagation & evolution model of protection events in a commercial Internet; & creates a traceability map of security event propagation. To simplify the difficulty of protection act detection & analysis, this research mixes features of enormous data volume &centralized control of a proposed industrial Internet. It has reference value for commercial Internet managers while developing node routing methods [45].

C. Suet al. (2019) This study examines numerous data security issues & suggests a large data security development approach in reply. The findings suggest that by integrating technology with suitable policies and regulations, the issue of huge data security and privacy protection may be best solved [46].

Y. Chenget al. (2019) This article explores 2 optical switching scheduling algo's dependent on input Queue (IQ) optical changing planning method of Stringent Delay First (SDF) and m - order Stringent Delay First (m - SDF) to solve DCN performance optimization scheduling and routing algorithm design difficulties. Examine 2 data center network models: Multiple Independent-DCN (MI-DCN) & Integrated dispersed DCN. SDN (Software Described Network) idea is brought into DC, & transfer routing algo is created to achieve data center resource load balancing [47].

K. A. Saedet al. (2019) This study planned to employ an extensive literature analysis to design questions & an in-depth discussion to gather information. This study's target respondents must be experts in the field of cloud security. Lastly, HPC3 (High-Performance Cloud Computing Center) will develop & test a data governance security evaluation concentrating on IaaS in cloud data centers [48].

7. CONCLUSION

Cloud computing is a trending technology in a computerized world. Security has become one of the major concerns with the continued development and spread of cloud computing. To avoid security attacks, and also the destruction of infrastructure and services, the CC platform has to provide dependable safety technologies. Cloud computing is undoubtedly the next development trend. Cloud computing gives us almost endless computing capabilities, good scalability, on-demand service, etc., and also difficulties in terms of security, private life, legal concerns, etc. However, it is very urgent to resolve the existing problems. This article discusses the fundamentals of CC& security problems that start with the cloud's fertilized, shared, public, private, and hybrid nature. A community must take proactive measures to guarantee security to promote cloud computing. And also presented a brief description of the data center network for cloud computing.

REFERENCES

[1] M. P. Vaishnnave, K. Suganya Devi, P. Srinivasan (2019), "A Survey on Cloud Computing and Hybrid Cloud", International Journal of Applied Engineering Research ISSN 0973-4562 Volume 14, Number 2, pp. 429-434

[2] DeLi (2012), Report of the Cloud Computing Technology Development (2012). Beijing: Science Press.

[3] Mandeep Kaur, Manish Mahajan (2013), "Using encryption Algorithms to enhance the Data Security in Cloud Computing", "International Journal of communication and Computer technology", Volume1, Issue3.

[4] Md. Faizul Bari, Raouf Boutaba, Rafael Esteves, Lisandro Zambenedetti Granville, Maxim Podlesny, MdGolam Rabbani, Qi Zhang, and Mohamed Faten Zhani (2013), "Data Center Network Virtualization: A Survey", IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 15, NO. 2, SECOND QUARTER.

[5] D. Abts, B. Felderman (2012), A guided tour through data-center networking, Queue 10 (5), 10: pp. 10–10:23.

[6] M. Chen, H. Jin, Y. Wen, V.C. Leung (2013), Enabling technologies for future data center networking: a primer, Netw IEEE 27 (4), pp. 8–15.

[7] T. Sivashakthi1, Dr. N. Prabakaran: A Survey on Storage Techniques in Cloud Computing" Volume3Issue12/IJETAE.

[8] Robert L.Grossman, YunhongGu, Michael Sabala, Wanzhi Zhang (2009). Compute and storage clouds using wide area high-

performance networks. Future Generation Computer Systems, 25(2): pp. 179-183.

[9] Brandon Rich, Douglas Thain (2008). DataLab: Transactional data-parallel computing on an active storage cloud. In: Proc. of the 17th International Symposium on High-Performance Distributed Computing, pp. 233-234.

[10] P. Mell and T. Grance (2011), "The nist definition of cloud computing,".

[11] C. Modi, D. Patel, B. Borisaniya, A. Patel, and M. Rajarajan (2013), "A survey on security issues and solutions at different layers of cloud computing," The Journal of Supercomputing, vol. 63, pp. 561–592, The final publication is available at Springer via http://dx.doi.org/10.1007/s11227- 012-0831-5.

[12] N. Dhivya (2017), A Survey Paper On Cloud Computing", IJAESE, Vol. 06, pp.1-8.

[13] Sized Amin Soofi, M. Irfan Khan (2014), "A Review on Data Security in Cloud Computing", International Journal of Computer Applications (0975 – 8887), Volume 94 – No 5.

[14] M. P. Vaishnnave and P. S. Devi, K. Suganya, M. P. Vaishnnave (2019), "A Survey on Cloud Computing and Hybrid Cloud,"" A Surv. Cloud Comput. Hybrid Cloud", Int. J. Appl. Eng. Res. ISSN 0973-4562 Vol. 14, Number 2 pp. 429-434, vol. 14, no. 2, pp. 429–434.

[15] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia (2009), "Above the clouds: A berkeley view of cloud computing," EECS Department, University of California, Berkeley, Tech. Rep. UCB/EECS-2009-28, [Online]. Available: http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.html

[16] A. Greenberg, J. Hamilton, D. A. Maltz, and P. Patel (2009), "The cost of a cloud: research problems in data center networks," SIGCOMM Comput. Commun. Rev., vol. 39, no. 1, pp. 68–73.

[17] Bin Wang (2015), "A survey on data center networking for cloud computing", Computer Networks, Science Direct, Elsevier

[18] K. Chen, C. Hu, X. Zhang, K. Zheng, Y. Chen, A.V. Vasilakos (2011), Routing in data centers: insights and future directions, IEEE Netw Mag 25, pp. 6–10.

[19] D. Abts, B. Felderman (2012), A guided tour through data-center networking, Queue 10 (5), 10: pp. 10–10:23.

[20] M. Chen, H. Jin, Y. Wen, V.C. Leung (2013), Enabling technologies for future data center networking: a primer, New IEEE 27 (4), pp. 8–15.

[21] A. Wang, M. Iyer, R. Dutta, G.N. Rouskas, I. Baldine (2013), Network virtualization: technologies, perspectives, and frontiers, J Lightwave Technol 31 (4), pp. 523–537.

[22] M. Chen, S. Mao, Y. Zhang, V. Leung (2014), Big data: related technologies, challenges and prospects, Springer briefs in computer science„ Springer.

[23] NIST, National Institute of Standards and Technology (NIST), 2010-2015, (http://www.nist.gov/).

[24] D. Borgetto, M. Maurer, G. Da-Costa, J.M. Pierson, I. Brandic (2012), Energy- efficient and SLA-aware management of IaaSS clouds, in: Proceedings of the e-Energy.

[25] S. Walraven, E. Truyen, W. Joosen (2014), Comparing PaaS offerings in light of SaaS development, Computing 96 (8).

[26] M. Kajko-Mattsson (2009), SLA management process model, in: Proceedings of the 2nd international conference on interaction sciences: information technology, culture and human, ICIS '09, ACM, New York, NY, USA, pp. 240–249.

[27] Vandana Bhatia and Ajay Jangra (2014), "SETiNS: Storage Efficiency Techniques in No-SQL database for Cloud Based Design" EEE International Conference on Advances in Engineering & Technology Research (ICAETR 2014), Dr. Virendra Swarup Group of Institutions, Unnao, India.

[28] Pratibha, Dr. G. Shobha and Vijaya Lakshmi P. S. (2015), "Efficient Data Retrieval From Cloud Storage Using Data Mining Technique" international Journal on Cybernetics & Informatics (IJCI) Vol. 4, No. 2.

[29] TianGuo, Thanasis G. Papaioannou and Karl Aberer (2014). "Efficient Indexing and Query Processing of Model View Sensor Data in the Cloud" Big Data Research, Published by Elsevier Inc http://dx.doi.org/10.1016/j.bdr.2014.07.005 2214-5796.

[30] Waraporn Leesakul, Paul Townend, JieXu (2014). “Dynamic Data Deduplication in Cloud Storage” 2014 IEEE 8th International Symposium on Service Oriented System Engineering.

[31] Xiao-Long Liu, Ruey-Kai Shue, Shyan-Ming Yuan, Yu-Ning Wang (2016). “A file-deduplicated private cloud storage service with CDMI standard” Computer Standards & Interfaces, Published by Elsevier Inc http://dx.doi.org/10.1016/j.csi.2015.09.01044, pp. 18– 27.

[32] Anitha Y (2013), “Securiy Issues in cloud computing”, “International Journal of Thesis Projects and Dissertations (IJTPD) Vol. 1, Issue 1, PP: (1-6), Month: October 2013

[33] Qi. Zhang Lu. Cheng, Raouf Boutaba (2010), “Cloud computing: state-of-the-art and research challenges”, “The Brazilian Computer Society”.

[34] Parsi Kalpana, “Data security in cloud computing using RSA”, International Journal of Research in Computer and Communication technology, ISSN 2278-5841, Volume 1, Issue 4, September 2012

[35] H. Narayanan and M. Gunes (2011), “Ensuring access control in cloud provisioned Healthcare systems,” in Consumer Communications and Networking Conference (CCNC), page no-.247–255.

[36] Chittaranjan Hota, Sunil Sanka, Muttukrishnan Rajarajan, Srijith K. Nair (2011), “Capability-based Cryptographic Data Access Control in Cloud Computing”, “Int. Journal of Advanced Networking and Applications” Volume: 03; Issue: 03; Pages:1152- 1161

[37] L. Arockiam and S. Monikandan (2014), “Efficient cloud storage confidentiality to ensure data security,” in International Conference on Computer Communication and Informatics. IEEE, pp. 1–5.

[38] N. Kaaniche and M. Laurent (2017), “Data security and privacy preservation in cloud storage environments based on cryptographic mechanisms,” Computer Communications, vol. 111, pp. 120–141.

[39] R. Velumadhava Rao and K. Selvamani (2015), “Data Security Challenges and Its Solutions in Cloud Computing”, Procedia Computer Science 48, pp. 204 – 209.

[40] W. Li et. al. (2021), "Survey on Traffic Management in Data Center Network: From Link Layer to Application Layer," in IEEE Access, vol. 9, pp. 38427-38456, doi: 10.1109/ACCESS.2021.3064008.

[41] F. Wang, H. Wang and L. Xue (2021), "Research on Data Security in Big Data Cloud Computing Environment," 2021 IEEE 5th Advanced Information Technology, Electronic and Automation Control Conference (IAEAC), pp. 1446-1450, doi: 10.1109/IAEAC50856.2021.9391025.

[42] V. Sharma and R. Mishra (2020), "A Comprehensive Survey on Data Center Network Architectures," 2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), pp. 222-228, doi: 10.1109/ICRITO48877.2020.9197934.

[43] P. Singh and S. K. Saroj (2020), "A Secure Data Dynamics and Public Auditing Scheme for Cloud Storage," 2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS), pp. 695-700, doi: 10.1109/ICACCS48705.2020.9074337.

[44] A. Bin Rosle, T. S. Chin and W. D. Shen (2019), "Performance Analysis of Optical Switches and Rack Placement in Mesh and Ring Topology in Data Center Network," 2019 15th International Computer Engineering Conference (ICENCO), pp. 1-6, doi: 10.1109/ICENCO48310.2019.9027374.

[45] J. Lin and L. Liu (2019), "Research on Security Detection and Data Analysis for Industrial Internet," 2019 IEEE 19th International Conference on Software Quality, Reliability and Security Companion (QRS-C), pp. 466-470, doi: 10.1109/QRS-C.2019.00089.

[46] C. Su (2019), "Big Data Security and Privacy Protection," 2019 International Conference on Virtual Reality and Intelligent Systems (ICVRIS), pp. 87-89, doi: 10.1109/ICVRIS.2019.00030.

[47] Y. Cheng (2019), "Based on the Cloud Data Center Optical Switching Scheduling and Routing Algorithm Research and Practice," 2019 4th International Conference on Mechanical, Control and Computer Engineering (ICMCCE), pp. 941-9414, doi: 10.1109/ICMCCE48743.2019.00212.

[48] K. A. Saed, N. Aziz, A. W. Ramadhani and N. Hafizah Hassan (2018), "Data Governance Cloud Security Assessment at Data Center," 2018 4th International Conference on Computer and Information

Sciences (ICCOINS), pp. 1-4, doi: 10.1109/ICCOINS.2018.8510612.

Corresponding Author

Rajiv Garg*

Department of Computer Science, CPU, Kota, India

rajeevgarg1967@gmail.com