World Journal of Research and Review (WJRR)
ISSN: 2455-3956, Volume-12, Issue-4, April 2021 Pages 26-32

Security Standards for Data Privacy Challenges in Cloud Computing

Pratibha, Devender Dhakad, Dr. Subhash Chandra Jat, Vinod Todwal

***Abstract*— The rapid growth in cloud computing is becoming very notable due to the rapid advancement of Cloud Computing technologies. Cloud Computing means using computer resources as an on-demand service via the internet. In recent years it received considerable attention, but protection is amongst the key inhibitors in reducing cloud computing (CC)development. In general, it transfers user information and application software to vast data centers, i.e. the remotely located cloud that does not monitor the user and cannot fully secure data management. This unique aspect of cloud computing, however, poses several security issues that must be explicitly addressed and understood. This paper provides an analysis of cloud security issues, as well as the benefits /drawback of the cloud computing model for the service and implementation. Also, we discuss the safety issues of emerging cloud computing systems. As cloud computing applies to both Internet providers and the infrastructural facilities (i.e., data center hardware and systems software) that provide these services, we have security issues concerning the varied applications and infrastructures. More questions about security problems should be taken into account, for example, availability, protection, data integrity, data recovery, and so on.**

***Index Terms*— Cloud Computing, Cloud Security, Data Security, Security Issues.**

I. INTRODUCTION

Computers needed huge space in the first years of the 1960s and consumed a great deal of electricity and costly electronic components. However, the room size of the smaller computers was gradually replaced. The size of the computer and infrastructure nodes were unified at the end of the last century to form a distributed system that improved performance [1]. The cost of conventional computer infrastructure has increased in recent years, with the requirement for data and internet users increasing considerably. Traditional computing does not operate anywhere and at any time for accessing data. To do this, we must keep the information on an external storage unit.

Moreover, the increase in the number of online users on social networks, web surfing, and video chat, etc. [1]. For the global use of the internet to rapidly grow, we are turning to cloud computing in new ways to deal with data volume, diversity, and availability.

CC is a modern framework of computing that offers consistent access to widespread-range resources distributed on-demand. The appearance of cloud-based computing has great implications for the IT industry over the last years, where major businesses such as Microsoft, Amazon, and Google are committed to providing more dependable, stable, and cost-effective cloud services. Even now in today's cloud computing, there are still many issues. A new survey from the Cloud Protection Alliance (CSA)[2] shows safety is crucial to cloud computing.

CC can be seen as a digital computing archetype that can provide services on request at a minimal cost. Software as a service (SAAS), platform as a service (PaaS), and infrastructure as a service are three popular and influential service models in cloud frameworks (IaaS). In SaaS, a cloud service provider uses software with all its associated data, which users can access via internet browsers. With PaaS, a supplier offers a range of software applications that can solve everyday activities. In IaaS, the cloud service provider provides services that enhance the business capacity of customers who use virtual machines and storage [3].

Data security is a significant issue for cloud users. This technology requires adequate protections and mechanisms to mitigate the concerns of users. Most of the consumers of cloud services have reservations about their personal information that can be accessed or exchanged with other cloud service providers. There are four sections to the user information that needs to be protected: (i) Usage data; computer device details acquired (ii) Sensitive knowledge, information about fitness, bank accounts, etc. (iii) Data that can be used to classify the individual Personal Information (iv) Exceptional computer individualities; exclusively noticeable details e.g. IP addresses, specific identities of hardware, etc.

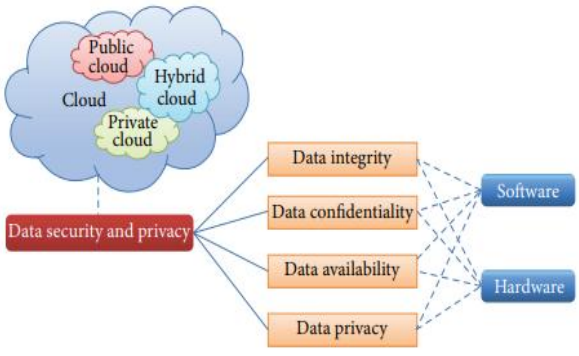

Fig. 1. Organization of data security and privacy in cloud computing

Thirty-five hazards were listed by the European News and Information Security Agency (ENISA), grouped into four categories: legal danger, organizational and policy hazards, technological hazards, and non-cloud-specific risk. ENISA listed eight of these risks as the most important. Five threats of which concern data protection, directly or indirectly. Such threats include failure of isolation, data security, compromise

Pratibha, M. Tech. Scholar, RCEW, Jaipur
Devender Dhakad, Computer Science, RCEW, Jaipur
Dr. Subhash Chandra Jat, Computer Science, RCEW, Jaipur
Vinod Todwal, Assistant Professor**,** Computer Science, RCEW, Jaipur

of the management interface, insecure deletion of data, and malicious insiders. The Cloud Protection Alliance (CSA) also describes 13 kinds of cloud computing threats. CSA declares seven of these 13 threats as major risks. The data confidentiality of five of the seven threats relates directly or indirectly to account operation, traffic hijacking, insecure application programming interface, information less/leaks, and malicious insiders. [4].

Section 2 shows the main concepts of cloud computing and architecture. The rest is arranged as follows. The security problems and issues are discussed in Sections 3 and 4. In Section 5, the paper is finished.

II. Cloud Computing

Cloud Computing offers a resource-sharing environment for the ascending systems, middleware and app development platforms, and business applications. Free infrastructure services that value other platform services, subscription infrastructure services, and shoppers' profitable free marketing services are among the Cloud operating models. ts. [6]. In some ways, the term cloud computing is characterized by researchers, scholars, business people, and IT businesses. Clouds is a vast pool of virtualized tools that are easily available and usable. These services can be modified dynamically to conform to a variable charge (scale), which enables maximum use of resources.

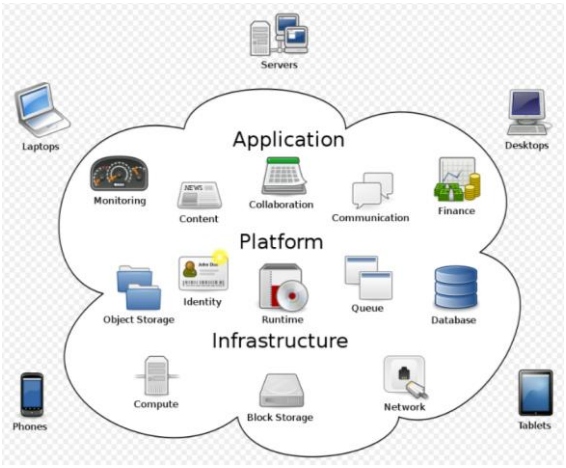

Fig. 2. Cloud Computing

Cloud computing is without a doubt the most popular subject in the IT industry. Google, Amazon, and Yahoo have implied a cloud computing strategy, and alternative web services firms, IBM, Microsoft, and other IT providers, as well as a large number of media service providers, are highly appealing in cloud computing, with the less price of the cloud computing platform being the emphasis of our industry.

A. Cloud computing benefits and drawback

A. Cloud computing benefits and drawbacks architecture of a cloud computing can be categories into four layers:

The Physical layer, the infrastructure layer, the platform layer, and the application layer, as indicated in Figure 2.

It provides different advantages.

- Infinite storage capacity
- Worldwide access to the document
- Modern version availability
- Easier group collaboration
- Lower cost computers for users

There are various disadvantages of cloud computing.

- Needs constant internet connection
- Stored data might not be secured
- Can be slow
- Cost comparison [5]

III. CLOUD COMPUTING ARCHITECTURE

CLOUD COMPUTING ARCHITECTUREThere is no doubt that cloud computing is the most famous topic in the IT business. Google, Amazon, Yahoo and alternative web service suppliers, IBM, Microsoft and alternative IT vendors have imply their cloud computing The architecture of a cloud computing can be categories into four layers:

The Physical layer, the infrastructure layer, the platform layer, and the application layer, as indicated in Figure 2.

The cloud computing architecture can be divided into four layers: the physical coating, the infrastructure layer, and the application layer, as shown in Figure 3.

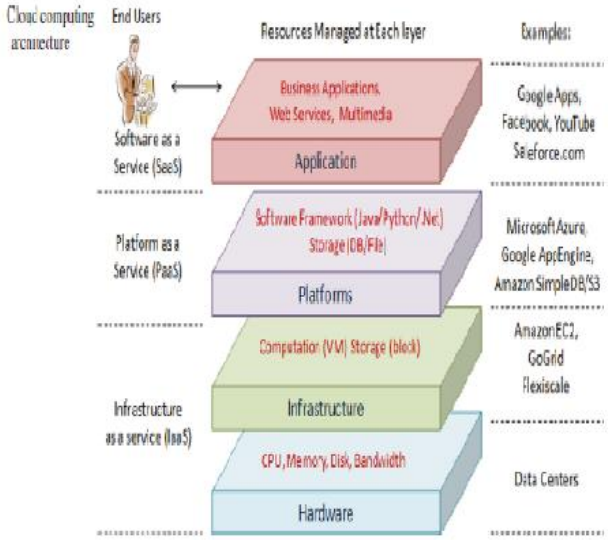

Fig. 3. Architecture Layers of Cloud Computing

i. **The Hardware layer:** The physical resources of the cloud, with rovers, servants, switches, refreshing structures, and control, are dealt with in the hardware layer.

ii. **The Infrastructure layer:** Often known as the virtualization layer is the infrared layer. The infrastructure level consists of a pool of storage and computer resources, which are split into KVM and VMware by physical resources.

iii. **The Platform layer:** The top-of-the-infrastructure layer platform level includes operating systems & requirement systems.

iv. **The Application layer:** The framework layer contains the existing cloud necessities, e.g. Multimedia and online services Business Apps. [6]

IV. Challenges of Cloud Computing

According to a 2008 survey showed by IDC, the key obstacles faced by forestry cloud computing are: square steps accepted by square organizations:

A. Security

The security problem has been a pioneer in cloud prevention. Without any doubt, golf shot your files, it seems to frighten you many that run your software system on someone else's magnetic disk victimization. Established security matters such as loss of information or phishing provide a significant threat to the information and software infrastructure of the company. Also, the multi-tenant model has raised new security problems with which new strategies are needed to cope. This means combined machine resources in cloud computing. For example, hackers use Cloud to arrange the Cloud normally offers several stable, comparatively cheaper infrastructure services to launch an attack.

B. Cost Accounting Model

Cloud clients should accept the balance of storage, connectivity, and convergence. Whereas migration to the cloud will dramatically decrease the value of the infrastructure, the price of the communication protocols will grow, i.e. that the value of transmitting the information to and from the general community and the Cloud community would probably be higher per unit of computing resources used. This limitation is defined in particular by the employer's hybrid model of the cloud where company information is dispersed through many public/private (in-house IT) clouds. Computing is sensitive only for intense hardware jobs on-demand intuitively.

C. Charging Model

The elastic resource pool has made it much more difficult to analyze value than conventional centers., measuring their pricing-assisted use of statistical computing regularly. Also, the corresponding instantiated virtual machine has been instead of the underlying physical server of the research unit. The importance of multi-residence growth among its donations is terrible for SaaS cloud suppliers. These include: redesigning and upgrading the kit that had been used in the beginning to provide one-tenant service; introducing new options to intensively configure, improving users' access performance and safety, and handling more than changes complexities.

D. Service Level Agreement (SLA)

While Cloud customers do not have any organization of the underlying computing infrastructure, they do so by transferring their main business functions into their entrusted cloud to ensure the consistency, comfort, responsibility, and efficiency of these resources. In other words, customers must receive service provision assurances from suppliers.

E. Cloud Interoperability Issue

Currently, each cloud has its solution, but cloud customers shift with the cloud, contributing to the creation of the "Hazy Cloud" This hinders the case of cloud ecosystems severely by forcing marketer security, which prevents consumers from choosing from multiple providers simultaneously to leverage resources within companies at entirely different levels. A lot of powerful, proprietary cloud arthropod sort makes the incorporation of cloud services in the current bequest systems operated by the nursing company difficult (e.g. a partner in the on-site nursing expertise center in the highly pharmaceutical industry for extremely immersive modeling applications). The key aim is to understand fluid awareness in clouds and between cloud and native apps. [6].

V. INFERENCE SECURITY LOOKING AND MODEL LIVE MODELS

The choice of deployment and delivery model are two key factors that define the level of concern in the cloud computing platform. According to Modi et al. & NIST, the industry-standard comprises three deployment and three distribution models. Each of these three models has specific security consequences. The following paragraphs address briefly each model and its safety implications:

A. Cloud Deployment Model

The three most popular modes of cloud deployment are private cloud, hybrid community, cloud, and cloud public. [7].

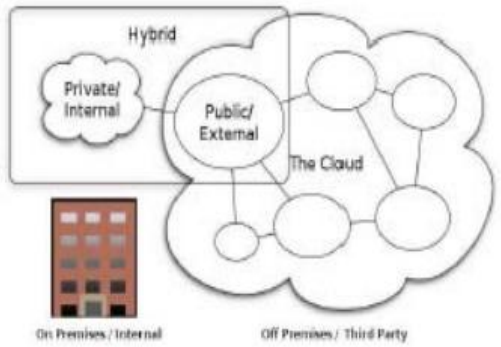

Fig. 4. Cloud Computing Deployment Model

1) Private Cloud

Cloud infrastructure functions and operates the company's private cloud data center. Many cloud infrastructure customers (e.g. corporate units) have a single organization's exclusive provision. In a private cloud, the customer and vendors' relationship is much easier to define because the technology of the same company is managed and controlled. Security threats are also more readily identifiable.

2) Public Cloud

The true representation of cloud hosting is where the Service Level Agreement (SLA) between users and providers is solid to protect your confidentiality. Accessible public and corporate access are offered in this cloud infrastructure. The public cloud environment is operated by corporations, researchers, and governmental agencies. This means that many companies will own a public cloud and run it. It poses several problems because it is difficult to protect them against attacks. After all, we don't know where or who controls the resources.

3) Community Cloud

The cloud infrastructure group of organizations that expressed issues made special arrangements for exclusive use (missions, security requirements, policy, and enforcement considerations). It is possessed, accomplished, and worked on campus or off-campuses by community groups, third parties, or any association of organizations. In short, many entities share a community cloud and manage it. [39]. This also decreases public cloud protection risk and reduces private cloud costs.

4) Hybrid Cloud

It's two or more wolves in combination (public, private, community). Typically, standardized and proprietary

technology blends data and applications. The benefits of various cloud deployment models are provided by hybrid cloud. Yet it's centralized and better than the public cloud by using the internet to access the organizations. [7].

A. Cloud Delivery Models

Infrastructure as a service (IaaS), Application as a Service (PaaS) & Software as a Service are the three models for cloud delivery proposed by and improved for the industry (SaaS) [8].

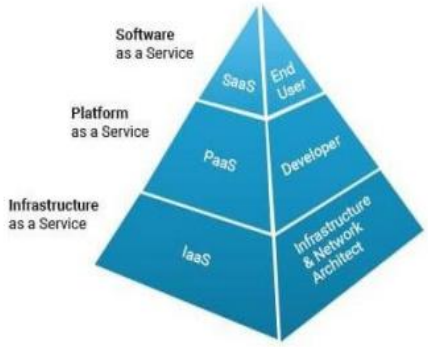

Fig. 4. Cloud Computing Services

1) Infrastructure as a service (IaaS)

Service Infrastructure is a multi-tenant cloud layer in which the allocated services of the cloud service provider are distributed only to contractual clients at a price. This usually means that the cloud user is provided with the operating system. The responsibility of the cloud service provider ends with the OS.

2) Platform as a service (PaaS)

(PaaS) is the most common distribution service where not only operating systems but development stacks are supported by the cloud provider. Providers in this model have a common practice of offering database and server maintenance along with advanced services. As in IaaS, PaaS is a user-friendly model.

3) Software as a service (SaaS)

A cloud provider, offering end-to-end services, including licensation, applications, networking, etc, is hosting the full application stack as a Service Software model., The cloud user usually uses the services in a web service or a software-based architecture in the data and business processes [8].

Table 1. Comparison of Private, Public and Hybrid cloud [9]

Attribute	Private Cloud	Public Cloud	Hybrid Cloud
Reliability	High	Medium	Medium to high
Scalability	Limited	Very high	Very high
Cost of use	High cost of initial set up	Pay-as-use basis	Pay-as-use basis
Data & Application Integration	Easy	Easy	Changing cloud systems is challenging.
Security	High	Low	Moderate
System Management	Easier	Easier	Compared to public and private cloud, this is challenging
Portability	Easy	Easy	Difficult
Data Security Solutions	Encryption of data on private servers	Better encryption techniques (authentication of user by the cloud provider)	Sensitive data should not be preserved in the public cloud while encrypting personal details
Performance	Very good	Low to medium	Good
Workload	Mission-critical workload with security concerns	Normal workload	Highly dynamic or changeable
Space Required	Very large	Very low	Medium

VI. Security Issues

The high scalability of the cloud computing framework removing Cloud service providers' need to schedule hardware supplies well ahead will deliver endless computing services at demand. Many firms, including Google, Amazon, and Microsoft, are driving the growth of the cloud computing system and growing customer support. In this paper, we discuss the security problem of a diversity of companies' existing cloud computing systems. . As Cloud Computing relates to applications provided as internet services and the infrastructure that delivers those services (e.g. hardware and system software in data centers).

Due to the investigation protection problem currently faced by businesses, the application of cloud computing systems to consumers is therefore not sufficient. More considerations should also be taken into account in the fields of security such as accessibility, privacy, data integrity, control, and audit, etc. These are [10]:

A. Availability

The aim is to ensure that its users can access cloud computing systems (including their applications and their infrastructures) anytime and anywhere. A Cloud computing system, as a web-based system, allows users to access the system from anywhere (such as applications, services). For all cloud computing systems this is valid (e.g., SaaS, PaaS, IaaS, etc.). The accessibility of the cloud infrastructure or the applications hosted in it is primarily improved by two techniques such as hardening and redundancy.

B. *Confidentiality*

It means that user data in cloud systems are kept secret. The privacy of cloud computing providers is thoroughly supported by two simple approaches (such as physical separation and cryptography).

C. *Data Integrity*

In the cloud environment, knowledge privacy is safeguarded (i.e., not lost or modified by unauthorized users). Data is a fundamental challenge for maintaining data integrity since it is the foundation for cloud storage services, such as data for a service, software as a service.

D. *Data Locations*

If operators use it, they're perhaps not sure precisely where their information is hosted and where it's storedService providers need to be asked if they can manage, especially arbitration, to store and change data. They will make a reasonable effort to satisfy local privacy standards based on their customers.

E. *Data Recovery*

It is characterized as the recovery of missing, corrupted, or accidental data.

F. *Trust Issue*

In cloud computing, trust is also a big problem. Trust may be between human beings to machines, machines to humans, human beings, and human beings. Trust revolves around confidence and trust [10].

VII. Importance of Security in Cloud Computing

There are several problems with safety due to the strength, extent, and ease of use of the CC. Although CC is a modern, intuitive way to access applications and make them easy to use, it still faces several challenges. Some problems are discovered by non-exhaustive searches in this area. These include SLA, what to migrate, security, etc. These include service level agreements. Cloud Computing has an automated upgrade function that will allow the user to be responded to by a single change by an administrator. This publicity leads to the conclusion that a large number of users immediately notice any software failures, which is a major safety risk for any company.

Many researchers also agree that safety is an enormous concern for cloud computing. A survey carried out by IDC on 263 managers shows that safety is one of the CC problems. Although an enterprise boasts high-quality security and does not regularly update its security policy, it will soon be prone to security breaches. [11].

VIII. Data Security in Cloud Computing

Data security is considered a significant research subject in cloud computing, according to an interview in previous papers. The most critical concerns related to data protection are information security, data availability, privacy protection, data accountability, and data control. Data security can be ensured through various aspects, such as access control and encryption. The supplier must ensure that its supply system is secure and customer data safe. On the client-side, they should examine the data-related security measures that the cloud provider provides for the security technique. The cloud provider selects the techniques provided. There are techniques of different encryption methods such as AES, RSA, etc. When data in the cloud is stored, the unauthorized user threatens the data. Control mechanisms should not be ignored to prevent this access. To avoid critical data threats, Cloud Provider should provide an authenticity checking method. Different authentication systems like SSL, PKI, and CHAP are in place to verify user Authenticity. Authorization can be given after authentication that restricts the user's access.

IX. Cloud Computing Security Standards

Security standards define structures and techniques for the implementation of a security program. Some specific steps to maintain a secure environment are carried out by using cloud-related activities according to these standards. To ensure privacy and security. Cloud is based on a concept called "Defense at Depth." The idea has defense layers. This allows overlapping strategies to protect if one of the systems fails so there is no weak point. Endpoints typically have the protection strategy, where access is monitored by the user. [12].

A. *Security Assertion Markup Language (SAML)*

SAML is essentially used for the safe contact of online partners in business deals. It is an XML based standard used by the partners for authentication. Three roles are specified by SAML: principal (user), the service provider (SP), an identity provider (IDP). For authorization and authentication in XML format defining user attributes, SAML provides queries and answers. The requester is a security detail web database.

B. *Open Authentication (OAuth)*

It is a way to communicate with protected data. It is used mainly for providing developer data access. Users can give developers and customers access to information without their identity being shared. OAuth does not protect by itself, it relies on other protocols such as SSL for safety.

C. *OpenID*

OpenID is a one-sign-on (SSO) solution. It is a mutual login procedure, which permits users to log in once and then use all the systems involved. It does not have a single user authentication authorization.

D. *SSL/TLS*

TLS is used for secure TCP/IP communication. TLS essentially operates in three stages: In the first stage, customer discussions are conducted to classify the ciphers used. The second step is used to authenticate the key exchange algorithm. These key exchange algorithms are algorithms of public interest. Enjoying and cipher encryption are used in the final and third stages. [12].

X. Practices for Cloud Security

A. *Secure Access*

Using the customer web browser, users typically access the

cloud. Make sure that the browsers are updated and secure from exploiting the browser. Data can be avoided to some degree from being threatened by doing this.

B. Backups and restoration

The service provider should have a proper process for the customer to provide cloud-based resources and data backups. Some of its offerings include Amazon S3 and Amazon Dynamo DB.

C. Data integrity

Limiting the field of resource usage for users to ensure data integrity. This will avoid data change and thus protect data integrity. If data confidentiality is enforced, backup data is retrieved by backup providers.

D. Encryption of Data

Cryption of data ensures data security. Crypt, before data is transferred to the cloud, should be performed. If an undesirable operator tries to access the critical data, it is much harder for the unwanted user to access the critical data.

E. Evaluation

Evaluate their importance and risk-based applications, business processes, and information and build the cloud with safeguards and tools to protect the cloud. [13].

XI. Literature Review

P. Sirohi and A. Agarwal (2015) The proposed system emphasizes the encryption and decryption technique which ensures data security for the cloud operator. The solution proposed only speaks of increased safety but not of efficiency. The solution includes also the operation of a virtual forensic machine, malware detection, and real-time monitoring of devices. This paper also contains an inquiry into various security risks and threats. A data protection architecture also offers accountability, to decrease risks to data security in the cloud world, to both cloud service providers and cloud users. [14].

S. P. Carolin and M. Somasundaram (2016) Proposed Virtual machine and Data Recovery for the creation and retrieval of lost data from cloud security data servers and agents. The virtualization is managed by a Cloud Manager and the fault is addressed. To improve data that initially divides the population into n parts, the erasure code algorithm is used. A semi-confident third party can be detected with an agent using artificial intelligence techniques and Malware modifications to data stored in data centers. Java Agent Development Framework (JADE) offers an agent development tool that promotes interagent communication and enables system computing services. The JAVA programming framework is intended for the recovery of data loss as a gateway or firewall. [15].

A. Arora et al. (2017) The proposed Hybrid Cryptographic System (HCS) integrates secure cloud surroundings that have the advantages of symmetric and asymmetric encryption. The paper emphases the development of a stable cloud environment in which multiple authentication and various hashing and encryption levels can be used. With the CloudSim simulator, the proposed framework and the algorithm are used. To this end, we present the working and the simulated effects of our proposed method. [16].

A. Sun et al. (2018) Offer a measurable security assessment framework for various clouds accessible via a consistent API. The assessment framework comprises a security scanning engine, security recuperation engine, quantifiable security assessment model, view display module, and so on. The safety assessment model consists of a collection of assessment components, covering various fields such as computation, storage, the network, maintenance, protection of applications, and so on. We assess our G-Cloud platform for various cloud users. It determines the dynamic security scanning score for one or more clouds, with visual graphs and directed operators to adjust configurations, enhance operational vulnerabilities, and fix vulnerabilities to enhance cloud security [17].

S. R. Rathi and V. K. Kolekar (2018) Focuses on a range of criteria such as data protection, individuality management (user uniqueness), authorization, authentication, and cloud security virtualization. Users of the cloud will use the model here to evaluate different cloud services. Finding faithful service is simple for the customer. This model also allows the cloud service provider to recognize vulnerabilities and develop services. This is a security assessment framework for various cloud services used by Cloud Service providers. [18].

Y. Sharma et al. (2019) [Base Paper] This paper discusses the significance of the use of several crypting techniques of data security and privacy protection. Also, it is necessary to apply successful encryption methods to improve data protection, which nature of attacks and problems may occur that can corrupt data. [19].

J. Shen et al. (2019) Present a new block design key contract protocol that supports many parties and, by its block design structure, can flexibly increase the number of cloud participants. We present general formulas to produce the popular IC conference key for several participants based on our proposed model for group data sharing. Notice that the machine complexity of the Proposed Protocol increases linearly with the number of people involved, by taking advantage of the (v, k + 1, 1) block architecture and substantially decreases communication complexity. The fault tolerance property of our protocol also helps cloud-based community data sharing to resist key attacks similar to Yi's protocol. [20].

R. L. Paikrao and V. H. Patil (2018) Has attempted to examine and evaluate many security vulnerabilities due to different aspects of cloud computing. We follow up on the ideas of different researchers and classify them largely as problems identified by CSA, problems identified because of their site of knowledge, networking problems and, more specifically, the challenges presented by virtualization vulnerabilities. In terms of VM control, hypervisor deficiencies are of concern. Virtualization Risk Protection as a service model is proposed. [21].

XII. Conclusion

To sum up, the cloud offers various services both to computer users and large and small businesses. It provides a

wider variety of computers and makes it easier to use simply by getting access via any connection to the internet. But it still has a vulnerable field to focus on, despite that, Protection is considered the weakest field through surveys. In this paper, we appear to define cloud computing, cloud computing services, the concept, styles, and properties of cloud computing, the ready-made model, and the challenges. In cloud computing, there are many challenges. Appropriateness, performance, service-level agreement, the confidentiality of information, and measures are examples of problems in cloud computing. Although cloud storage poses numerous security problems, we have addressed some of these and strategies in this document to help avoid them, they can also be used to keep connectivity safe and address security issues. Some standards can also be used for safe cloud networking and protection as many devices communicate there and conduct operations. There are also common standards.

REFERENCES

[1] Singh, S., Jeong, Y.-S., & Park, J. H. (2016), "A survey on cloud computing security: Issues, threats, and solutions", Journal of Network and Computer Applications, 75, 200–222, doi:10.1016/j.jnca.2016.09.002.

[2] Amandeep Verma and Sakshi Kaushal, "Cloud Computing Security Issues and Challenges: A Survey", International Conference on Advances in Computing and Communications, pp 445-454.

[3] Sun, Y., Zhang, J., Xiong, Y., & Zhu, G. (2014). Data Security and Privacy in Cloud Computing. International Journal of Distributed Sensor Networks, 10(7), 190903. doi:10.1155/2014/190903.

[4] Sized Amin Soof et al., "A Review on Data Security in Cloud Computing", International Journal of Computer Applications (0975 – 8887) Volume 94 – No 5, May 2014.

[5] N. Dhivya and Dr.S.Vijayalakshmi, "A Survey Paper on Cloud Computing", International Journal of Advanced Research in Science and Engineering, Vol. 06, Issue 12, December 2017.

[6] Palvinder Singh and Er. Anurag Jain, "Survey Paper on Cloud Computing", International Journal of Innovations in Engineering and Technology (IJIET), April 2014.

[7] Saurabh Singh et al., "A Survey on Cloud Computing Security: Issues, Threats, and Solutions", Journal of Network and Computer Applications, DOI: http://dx.doi.org/10.1016/j.jnca.2016.09.002.

[8] Gururaj Ramachandra et al., "A Comprehensive Survey on Security in Cloud Computing", The 3rd International Workshop on Cyber Security and Digital Investigation (CSDI 2017).

[9] K. Sharmila, "A Review Paper on Cloud Computing Models", International Conference on Artificial Intelligence and Machine learning.

[10] Manisha Thakur and Dr. Neeru Bhardwaj, "A Review Paper on Cloud Computing & Security Issue", International Journal of Computer Science and Mobile Computing, IJCSMC, Vol. 8, Issue. 5, May 2019, pg.23 – 3

[11] Gurjeet Singh, and Dr. Mohita Garg, "Data Security in Cloud Computing: A Review", International Journal of Computers & Technology, 17(2), Doi: 10.24297/ijct.v17i2.7551

[12] Garima Gupta et al., "A Survey on Cloud Security Issues and Techniques", International Journal on Computational Science & Applications, 4(1), DOI: 10.5121/ijcsa.2014.4112

[13] Jasleen Kaur et al., "Survey Paper on Basics of Cloud Computing and Data Security", International Journal of Computer Science Trends and Technology (IJCST) – Volume 2 Issue 3, May-Jun 2014.

[14] P. Sirohi and A. Agarwal, "Cloud computing data storage security framework relating to data integrity, privacy, and trust," 2015 1st International Conference on Next Generation Computing Technologies (NGCT), Dehradun, 2015, pp. 115-118, DOI: 10.1109/NGCT.2015.7375094.

[15] S. P. Carolin and M. Somasundaram, "Data loss protection and data security using agents for a cloud environment," 2016 International Conference on Computing Technologies and Intelligent Data Engineering (ICCTIDE'16), Kovilpatti, 2016, pp. 1-5, DOI: 10.1109/ICCTIDE.2016.7725349.

[16] A. Arora, A. Khanna, A. Rastogi, and A. Agarwal, "Cloud security ecosystem for data security and privacy," 2017 7th International Conference on Cloud Computing, Data Science & Engineering - Confluence, Noida, 2017, pp. 288-292, DOI: 10.1109/CONFLUENCE.2017.7943164.

[17] A. Sun, G. Gao, T. Ji and X. Tu, "One Quantifiable Security Evaluation Model for Cloud Computing Platform," 2018 Sixth International Conference on Advanced Cloud and Big Data (CBD), Lanzhou, 2018, pp. 197-201, doi: 10.1109/CBD.2018.00043.

[18] S. R. Rathi and V. K. Kolekar, "Trust Model for Computing Security of Cloud," 2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA), Pune, India, 2018, pp. 1-5, doi: 10.1109/ICCUBEA.2018.8697881.

[19] Y. Sharma, H. Gupta and S. K. Khatri, "A Security Model for the Enhancement of Data Privacy in Cloud Computing," 2019 Amity International Conference on Artificial Intelligence (AICAI), Dubai, United Arab Emirates, 2019, pp. 898-902, doi: 10.1109/AICAI.2019.8701398.

[20] J. Shen, T. Zhou, D. He, Y. Zhang, X. Sun and Y. Xiang, "Block Design-Based Key Agreement for Group Data Sharing in Cloud Computing," in IEEE Transactions on Dependable and Secure Computing, vol. 16, no. 6, pp. 996-1010, 1 Nov.-Dec. 2019, doi: 10.1109/TDSC.2017.2725953.

[21] R. L. Paikrao and V. H. Patil, "Security as a Service Model for Virtualization Vulnerabilities in Cloud Computing," 2018 International Conference on Advances in Communication and Computing Technology (ICACCT), Sangamner, 2018, pp. 559-562, doi: 10.1109/ICACCT.2018.8529573.