ISSN: 2366-1313

Security Challenges and Issues in Cloud Computing

Dr. Jaibir Singh

Associate Professor, OPJS University, Churu

Abstract: *Using cloud computing, one may dynamically increase capacity or add capabilities without spending money on new equipment, hiring new staff, or approving new software. Despite all the hoopla around the cloud, commercial clients are still cautious to move their operations there. One of the key issues halting the growth of cloud computing is security, and issues with data security and privacy are still plaguing the business. When used in a cloud context, the cloud architecture compromises the security of the current technologies. Users of cloud services must be cautious and aware of the hazards of data breaches in this new environment. The security of data in cloud computing is covered in this essay. It examines security issues connected to cloud data and its associated elements..*

Keywords: *Cloud computing, Data security, Data protection, Risks and threats, Encryption*.

I. INTRODUCTION

Recent developments in cloud computing are not being completely tapped. A "network solution to provide cheap, reliable, clean and easy access to IT assets" [1] is one of several definitions, but it is the only one. Cloud computing is seen as a service, not an application. For the user who gives up, cloud computing's service-oriented structure offers flexibility and greater overall performance while lowering infrastructure and ownership costs. [2]. The security and privacy of cloud data editing is a significant problem. For cloud service providers, maintaining information security, confidentiality, and integrity might be essential. Depending on the form, quality, and length of the data, several service providers use distinctive standards and processes for this objective.

Data sharing across multiple businesses is one of the benefits of cloud computing. This benefit poses a danger to the data itself, however. To prevent the possible risks of facts, the repository of information must be protected. The choice of whether to utilise a third-party cloud operator or build an internal organisational cloud is crucial when utilising the cloud to store data. Records like highly private national security material or knowledge about upcoming products, among many others, are sometimes too sensitive to be kept on

ISSN: 2366-1313

the public cloud. When this kind of material is made public, the repercussions might be disastrous since it can be incredibly sensitive. In these circumstances, storing information in an internal organisational cloud is mostly suitable. Through the enforcement of local information use coverage, this strategy may aid in data protection. Although many agencies lack the necessary certification to provide all necessary levels of protection for sensitive data, this still does not ensure total security and confidentiality of data. This article examines the statistical security methods used at some point in the field to protect and guarantee data in the Cloud. With the assistance of several service providers, analyse possible risks to the data in the Cloud and their solutions to safeguard information.

Three different service delivery methods are used by cloud computing to provide customers a unique experience. SaaS, PaaS, and IaaS are the three distribution methods, and they give customers software, utility platforms, and infrastructure resources. A certain degree of protection is also imposed on the cloud environment by these service models. All cloud services are based on an IaaS basis, with PaaS and SaaS built on top of it. Issues and hazards related to data security are inherited, just like talents. Regarding built-in features, complexity vs scalability, and security, each paradigm offers considerable economic prospects. Users are more in charge of enforcing and managing security skills if the cloud service provider's issuer only deals with security at the base of the security architecture [3].

Businesses across all sectors are eager to start using cloud computing, according to a new poll by the Cloud Security Alliance (CSA) and IEEE. Security is still necessary to embrace the cloud and comply with regulatory requirements. Additionally, it notes that cloud computing is influencing IT's future, but that its growth is being severely hampered by the absence of a compliant environment. The security and privacy concerns of non-sensitive packages must be addressed by organisations who employ cloud computing as a supplier of infrastructure. However, since the "cloud" offers specialised services like SaaS, PaaS, and IaaS, it is difficult, if not impossible, to guarantee the security of corporate data there. Every operator has unique security concerns.

ISSN: 2366-1313

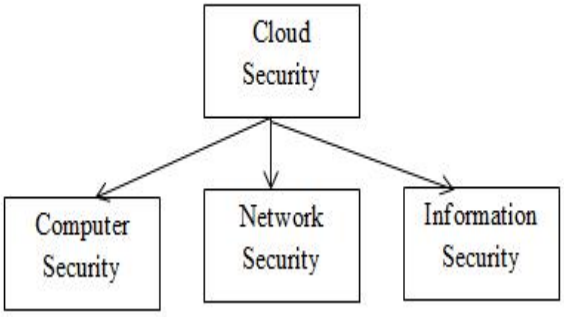

Fig.1 Scopes of Cloud Computing Security

This paper specializes in understanding the regular aspects of cloud security. To provide a more general view of cloud security, we show a high structure of the security dimensions of cloud computing protection in Figure 1. As shown in the picture, there are three important aspects: computer security, community security, and registry security. These three aspects will guide the form of this survey. The most effective survey selects general and representative factors for the reviews in each measurement due to page restrictions.

II. REVIEW OF LITERATURE

Many researchers were provided different security techniques to the cloud computing. Some of the implementations are described below.

Giri et al.[2019] The study concluded that cloud computing is important for Nepal's available data, regulations, and garage format. Nepal is below the developed U.S.

Yes. At the same time, you don't have enough technical knowledge, financial resources, large digital distribution, and professional human resources, so the security issue is real. Storage, virtualization, and networking are top security concerns in cloud computing. Virtualization is one of the key issues for cloud users and providers, allowing some users to share physical servers. Cloud networks are particularly vulnerable to attacks, even when talking to remote digital systems is their primary purpose. It is clear that Nepal is going through many difficult situations in cloud computing: security, storage, data center operation, cost model, charging model, service level agreement, locality, integrity, access, segregation, breaches, and privacy. Nepal is one of the developing United States. It needs to start using its servers and satellites for verbal exchange and the data center or record financial institution.

Santoso et al. [2018] A Cloud drive is an operator that provides cloud log storage. As the rapid globalization of cloud driving continues, there are constant concerns about trust, privacy, and security over how private user data and data can be viewed by other users or misused by the Cloud Pressure Service. Can This test provide empirical evidence on factors that affect users' cloud pressure identification using

ISSN: 2366-1313

seven constructive variables: trust, perceived risk, ease of use, perceived usefulness, security, and behavior. There are intentions and thematic standards. Collected data from 294 respondents with the help of an online questionnaire. Evaluating the information used became structural equation modeling (SEM) analysis. This study shows that what influence the purpose of using cloud power are belief, perceived randomness, and thematic routine.

Ahmed et al. [2018] The rise of cloud computing and the consequent changes in infrastructure and working methods leave no doubt that top-notch computing systems can become increasingly vulnerable to security issues. Therefore, in the context of the security framework, one must recognize issues related to the exploitation of hard or soft network elements in the cloud fabric. To be relevant to any cloud architecture, this type of framework wants to play its part in the operational context of cloud computing. This framework is presented as a classification of security risks specifically for the cloud computing environment.

Kumar et al. [2018] This paper also described cloud computing models, including deployment and supplier delivery models. Records were crucial in any business or cloud computing; data leaks or corruption could shake people's self-confidence and disrupt the business. Many organizations use cloud computing directly or indirectly. If there is any information leakage in cloud computing, then as a way to influence the business of cloud computing and organization. It was an important reason for cloud computing organizations to pay more attention to data protection.

Randeep Kaur et al.[2015] This paper addressed strategies to overcome cloud computing security and data privacy issues. Before looking at the security issues, provide a quick dialogue below on the definition of cloud computing, then explores the cloud security issues and the hassles of using a cloud provider. Cloud Explaining key pixel patterns and image steganography techniques to overcome the problem of information security.

Hemalatha et al.[2014] Cloud computing is a collection of IT services provided to the buyer primarily on a lease basis. Although many security issues have been addressed, some have gone unnoticed, and many algorithms have been proposed for security issues. This paper provided an overview of cloud computing technology, key features, classification, shipping methods, and various encryption methods. A comparative study of various encryption strategies was used to maintain

ISSN: 2366-1313

confidentiality within the cloud. Finally, the key issues of statistical security in cloud computing are discussed.

III. RISKS AND SECURITY CONCERNS IN CLOUD COMPUTING

Several risks and security problems are linked with cloud computing and its data. However, this investigation will examine the virtualization, storage in the public cloud, and multi-tenancy, which are connected to the data security in cloud computing.

Virtualization

Virtualization is a technique in which a fully serviceable operating system image is captured in another operating system to utilize the resources of the real operating system fully. A special feature known as a hypervisor is required for a guest operating device to run as a virtual system on multiple operating devices.

Virtualization is a key element of cloud computing that facilitates the delivery of the core values of cloud computing. However, virtualization poses some risks to data in cloud computing. One potential danger is compromising with a hypervisor. Hypervisor number one can be a target if you have too much inclination. If a hypervisor is compromised, the whole device can be compromised, and so is the information.

One way to work on these issues is to plan for the use of virtualization. Use resources with caution and thoroughly verify facts before resources are distributed.

Storage in Public Cloud

Data storage in the public cloud is another security challenge in cloud computing. Clouds typically implement a central garage hub, an attractive target for hackers. Storage assets are complex structures that can be incorporated into hardware and software implementation and may be intended to generalize facts if there is a minor breach within the public cloud [10]. It is always recommended to have a non-public cloud, if possible, for highly sensitive information to avoid such risks.

Multi-tenancy

Shared access or multi-tenancy is also considered one of the most important threats to statistics in cloud computing. Because multiple users use the same shared computing resources such as CPU, storage, and memory. This is now very dangerous not only for one user but also for multiple clients. There is a constant risk of accidentally leaking personal information to other users in such cases. The exploitation of multiple users can be

ISSN: 2366-1313

particularly volatile because a bug in the system could allow another user or hacker access to all other data.

IV. DATA SECURITY IN CLOUD COMPUTING

Data security in cloud computing involves more than data encryption. Requirements for data security depend upon on the three service models SaaS, PaaS, and IaaS.

1) Software-as-a-Service (SaaS)

SaaS is also known as an on-demand service that allows users to use applications hosted on a cloud server and stored on the Internet. This may include online office suites and email applications. Instead of buying new software, consumers can subscribe to fully Internet-based software services to fulfill their business aspirations at a lower cost. Buyers rely on carriers for safety. SaaS no longer requires users to have unique hardware or software. But it requires a perpetual internet connection.

2) Platform-as-a-service (PaaS)

PaaS, the bottom layer of SaaS, allows developers to efficiently write and extend SaaS packages and install them on the PaaS layer. The PaaS software program fully supports the life cycle and is a cost-effective alternative for developers, allowing them to focus on building and running packages rather than overseeing infrastructure. Service companies are responsible for building and maintaining infrastructure for builders.

3) Infrastructure-as-a-service (IaaS)

IaaS, the bottom layer, provides the infrastructure for the upper layers. IaaS includes network hardware, servers, framework (OS), and storage. It allows users to use the full resources without purchasing a physical system. IaaS is also a fast, cost-effective option for dealing with workloads without the need to purchase or control infrastructure. However, since it relies heavily on Internet connectivity, availability is a major concern.

There are a wide variety of security issues related to cloud computing. However, those issues fall into two broad categories: the security issues facing cloud providers and the security issues they face with their customers. Here, the supplier needs to ensure that their infrastructure is comfortable and that their buyer's data and programs are covered at the same time as the customer must ensure that the company compiles its statistics. Adopts proper safety features for safety. Security has always been a major concern for IT executives regarding cloud adoption. However, cloud computing combine's

ISSN: 2366-1313

technology, operating systems, storage, networking, and virtualization, each with inherent security issues. (For example, purely browser-based attacks, denial of service, and community intervention transmit threats to cloud computing.) Cloud protection architecture is more effective if the best security deployments are in the region. Must identify problems to adapt an effective cloud security structure to security management. Security control solves these problems with security control. These controls are placed in the area to protect any vulnerability in the device and minimize the attack's impact. Although there are several types of controls at the back of cloud security architecture, they can usually be found in one of the following categories:

Cloud Computing Security Requirements

Privacy requires the unauthorized disclosure of CC providers' user data. Cloud providers charge users to ensure privacy. In CC, the focus is on verifying cloud sources (for example, each user requires a username and password). Furthermore, availability is the ability of the user to use the system as intended. The availability of a sponsor can be guaranteed as one of the terms of the agreement. A company can also host large capacity and exceptional infrastructure to guarantee availability. Accountability involves checking the client's various games in Log Clouds. Accountability is achieved by verifying the records that all users use (and which are recorded in different places in the data cloud). Security issues in supplier models.

Classification of Cloud Security Issues

CC contains many categories, each of which has many security concerns. The security issues occur throughout CC hardware, software, and communication. Data defects in cryptographic methods can cause security issues in data centers or in communication. These issues can also come from the customer if the authentication policy is weak.

Current security solutions

Various researches are being done in the field of cloud security. Various companies and corporations are interested in developing fashion and security responses for the cloud. Cloud Security Alliance (CSA) Cloud Record Assurance ("Cloud Security Alliance (CSA) - world-class security." Exercises for Cloud Computing ", 2009 (Cloud Security Alliance, 2010a, 2010b). Cloud Standards Website Collecting and integrating data on cloud-related needs that are being improved with the help of agencies. The latest grid forum publishes archives containing details and

ISSN: 2366-1313

statistics on security and infrastructure for grid computing developers and researchers (OWASP, 2010) , 2010).

V. SECURITY CHALLENGES

Cloud computing promises to help businesses and their IT departments provide more vibrant, green, and new, cost-effective services that allow their organizations to thrive. But the promise of the cloud cannot be fulfilled unless IT experts become more confident about the safety and security of the cloud. We recognize that with the security of cloud computing, IT concerns are critical to the commercial adoption of the cloud. But before the IT industry can address these concerns, more expertise is needed.

Many security and privacy threats, including malware or any malicious internal threat, appear everywhere in today's record technology scenario and are addressed as part of a broader national and global cyber security plan. Need the security challenges facing organizations that want to use cloud services are no different from traditional security issues and threats. The same internal and external threats are a gift, and proper mitigation and destructive control regulations are needed to protect privacy and security.

To learn about the top security risks in cloud computing, the Cloud Security Alliance surveyed industry professionals to gather expert opinions on the best vulnerabilities within cloud computing. In this latest peak version of the list, experts have identified the following nine major threats to cloud protection (classification in order of magnitude).

Data Breaches

A data breach is a security incident in which an unauthorized man or woman copies, transmits, analyzes, steals, or uses confidential, confidential, or proprietary records. The issuer of the cloud service provider must ensure that the security level of the verification and authorization process is the first class to ensure some security of information. If a multi-tenant cloud service database is not well designed, an error in a client's application may allow an attacker to access that user's data, and every other can also access client statistics.

Data Loss: For both consumers and agencies, the potential for the complete loss of information is alarming. Of course, could lose the data stored inside the cloud for reasons other than malicious attacks. Any unintentional deletion, or worse, a physical disaster with fire or earthquake through the issuer's use of the cloud service, resulting in permanent loss of customer data unless the issuer takes appropriate action. Do Suitable for data

ISSN: 2366-1313

backup. Furthermore, the burden of preventing record losses does not fall entirely on the company's shoulders.

Account Hijacking: Account hijacking is not a new threat to computing. It is a form of identity theft where the attacker uses the stolen account information to carry out malicious or unauthorized activities. Account hijacking is usually carried out through phishing, sending fake emails to someone, guessing passwords, or other hacking strategies. In many cases, an email account is related to one's social networks and financial networks, and many others. And with the help of account duplication, A hacker can gain access to these special records for illicit purposes.

Insecure APIs: Cloud service users access their records through some of the interfaces provided by the service providers. The security and availability of modern cloud services depend on the security of these basic APIs. These interfaces should be designed to defend against malicious and unintentional attempts to block policy from authentication and login to encryption and interest tracking management.

Denial of Service: Denial of service (DOS) attacks are nothing new and have been a thorn in the side of data center managers and IT staff for over a decade. With DOS, a hacker no longer wants to raid the entire infrastructure. Of course, they can choose the most useful resource depth application that the user is running in the cloud and use a simple low bandwidth attack to terminate the service.

Malicious Insiders: Cloud computing as a system is managed, controlled, and maintained by the administrators of the online website. By default, they have the key to dealing with all agency statistics, documentation, and privileged documents and resources. From time to time, these directors may leak important customer information or distribute the company's private or well-known financial information due to some organizations.

VI. DATA SECURITY USING ENCRYPTION

Encryption techniques and transit statistics can be specific for easy information. For example, encryption keys for data in transit may be faster, while they may keep keys longer for the rest of the record.

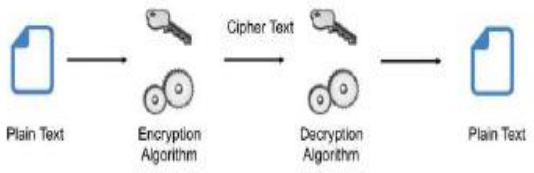

Fig.2 Basic Cryptography Process

In recent times, various cryptographic techniques have been used to encrypt

ISSN: 2366-1313

records. Cryptography extends the scope of data security to ensure the integrity, authenticity, and availability of content. In the simplest form of encryption, plain text is encrypted into cipher text content using the encryption key. The resulting cipher text content is decrypted using the decryption key, as shown in Fig.2.

To protect the data stored in the cloud and to ensure security for the clients, scientists have come up with the following four security techniques:

Homomorphic encryption:

An encryption scheme provides a unique way of calculating encrypted information, which is not possible with other encryption schemes. With this method, one can save files in the cloud in an encrypted format and perform any required calculation without cracking encrypted statistics.

Search-Based Encryption: This approach also uses homomorphic encryption as a basis. The search encryption method allows you to search the database for encrypted records with encrypted keywords. It ensures that the cloud never sees the facts and that the calculations are complete in statistics.

Proofs of storage: Proof of storage is a carrier-level agreement between CSPs and their users and guarantees that customer data stored on CSP's servers cannot be tampered with or used by CSP without the customer's consent. This ensures that can retain the data stored inside the cloud.

Server aided secure computation: This security approach allows servers and users to perform some computations on their encrypted data simultaneously without disclosing the contents of the original data. Communication events and the cloud are completely blind to the calculations and final results.

VII. CONCLUSION

Cloud computing is one of the most attractive areas of today, at least partly because of its affordability and capability. Cloud computing is a paradigm shift in which computing is transferred from private computers or even individual agency utility servers to the "cloud" of computers. This paper discussed the risks and protection dangers to data in the cloud and summarized three types of security situations. Virtualization is analyzed to find out the threats generated by the hypervisor. Also, threats generated by Public cloud and multi-tenancy have been examined. One of the major problems of this paper was data security and its threats and solutions in cloud computing. The study provided an overview of risks and security concerns in cloud computing, data

ISSN: 2366-1313

security in cloud computing, security challenges, and cloud security using encryption.

REFERENCES

1. S Shakya and S. Giri, 2019, “Cloud computing and data security challenges: A nepal case,”, pp. 146–150.
2. Kusyanti A and N. Santoso, 2018, “Trust and security concerns of cloud storage: An indonesian technology acceptance,” IJACSA, pp. 453–458.
3. Ahmed M. and Litchfield A. T, 2018, “Taxonomy for identification of security issues in cloud computing environments,” JCIS, pp. 79–88.
4. Kumar P. R., and P. H. Raj, 2018, “Exploring data security issues and solutions in cloud computing,”, pp. 691–697, 2018.
5. Prasadu Peddi (2021), “Deeper Image Segmentation using Lloyd’s Algorithm”, ISSN: 2366-1313, Vol 5, issue 2, pp:22-34.
6. A. Jenis and N. Hemalatha, 2014, “A comparative analysis of encryption techniques and data security issues in cloud computing,” IJCA, vol. 96, no. 16, pp. 1–6.
7. Joshi J. B. D and Ahn G. J, 2010, "Security and privacy challenges in cloud computing environments," IEEE Security and Privacy, Vol. 8, No. 6, 2010, pp. 24-31.
8. E. Mohamed, “Enhanced data security model for cloud computing,” Informatics Syst. (INFOS), 2012 8th Int. Conf., pp. 12–17, 2012.
9. Winkler V. J, “Securing the Cloud,” Cloud Comput. Secur. Tech. tactics. Elsevier., 2011.
10. J. Walters, and Wills B, 2014, “Security Challenges in Cloud Storage,” pp. 1–6.