Global Scientific JOURNALS
GSJ: Volume 9, Issue 11, November 2021, Online: ISSN 2320-9186
www.globalscientificjournal.com

A Survey of data Security in Cloud Computing

Sadia Kousar[1], Hafsa Bashir[2], Hassan Raza[3], Tayyba Khalid[4]
Department of Computer Science & Information Technology
University of Sialkot, Sialkot, Pakistan
[1]21201009-014@uskt.edu.pk [2]21201009-023@uskt.edu.pk
[3]21201009-025@uskt.edu.pk [4]21201009-034@uskt.edu.pk

***Abstract* - Major technological advancements have developed in the last decade that have the potential to improve daily life activities not just for businesses, but also for individuals. Cloud computing has made considerable advancements in its application and is now widely used in both the private and public sectors. Many companies and businesses have recently made it clear that they are moving their workloads to the cloud. Security, on the other hand, is a major issue for cloud computing services, which rely on Internet connections and are thus affected by a variety of attacks. Deny the reality that the security measures in place Security concerns about cloud computing are growing with each passing year. It is still a challenge. We did a survey study on in this paper. Different forms of attacks were addressed using cloud computing. possible threats to this new technology, as well as possible solutions/methodologies and available countermeasures against such attacks.**

Keywords*— *cloud computing, security, attacks, countermeasures, challenges.

I. INTRODUCTION

Cloud computing allows for a more practical model. Its low-cost attraction is attracting an increasing number of businesses and users to outsource their data to, and high-quality services to outsource their data to a server in the cloud Users and servers of the cloud, on either side, The cloud servers are in a distinct trusted domain than the cloud ability to govern and monitor the data that has been outsourced, as well as the exchange of information between users and servers to secure data privacy, storage, and transmission security, a variety of solutions have been investigated. To preserve data privacy and prevent unauthorized access, encrypting sensitive data is a logical solution, but it poses significant hurdles to optimal data utilization. Similarly, cloud servers should give similar services to data users, while maintaining data protection and search privacy. [1]

Cloud computing security is a crucial area of concern of information security that presents a significant challenge to cloud providers rapid use of technology Due to the fact that Cloud computing services are They are vulnerable since they rely on a Connection to the internet to a wide number of threats and other security risks have the potential to have serious consequences, such as DDoS (Distributed Denial of Service). Sync cookies, as well as limiting the number of users connected to the server through cloud technology, may be used as countermeasures to prevent DDoS and man-in-the-middle attacks (MITM). [2]

Cloud computing is providing share storage and computing resources to the companies and the organization. Instead of developing and operating own infrastructure using the services of Cloud Computing can reduced time and cost for the computation with flexible and secure infrastructure Consumers and companies can utilize cloud computing applications without installing them and access their personal files from any computer with internet connectivity. This technology makes it possible to centralize storage, memory, computation, and bandwidth for considerably more efficient computing. [3]

Cloud computing is related with several security risks. The problems are divided into two groups. To start, there is a level of security provided by cloud providers. Second, there are security concerns that their customers have. They entrust the supplier with their data and put it in the cloud. That is why cloud computing data security is required. To limit the risk, data security becomes a critical concern in cloud computing. Open, shared upload, and distributed environments are often related with these risks. [4]

The remainder of this paper divide into following sections. Section 2 outlet of cloud computing. Section 3 including background study, Section 4 is including data security issue in cloud computing. Section 5 methods for data security in cloud computing and Section 6 conclusion.

II. OUTLET OF CLOUD COMPUTING

According to the National Institute of Standards and Technology (NIST) “Data center for software control, on-demand process demand access to a shared of configurable (e.g., server, network, application, storage, and services) that can be faster configured and removed with reduced delay and or internet service provider interaction,” [2].

A. Architecture of cloud computing

Architecture of cloud computing divide into three service delivery models such as PaaS (Platform as a Services), SaaS (Software as a service), and IaaS (Infrastructure as a Service). [1] As seen in Figure 1, this architecture is built from the ground up.

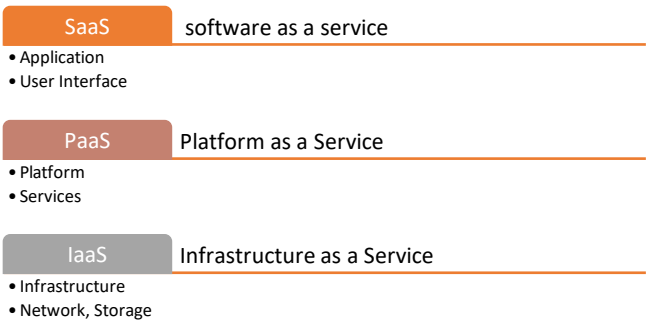

Figure 1 Cloud Service Model

i. SaaS (Software as a service)

SaaS (Software as a Service) is a type of software distribution in which a cloud service provider hosts programmers and makes them available to end users through the internet. In this case, an individual software vendor (ISV) might employ a third-party cloud service provider to host the application. The cloud provider may also be the software vendor in some situations, such as with Microsoft.

ii. PaaS (Platform as a Service)

Customers can provision, configure, run, and administer a customizable bundle that comprises a computing device and one or so more services without the complexities of handling the infrastructure involved with developing and delivering the application(s); and developers can construct software bundles.

IaaS (Infrastructure as a Service)

Infrastructure as a service (IaaS) is a browser service that offers high-level APIs for obtaining low-level communication network details including physical computing resources, geography, memory management, scalability, security, and backups, among many other things.

B. Cloud deployment models

Private, community, public, and hybrid deployment methods are available on the cloud platform for architectural solutions. [5] according to Figure 2.

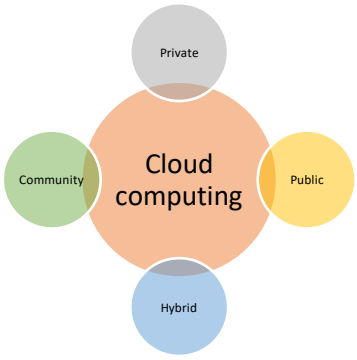

Figure 2 Cloud Deployment Models

i. public cloud

In a public cloud environment, software and hardware resources are shared publicly among multiple users. This environment is managed and monitored by a third-party public-cloud service provider; hence such clouds are ideal for non-sensitive data.

ii. private cloud

A private cloud is managed by a single company, and all of the cloud's systems and services are only available within that company's bounds. The corporation is responsible for all infrastructure management and maintenance; a private cloud is therefore more expensive than a public cloud, but it is more secure.

iii. hybrid cloud

A hybrid cloud is one that merge two or more types of cloud computing. (For example, a public–private cloud.) Because it exemplifies This type of deployment model is based on the characteristics of the clouds involved. It gives a lot of scalability and flexibility, as well as a lot of features choices for data distribution The management of a hybrid cloud centrally.

iv. Community cloud

In many ways, community clouds are comparable to public clouds; however, this cloud architecture is typically designed for specific individual, enterprises, or organizations with similar cloud needs. In a community cloud, the shared resources can be managed by either community members or a third-party service provider.

III. BACKGROUND STUDY

[9] (Thabit, 2021) in 2021 proposed the security of cloud computing is the main issue. in this paper the researcher proposed the idea of a cryptographic technique base on Feistel cipher. They used 16 bytes block and key size to encrypt and decrypt the data. The result enhances the security, improve the encryption and decryption process, and reduce computation cost. They named this technique as new lightweight cryptographic algorithm.

[10] (Qazi, 2020) in 2020 proposed a technique Elliptic Curve Cryptography for data security in cloud computing. Encryption, key generation, and decryption are all performed using ECC. Two layered methods are applied. The first is to divide the data into small chunks, and the second is to encrypt it with random encrypted curves. There are two steps, first step in cloud computing data storage is to divide the data into five data packets. Add four bits to these five data packets: 0000(1), 0001(2), 0010(3), 0011(4), 0100 (5). These 4-bit data can be applied to data packets at random. Second, in a cloud environment, Elliptic curves with various key sizes are used to encrypt data. As a result, the Elliptic curve's parameters are chosen from a list of pre-selected stable Curves. The proposed encryption key size is small to reduce computing power. This random collection of curves can boost data security in a variety of ways. The proposed approach much faster than RSA and the

level of security achieved with elliptic curves is far better to that of RSA.

[11] (Ogiela, 2020) Hybrid CAPTCHA codes were proposed in 2020 as a new approach for creating complex multilayer user authentication systems. The methods are based on the use of cognitive characteristics as well as expert knowledge. These protocols allow the user to proceed through various phases in which different degrees of knowledge and perceptual abilities may be assessed.

[12] (Sajay, 2019) in 2019 a solution has been presented that secures data in the cloud. To improve cloud security, this solution employs two algorithms: homographic and Blowfish encryption, which are applied by using the Python software tool and cryptographic techniques. There are two layers, The first layer uses a multilayer cryptography technique with homographic encryption, while the second layer uses blowfish encryption. The input text passes the first step of homographic encryption. The result of the encryption will then be acquired. The encryption result is then given to the second layer, the blowfish encryption layer. The encryption layer's result is obtained. This hybrid method also uses encryption techniques to provide a security strategy and better storage over cloud architecture.

[13] Singh, Abhishek, and Shilpi Sharma in 2019 proposed the mixture of AES and some parts of SHA-1 calculation is used to encrypt the data. And for decrypting the data that same calculation will be required. But for unauthorized access it is impossible for them to decode that information and made the information comprehensible. The suggested method divides the file into distinct pieces before attempting to encrypt and store it on numerous cloud servers. To avoid the risk of being attacked and losing the file. To prevent the possibility of various illegal activities, we must employ as many clouds as possible. The notion is that the logic should be broken down into components, which should then be distributed over various clouds. AES is based on the 'substitution-change organise' standard, in which the mix on each substitution and stage is quick in each bundle and piece of equipment. The usage of AES with SHA-1 will make the system enough strong to encrypt the data in this way that it can be mostly impossible for the unauthorized person to access the files on cloud and decode the information. The administration password will offer protection for the client and will be able to prevent any harmful behaviour. The user and the developer will go through the user-related checks as well as some validation to ensure that the data is protected from unwanted access. To login to the cloud the user must need to use the login credentials provided by the cloud service providers. And the system must check if the credentials are valid or not. In the new enhanced system, the system will be enough capable of providing the backup by using the different databases to prevent the data loss. Data can be stored offline in the proposed system.

[14] (Singh S. a., 2018) in 2018 proposed a new way to ensuring the privacy and integrity of data stored on cloud servers. The Advanced Encryption Standard (AES), a symmetric block cypher that performs all its computations on bytes is one such cryptographic technology. The number of rounds varies depending on the length of the key. Many firms apply AES because it is more secure than other algorithms and faster in both hardware and software. The suggested model was successfully implemented on a Windows PC with an Intel core i3 CPU TM-4005U running at 1.70 GHz and 4G memory, using the java crypto package, java crypto, ire v1.8.0, and PHP v5.4.38. When compared to other cryptographic methods, the AES algorithm has the shortest execution time for data encryption and decryption.

[15] (Kumar, Exploring data security issues and solutions in cloud computing, 2018) in the proposed cloud concerns in 2018 are mostly concerned with the security and privacy of information stored in the cloud. Heterogeneity, virtualization, resource sharing, multi-tenancy, mobile cloud computing, and service - Level agreements (SLA) are examples of cloud settings that make cloud security more susceptible. This article discusses information security concerns and how to deal with them.

[16] (Sukhodolskiy, 2017) For Internet security, a framework based on multi-agent systems was created. This approach's system architecture is made up of three different sorts of entities, each with their own set of functions. The first is in responsibility of intrusion prevention; the second oversees message encryption / decryption; and the third is a hybrid of the first two. Although this method has resulted in a helpful security system, it fails to solve certain critical concerns such as authentication, authorisation, digital signatures, and verification security services. Balakrishnan et al. [worked on the challenge of assuring data storage integrity and security in Cloud Computing]. Cloud security is done by signing data blocks before transferring them to the cloud. They signed with the BLS algorithm, that is more secure than other methods. They established an effective third-party inspector on behalf of the cloud client to check the reliability of the evidence kept in the cloud and audit user's outsourcing data as needed to ensure the accuracy of data. To accomplish privacy-preserving public auditing system, they used a public key based on homomorphic authenticator with random masking. They employed the bilinear aggregate signature approach to do batch auditing, which entails performing several auditing jobs at the same time. Batch auditing cuts down on computation time. Because cloud data is utilised by so many businesses, data alteration is unavoidable. The new approach also allows for safe and fast dynamic data block operations such as data update, deletion, and add. They investigated the Reed Solomon approach, which is an effective error correcting procedure that assures data accuracy.

[17] Administrative accounts must be used solely for system administration operations in organisations that use cloud computing. For their administrative and non-administrative accounts, administrators must use distinct passwords. Each user having administrator capabilities on diverse devices such as laptops, desktops, and servers must be validated by a senior executive using automated methods. All administrator passwords must be complicated, containing a combination of numbers, letters, and special characters. Passwords should be

encrypted or hashed before being stored. Before installing any new devices in network security, all default passwords for online browsers, apps, firewalls, router, wireless connections, and other networks should be changed. Passwords must not be reused for at least the following six months, according to operating systems. When an administrator account's login attempt fails, the system should generate a log entry and an alert. Biometrics security and domain admin access should be utilised for all administrator privileges. Various approaches, such as the usage of smart cards with certificates, biometric access, One Time Password (OTP) tokens, and so on, might be used for this type of authentication. The private key must still be stored in a safe and trustworthy hardware, and password protection must be used to enable general steps credential verification.

[18] Cloud computing is a network of computers, generally connected via the internet, that share a variety of resources that are scalable to meet the requirements of the user and are provided by a service provider. Cloud computing allows customers to utilise multiple service models to access software applications and computational capabilities, such as Infrastructure as a Service, Platform as a Service, and Software as a Service. Many approaches are employed to achieve data security. Filtering, erasure, backups, and encryption are the four categories in which these approaches can be classified. Cryptography appears to be the greatest approach to safeguard outsourced data in an unstable environment, such as cloud computing, where we do not have physical control over our data. Indeed, multi-tenancy features and simple provider access to data require us to rely on new solutions based primarily on encryption and access control to maintain confidentiality.

[19] Xiao Zhang proposed a system for ensuring data security in cloud computing in 2011. The defined framework was divided into three aspects of security i.e., Storage protects, transfer protect and authorize. Several regional data centres are being built by cloud storage providers. Single-server level, cross-cabinet level, cross-server level, and cross-data server level are the four levels of file security, ranging from low to high. SSL and TLS, as well as its predecessors, are cryptographic protocols that offer security for network communication. WS security is widely used in cloud computing as it provides XML encryption and XML signature to avoid data integrity and data confidentiality.

IV. DATA SECURITY ISSUES IN CLOUD COMPUTING

To the end-user, cloud computing provides three services: SaaS, PaaS, and IaaS. In cloud computing, multiple levels of security are given in these service types of environments. Cloud computing security technique that is effective It is necessary to have properly secured cloud computing as well as to accelerate the cloud implementation In SaaS, there is a security component data security, data integrity, and identity management are examples of service models. Management, data location, data availability, and so on must all be considered. In cloud computing, enhanced data security is being investigated.

i. Data Security and Protection

Once a client uploads data to the cloud, there should be some certainty that only those who have been given authorization have access to it. Another danger that might have an impact is cloud employees having unauthorised access to sensitive customer information.

ii. Data Integrity

Cloud service providers should develop techniques to ensure data integrity and be able to explain what occurred to a dataset and when it happened when it comes to data security. Detailed records of what data was saved in a public cloud may be necessary.

iii. Data Availability

Normally, customer data is maintained in a database. chunk on a variety of servers, many of which are in different regions maybe in various clouds Data availability becomes a concern in this situation. The availability of uninterruptible and reliable power is a serious concern. It becomes more difficult to provide a smooth service. So, there you have it. It is critical for the provider to ensure proper data availability to the customer user who has been given permission.

iv. Identification Management

Each user's identity is used for a variety of purposes gaining access to a cloud service an explanation should be provided by the provider. Authentication and authorization are provided by an identity management system authorization. This is a critical issue for both the provider and the client in a cloud computing environment, as well as a user. While Authentication and permission are provided by an independent third party federated Identification Management, credential synchronization, and Identification Management stack implemented.

V. METHODS FOR DATA SECURITY IN CLOUD COMPUTING

Data security in a cloud computing environment is defined as a set of policies, protocols, and standards that ensure data security. Cloud computing data security addresses both physical and logical security issues across all service models and delivery kinds. Data backup and disaster recovery techniques must be effective, even though the client's data must be kept in the cloud. Several successful techniques are used in the data recovery and backup process, some of which are discussed below.

A. Elliptical Curve Cryptography

Elliptical curve cryptography (ECC) is a public key encryption technique that uses elliptic curve theory to provide smaller, quicker, and more efficient cryptographic keys. It was proposed for the first time in 1985. (ECC). ECC may achieve a level of security with a 164-bit key that other methods require a 1,024-bit key to achieve. [1] There are two steps, first step

divide cloud data into five packets and add four bits to these five data packets: 0000(1), 0001(2), 0010(3), 0011(4), 0100 (5). These 4-bit data can be applied to data packets at random. In second step elliptic use various size key to encrypt data.

B. Advance Encryption Standard

The AES is a symmetric block cipher. This method executes cloud data in the shortest amount of time. In AES First, data is separated into blocks of 128 bits with different keys sizes of 128, 192, and 256 bits. Second Key expend into blocks then add round apply (key added into block message), this is done by XOR Operation. Substitution steps apply by using substitute table to substitute each byte. The second row has been relocated one space to the left, the third row has been pushed two spaces to the left, and the fourth row has been pushed three spaces to the left as part of the shift row procedure. After completing the mix column procedure, apply the round key to the encrypted data.

C. DNA Based Encryption

The fundamental purpose of a DNA-based data encryption technique for cloud computing is to assure strong data security by generating a lengthy 1024-bit DNA-based password or secret key through a series of procedures. It contains four phases. 1. system setup, 2. registration and login, 3. DNA-based big data storage, and 4. large data access. After completing these four steps data is encrypted.

D. Fully Holomorphic Encryption

An ongoing leap forward in fully holomorphic encryption (FHE) has demonstrated the general consequences of secure calculation outsourcing to be suitable in principle at least now. Holomorphic encryption is a kind of encryption that enables calculations to happen on the figure content to get the figure content, and it is an indistinguishable outcome from the calculations did on the open content. Typically, the holomorphic function underpins either addition or multiplication.

E. Feistel Cipher

Feistel cipher (also known as Luby–Rackoff block cipher) is a symmetric structure used to construct or develop many block ciphers. Same encryption, as well as decryption algorithm, is used. Both encryption and decryption consist of a function called "round function" for fixed several times. A separate key is used for each round. However same round keys are used for encryption as well as decryption.

F. Physical Isolation Implementation

Physical isolation implementation, which can be consolidated in Service Level Agreements. Likewise, the infrastructure is imparted just to "friendly" VMs which are possessed by the same client or other dependable clients.

G. ACPS

System performance gets barely debased, and a little performance penalty is experienced. This system goes about as an impediment towards the acknowledgement of an ACPS system. ACPS Conduct of cloud components can be observed by logging and intermittent checking of executable system files.

H. Caesar Cipher

Caesar cipher, also known as Caesar's cipher, the shift cipher, Caesar's code, or Caesar shift, is one of the oldest and most basic data encryption methods. It's a substitution cypher, which means that each letter in each text is exchanged with such a word with a specified number of places.

I. New Lightweight Cryptographic Algorithm (NLCA)

The proposed algorithm gives an effective structure for security in cloud computing. It uses 16 bytes block cipher and 16 bytes key for encryption and decryption. It comprises only 5 rounds and use unique key at each round. A minor shift in input data can bring dramatic change in ciphered text. As it uses swap and transposition technique. Experimental results shows that it provides high security, low computation cost and clear improvement in encryption and decryption process.

J. Using different cloud servers to save data

In this method, the system divides the provided data from the user into different parts and then encrypts that data with the usage of encryption techniques. After encrypting the data, the system then save that encrypted data onto different servers to prevent the complete loss of data if an attacker gets unauthorized access.

VI. CONCLUSION

Cloud computing is the most recent technological advancements enables quick access to high-performance computing resources without the need for software or hardware installation It has a lot of advantages for its users, but it also has a lot of drawbacks issues with security. It also has a problem with data security. In this study, a thorough examination of data encryption techniques that are applied to convert plain text data into encryption data using a cloud computing system is carried out. We also covered over cloud deployment models, cloud computing service delivery models, cloud security challenges, and data security procedures in depth. These strategies' ultimate purpose is to provide high-level security in cloud-based systems.

References

[1] P. N. X. a. J. R. Yang, "Data security and privacy protection for cloud storage: A survey," *IEEE*, pp. 131723-131740, 2020.

[2] P. R. a. R. P. H. a. J. P. Kumar, "Exploring data security issues and solutions in cloud computing," *Elsevier*, vol. 125, pp. 691--697, 2018.

[3] N. Leavitt, "Is cloud computing really ready for prime time," *Growth*, vol. 27, pp. 15--20, 2009.

[4] B.-H. a. D. E. K. a. W. M. F. Lee, "Data security in cloud computing using AES under HEROKU cloud," *IEEE*, pp. 1--5, 2018.

[5] H. a. R. M. K. Tabrizchi, "A survey on security challenges in cloud computing: issues, threats, and solutions," *Springer*, vol. 76, pp. 9493--9532, 2020.

[6] P. R. a. R. P. H. a. J. P. Kumar, "Exploring data security issues and solutions in cloud computing," *Elsevier*, vol. 125, pp. 691--697, 2018.

[7] S. Namasudra, "An improved attribute-based encryption technique towards the data security in cloud computing," *Wiley Online Library*, vol. 31, p. e4364, 2019.

[8] K. Jakimoski, "Security techniques for data protection in cloud computing," *International Journal of Grid and Distributed Computing*, vol. 9, pp. 49-56, 2016.

[9] F. a. A. S. a. A.-A. A. H. a. J. S. Thabit, "A new lightweight cryptographic algorithm for enhancing data security in cloud computing," *Elsevier*, vol. 2, pp. 91--99, 2021.

[10] R. a. K. I. A. Qazi, "Data Security in Cloud Computing Using Elliptic Curve Cryptograph," *Arabixiv*, 2020.

[11] U. Ogiela, "Cognitive cryptography for data security in cloud computing," *Wiley Online LibrarY*, vol. 32, p. e5557, 2020.

[12] K. a. B. S. S. a. V. Y. Sajay, "Enhancing the security of cloud data using hybrid encryption algorithm," *Journal of Ambient Intelligence and Humanized Computing*, pp. 1--10, 2019.

[13] A. a. S. S. Singh, "Enhancing Data Security in Cloud Using Split Algorithm, Caesar Cipher, and Vigenere Cipher, Homomorphism Encryption Scheme," *Emerging Trends in Expert Applications and Security*, pp. 157--166, 2019.

[14] S. a. S. A. P. Singh, "Ensuring data security in cloud storage," *Int. J. Mach. Learn. Comput*, vol. 8, pp. 382--386, 2018.

[15] P. R. a. R. P. H. a. J. P. Kumar, "Exploring data security issues and solutions in cloud computing," *Procedia Computer Science*, vol. 125, pp. 691--697, 2018.

[16] I. A. a. Z. S. V. Sukhodolskiy, "An access control model for cloud storage using attribute-based encryption," *2017 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus)*, pp. 578--581, 2017.

[17] K. Jakimoski, "Security techniques for data protection in cloud computing," *International Journal of Grid and Distributed Computing*, vol. 9, pp. 49--56, 2016.

[18] M. a. B. S. K{\"o}hler, "VCE-A versatile cloud environment for scientific applications," *The Seventh International Conference on Autonomic and Autonomous Systems (ICAS 2011)*, pp. 22-27, 2011.

[19] X. a. D. H.-t. a. C. J.-q. a. L. Y. a. Z. L.-j. Zhang, "Ensure data security in cloud storage," *2011 International Conference on Network Computing and Information Security*, vol. 1, pp. 284 - - 287, 2011.

[20] S. a. D. D. a. K. S. a. S. R. a. S. A. Namasudra, "Towards DNA based data security in the cloud computing environment," *Elsevier*, vol. 151, pp. 539--547, 2020.