Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 5, No. 3, May : 2023

# ANALYSIS OF SECURITY THREATS IN CLOUD COMPUTING

**Ayush Kumar,** Student, Computer Science and Engineering, Medi-Caps University
**Deepanshi Joshi,** Student, Computer Science and Engineering, Medi-Caps University
**Giraj Neema,** Student, Computer Science and Engineering, Medi-Caps University
**Ms. Swati Tahiliani,** Assistant Professor, Dept of Computer Science and Engineering, Medi-Caps University

## ABSTRACT
In recent years, the term "cloud computing" people and organisations to maintain all of their crucial data, software, and infrastructures running properly on internal computer servers because of the exponential expansion in data use that occurred with society's shift towards the digital age of 21st century. The on-demand distribution of IT resources via the internet with pay-per-use modifications is known as cloud computing. You can pay to use a cloud computing service in place of purchasing and maintaining computer hardware and software. There is no need for you to invest the necessary time, effort, or resources. Even if many security issues are taken into account, some remain unresolved, and several techniques are suggested to overcome security issues. This paper provides an overview of cloud computing systems, including key traits, categories, delivery paradigms, and different encryption techniques. Several encryption methods have been compared in order to guarantee the privacy of data on the cloud. The primary data security concerns related to cloud computing are finally covered.
**Keywords :**Cloud Computing, Data Security, Threats, Confidentiality, Encryption.

## 1. INTRODUCTION
The usage of data and computational resources from the cloud over the Internet is known as cloud computing. It doesn't store any information on users' PCs. Servers, networking, databases, data storage, and other computer services are all available on demand. Many facets of cloud computing may be traced back to the 1950s, when businesses and academic institutions started renting out mainframe computer calculating time. Renting was one of the only ways to acquire computing resources at the time because owning or managing computing technology on one's own was prohibitively expensive and difficult. The concept of cloud computing originated when mainframe computers were launched in 1950 and made accessible via thin/static clients. The National Institute of Standards and Technology (NIST) provides one of the standard definitions, [1] “a model for enabling convenient, on demand network access to a shared pool of configurable computing resources (e.g., Network, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction”. In cloud computing, security and privacy are always the top priorities. Although cloud computing holds great promise for IT applications, there are still some problems that need to be fixed before people and companies can store data and run programmes there. Data security, which is accompanied by problems with compliance, privacy, trust, and legal difficulties, is one of the biggest obstacles to adoption. Because data are dispersed across numerous machines and storage devices, including servers, PCs, and other mobile devices like wireless sensor networks and smart phones, data security becomes a particularly critical issue in the cloud computing environment. In comparison to traditional information systems, data security in the cloud is more difficult.
Computing and data storage are the two fundamental types of services offered by cloud computing environments. Customers of cloud services do not need anything to use the cloud computing environment; all they need is Internet connectivity to access their data and complete their computing chores. Clients don't even know where the data are kept or which machines are doing the computing during data access and computation. When it comes to data storage, user trust and the successful use

of cloud technologies are mostly determined by data protection and security. In the study of cloud computing, a number of data security and protection methods have been put forth. However, techniques connected to data protection need to be improved much more. The meaning of security is plentiful. Information availability, the prohibition of unauthorised withholding of information, anonymity, the prevention of unauthorised disclosure of information, and information integrity are all components of security. In the current era of the long-dreamed-of concept of computing as a utility, security plays a crucial role. It can be divided into five subcategories: *Security of Cloud Infrastructure, Security of Cloud Applications, Security of Cloud Data, Identity and Access Management in the Cloud and Compliance and Governance in the Cloud*.[2]
The structure of this paper is as follows: The Essentials of Cloud Computing are discussed in Section 2, and the Cloud Computing Classifications are presented in Section 3. Delivery/ Deployment Models for Cloud Computing are shown in Section 4. The various encryption techniques for data security in cloud computing are explained in Section 5. Section 6 lists Current Cloud Computing Data Security Issues, and Section 7 wraps up the paper.

## 2. Key points of Cloud Computing.

- **On-Demand Self-Service:** The provisioning of computer services, such as server time and network storage, can be automated with cloud computing. You are not required to interact with the service provider. Customers of cloud services can access their cloud accounts through a web self-service portal to view their cloud services, monitor their consumption, and provision and de-provision services.
- **Broad Network Access:** Access to a wide range of networks is another crucial feature of cloud computing. Mobile devices, such as laptops, desktop computers, tablets, and cell phones, can access cloud services across a network. A private cloud employs a local area network, whereas a public cloud uses the internet. Since they have an effect on service quality, latency and bandwidth are crucial for both broad network access and cloud computing.
- **Resource pooling:** Using a multi-tenant approach, resource pooling enables numerous customers to share physical resources. This paradigm distributes and redistributes physical and digital resources according to demand. With multi-tenancy, customers can share the same apps or infrastructure while still maintaining their security and privacy. Customers may be able to designate the location of their resources at a higher level of abstraction, such as a country, state, or data centre, even though they won't know the precise location of their resources. Customers can pool a variety of resources, including memory, computing power, and bandwidth.
- **Rapid Elasticity:** Customers can scale swiftly based on demand thanks to the elastic provisioning and releasing capabilities of cloud services. There are essentially no limits on the capabilities that can be provisioned. Customers can use these features whenever they want and in whatever amount. Customers can scale cloud capacity, cost, and usage without incurring additional contracts or charges. Quick elasticity means you can use the cloud computing capabilities offered by the cloud provider rather than buying new computer gear.
- **Measured Service:** In cloud-based systems, metering capabilities optimise resource use at an abstraction level appropriate for the service being provided. For instance, you may employ a metered service for users, storage, processing, and bandwidth. Using a pay-for-what-you-use business strategy, customers are only charged for what they really consume. A transparent experience is produced for both service users and providers by monitoring, managing, and reporting resource utilisation.

## 3. Functionality of Cloud Computing

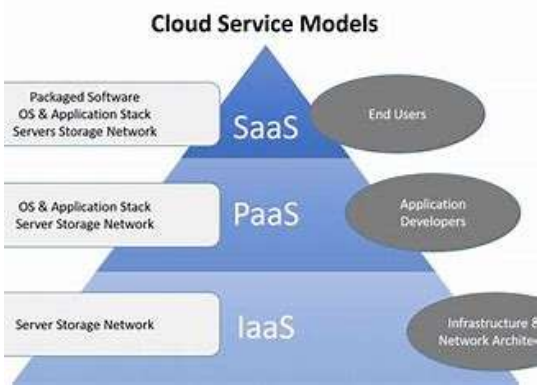
Cloud computing is usually classified based on location, or on the service that the cloud is offering. Based on cloud location, we can classify cloud as public, private, community and hybrid.

- **Public Cloud:** The whole computing infrastructure of a public cloud is housed on the grounds of the provider of the cloud service. It is the IT infrastructure that is utilised concurrently by numerous businesses and services. It is the most cost-effective choice for users because the infrastructure and bandwidth costs are covered by the service provider. It only comes in a few variants, and pricing is based on consumption. They provide a simple, inexpensive, and highly scalable alternative to traditional methods for deploying websites and business processes.
- **Private Cloud:** Large corporations use the private cloud, as the name suggests, to create and run their own data centres for specific business and IT processes. A single organisation is in charge of and manages a secure IT infrastructure. The company can either operate its own private cloud in-house or contract out this work to a third party. Infrastructure might be installed in a data centre or on the customer's property. The best private cloud is one that is established on an organization's property and is managed by staff members.
- **Community Cloud:** A community cloud is shared by organisations that have a common aim or are part of a specific community (professional community, geographical community, etc.). A community cloud, for instance, may be owned by a single nation's government. Community clouds can be located both on and off the premises.
- **Hybrid Cloud**: A hybrid cloud is created by combining a private and public cloud, allowing for greater flexibility, cost-effectiveness, and control over important operations and assets. This kind of cloud is frequently used when an organisation experiences seasonal activity spikes; in other words, when the internal IT infrastructure is unable to handle the present problems, some facilities are moved to a public cloud (for instance, enormous quantities of raw statistical data or something else that doesn't improve the enterprise), as well as to give users access to enterprise resources (for private clouds) via a public cloud.

## 4. Cloud Computing Deployment Models

Services provided by cloud companies are classified into the following three categories:

- Software as a Service (Saas)
- Platform as a Service (Paas)
- Infrastructure as a Service (IaaS)




- **Software as a service:**

SaaS, also referred to as software as a service, is essentially a web platform that gives consumers subscription-based access to cloud computing. Instead of being purchased once, as with a product, the answer is delivered regularly, much like a service. SaaS services offer data management and storage capabilities to businesses. These services frequently involve marketing, collaboration, process automation, and data organisation. Development environments may also be provided as a software as a service (SaaS) offering. In this case, software developers have access to a platform where they may

create, test, and release products, customise their features, and work using pre-built tools and templates.
Examples of Saas- Google's G suite, Microsoft Office 365, Salesforce.

- **Platform as a service**:

Platform as a Service (PaaS) is software that gives users access to development tools, APIs, and deployment tools. Users have access to cloud storage and virtual development environments, which they can use to create, test, and run apps in. Users of PaaS are only charged for the platforms they use during the time the services were used. Like with desktop solutions, there is no need to pay for too functional features.
Examples of Paas- AWS Elastic Beanstalk, Apache Stratos, Magento Commerce Cloud.

- **Infrastructure as a service:**

IaaS offers enterprises ready-to-use IT infrastructure, including tools for software development and testing, private networks, secure data storage, development environments, and functionality monitoring. The businesses may fully power the development process with third-party servers and cloud backup storage, eliminating the requirement for them to create and safeguard their own IT infrastructure.
Examples of Iaas- Amazon web services, Microsoft Azure, IBM Infrastructure, Google Cloud Infrastructure.

## 5. Methods of Encryption for data security in cloud.

To protect sensitive information, encryption techniques are employed [3]. For cloud-based data, there are two standard encryption algorithms:

- **Symmetric encryption:**

Both encryption and decryption employ the same key. Bulk data encryption is where this technology is most frequently used. It is less secure than the asymmetric option despite being quicker and more simply implemented because anyone with the encryption key can decode the data.

**Asymmetric encryption:**

Data is encoded or decoded using two keys—a public and a private authentication token. The keys are not the same even though they are connected. This approach offers improved security since users must possess both a public, shareable key and a personal token in order to access the data.

Classical encryption algorithms are typically divided into two categories:
¬ Substitution Cipher (where one character replaces another)
¬ Transposition Cipher (where characters are reordered).
The idea of homomorphic encryption comes from the mysterious field of abstract algebra. Homomorphic refers to the ability to turn two separate groups of objects into one with the same shape or effect. There are no restrictions on the kind of manipulations that can be done thanks to fully homomorphic encryption (FHE) [4].
Multiple symmetric encryption methods that successfully handle vast amounts of data are discussed in the following section:

❖ **Classical Substitution Cipher Algorithm**

In contrast to the original Caesar Cypher, Padmapriya et al.'s method for supplying the inverse of the Caesar Cypher [5] enables greater data protection. Their paper's major focus is on a new level of encryption for ASCII whole characters, which is crucial for building a comprehensive data security solution. The letter three positions below in the alphabet is being replaced by the Caesar Cypher. For instance, the plain phrase "COME" will be transformed into the cypher text "FQOH". However, since there are only 25 key possibilities, this cypher is vulnerable to a brute force attack.
Playfair cypher, which encrypts several letters, was devised by Sastry et al [6]. They employed a 5x5 square matrix with appropriately spaced-out alphabetic letters. The key can be chosen by the user and entered into the matrix. A key can be chosen by the user and entered into the matrix. The remaining

English alphabet letters are then sequentially added to the Playfair cypher matrix using the key. The plain text is divided into pairs, and if a pair contains the same alphabet, the filler letter "x" is used to separate the pairs.

**Fully Homomorphic Encryption**

The implementation of a method to work with encrypted data without having to decrypt it was suggested by Maha Tebaa et al [7]. The results of the computations will be the same as if the authors had worked directly with the raw data. Without previously decoding it, the Homomorphic Encryption approach can work with encrypted data. The client is the only one who has access to the secret key in homomorphic encryption systems, which are used to access encrypted data without having access to the private key (decryption-free). In their study, a novel security paradigm that respects data secrecy allows for the provision of calculations' results on encrypted data without disclosing the original data used for the calculation. Homomorphic encryption algorithms' complexity is increasing, and it compares how quickly they respond to requests for the public key.

Fully homomorphic encryption (FHE), as introduced by Huda et al. [8], enables a user to compute any result from the data without knowing the secret decryption key. The author uses a key delegation-based FHE technique to protect the availability, secrecy, and other attributes of multi-level hierarchical data. They suggest adopting homomorphic cryptography along with attribute-based encryption as their framework approach.

**Cryptography, Encryption Technique**

Sugumaran et al.'s [9] reviewed data security tactics and recommended an architecture for cloud data security. Their architecture was created to store data in the cloud in an encrypted format using block cipher-based cryptography. A secure cryptographic technique is the foundation of their proposed solution for data storage. Using block-based symmetric cryptography, this architecture was created for data security and offers better storage performance. By focusing on the symmetric layer, they strengthened data encryption, and using this technology to maintain user data in the cloud is effective. A "Three-way mechanism" that enables simultaneous data security, authentication, and verification has been proposed by Prashant et al. [10]. Their suggested architecture would combine the Diffie Hellman key exchange and digital signature with the AES algorithm to safeguard the privacy of data kept in the cloud. They recommend a method that makes it challenging for hackers to undermine the security mechanism, protecting cloud data.

¬ Diffie Hellman keys in exchange.

¬ Digital Signature used for authentication

¬ User’s data files are encrypted or decrypted using the AES encryption technique.

Two different servers are maintained in a cloud storage environment to prevent data alteration. One server is used for the encryption process and is referred to as a computing platform, while the other is referred to as a storage server to store user data.

**Cloud DES Algorithm**

The DES method has been suggested for use in the protection of data in cloud computing by Neha Jain and Gurpreet et al [11]. Both clients and servers should feel secure using this cypher block chaining method. The system's security architecture was created utilising DES cypher block chaining, which ends the current practise of leveraging stolen data to commit fraud. There is no risk associated with the sent data being intercepted and replaced. Although the encryption system is tolerably safe, as computing power grows, the degree of encryption must be increased. A symmetric key is used to encrypt the communication system between the modules in order to secure it. The author claims that when examining data security risk, requirements, deployment of security features, and data security method through encryption, cloud data security must be taken into account. Their paper's key contribution is a new perspective on encryption-based data security solutions, which is significant and useful for creating comprehensive security solutions.

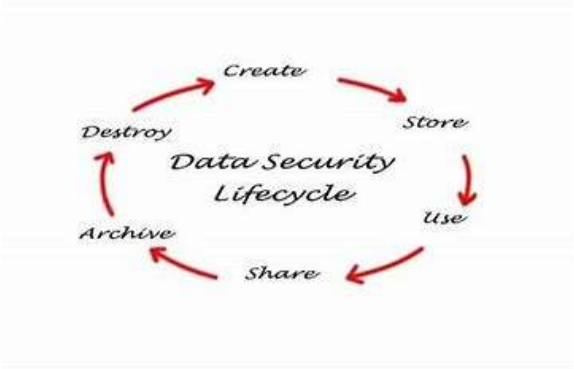
In order to safeguard the data from unauthorised access, Monikandan et al. [12] have presented an encryption technique that addresses the concerns regarding privacy and security in cloud storage. Two methods can be used to assault data. An administrator having access to user data constitutes an insider attack. Third parties can access user data when there is an outside attack. To prevent unauthorised access to the data saved in cloud storage, the author suggested a symmetric encryption technique. Their suggested method translates plain text to the which corresponds to the ASCII code value for each letter of the alphabet, with key values ranging from 1 to 256. By combining replacement cypher and transposition cypher, this method enhances conventional encryption methods. Large amounts of data can be encrypted in cloud storage with symmetric encryption because of its speed and computational efficiency. Their suggested approach is used to encrypt user data in cloud storage so neither administrators nor attackers can access it. This paper's main contribution is a comparison of different symmetric encryption algorithms based on their methodologies, descriptions, ideas, security, and challenges addressed.

## 6. Data Security Concerns in Cloud Computing

Data security is the process of defending data against unauthorised access, modification, or destruction. In the cloud computing model, the service provider is in charge of upholding data security. In recent years, technology has concentrated solely on the process management stage of the data security life cycle. The steps of the data security life cycle are shown in Figure 2.

¬ **Create**: This stage involves creating new digital content for clients or servers in the cloud.

¬ **Store**: Data is saved in the repositories or across several nodes during this phase, which follows the creation process simultaneously.




¬ **Use**: This stage employs the repository's data in a number of procedures.

¬ **Share**: Data communication between customers and partners takes place during this phase.

¬ **Archive**: This stage involves using the data that has been saved for later use.

¬ **Destroy**: Anything stored in the repositories will be permanently deleted during this phase.

Threats to data security can be categorised as either internal or external. Because cloud service providers and users are the primary causes of these dangers, internal threats typically result from an insider attack. Because third parties can access data, external hazards primarily arise from outside attacks. The user's private information is at risk of theft [13]. When talking about data security in the cloud, there are six different categories of important issues [14]:

¬ **Authentication**- A data set's integrity and origin are verified by data authentication. Data integrity ensures that the person receiving it can be certain the information hasn't been altered. Data origin authentication proves to the recipient that the data was sent by the specified sender at first.

¬ **Privacy and Confidentiality-** As more and more conceivably sensitive personal data is collected, archived, and released by both government and non-government organisations, data privacy has become a major problem in contemporary culture. When it comes to statistics agencies, the owners or

stewards frequently assess both the types of data they make available to the public and the structure of the data products they release.

¬ **Integrity-** This term refers to consistency of the quality, correctness, and completeness of data over time and across different forms. Your company performs ongoing data integrity maintenance. Although the two notions are related, it's crucial to keep in mind that data integrity and data security are two separate principles. Data security comprises protecting data from internal and external dangers while preserving the privacy of the subjects. This helps to preserve the integrity of the data by certifying that it hasn't been impacted by those dangers.

¬ **Location-** The location of the data's hosting was unknown to cloud customers, who in reality wish to know the precise location. The users must contractually agree that the data will remain in a specific location.

¬ **Availability**- The process of making sure data is accessible to applications and end users when and when they need it is known as data availability. Along with the essential IT and management procedures, tools, and technologies needed to allow, manage, and keep making data available, it determines the level or extent to which data is easily useful.

¬ **Storage, Backup and Recovery-** Users who choose to transfer their data to the cloud should make sure the cloud provider has suitable resilience storage systems. Data recovery and backup procedures are made easier. The cloud service providers will spread out the data storage among numerous different servers.

## 7. CONCLUSION

The technology of cloud computing is flexible and has received a lot of attention recently. When talking about cloud security, both customers and providers have a responsibility to ensure that the data stored in the cloud is protected from all internal and external risks as well as cooperation between those parties. Data security is one of the biggest problems with cloud computing because it has several facets, including surveillance, reliability, availability, security, anonymity, communications capacity, government, backup, and recovery. However, securing data stored in cloud storage is the most crucial aspect of data security. This paper examines the significance of cloud data security. Symmetric encryption algorithms are used because they can manage the encryption of massive amounts of data and can store data quickly in the cloud.

## 8. REFERENCES

[1] T. Grance and P. Mell, “The NIST Definition of Cloud Computing”, September 2011

[2] Tim Mather, Subra Kumaraswamy, and Shahed Latif, "Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance", September 2009.

[3] Subhasri and Padmapriya,” Cloud Computing: Security Challenges & Encryption Practices”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 3, ISSN: 2277 128X, March 2013.

[4] C. Gentry, "Computing Arbitrary Functions of Encrypted Data", ACM, Vol. 53, Issue 3, March 2010, pp. 97-105

[5] Padmapriya, Subhasri,” Cloud Computing: Reverse Caesar Cipher Algorithm to Increase Data Security”, International Journal of Engineering Trends and Technology (IJETT), Volume 4, Issue 4, 2013.

[6] S. Durga Bhavani, N. Ravi Shankar and V.U.K. Sastry, “A Generalized Playfair Cipher involving Intertwining, Interweaving and Iteration”, International Journal of Network and Mobile Technologies, pp 45-53, 2010.

[7] Saïd El Hajji, Maha Tebba and Abdellatif El Ghazi, “Homomorphic Encryption Applied to the Cloud Computing Security” Proceedings of the World Congress on Engineering, London, U.K. ISBN: 978-988-19251-3-8 ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online), Vol 1, July 4 - 6, 2012.

[8] Elmogazy Huma and Bamasak Omaima,” Towards Healthcare Data Security in Cloud Computing”, IEEE 8th International Conference for Internet Technology and Secured Transactions (ICITST-2013)

[9] B. D. Kamalraj, Sugumaran and BalaMurugan.” An Architecture for Data Security in Cloud Computing”, IEEE World Congress on Computing and Communication Technologies 2014
[10] Pawar Yogita and Rewagad Prashant,” Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing”, 2013 IEEE International Conference on Communication Systems and Network Technologies
[11] Gurpreet Kaur and Neha Jain,” Implementing DES Algorithm in Cloud for Data Security” VSRD-IJCSIT, Vol. 2 (4), 2012, 316-321.
[12] S. Monikandan and L. Arockiam,” Data Security and Privacy in Cloud Storage using Hybrid Symmetric Encryption Algorithm”, International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 8, August 2013.
[13] Qiaoyan Wen, Xiaojun Y,” A View about Cloud Data Security from Data Life Cycle”, IEEE 2010.
[14] Parsi Kalpana and Sudha Singaraju, “Data Security in Cloud Computing using RSA Algorithm”, International Journal of Research in Computer and Communication technology, IJRCCT, ISSN 2278-5841, Vol 1, Issue 4, September 2012.