*International Journal of Engineering & Technology*, 7 (4.39) (2018) 485-491

International Journal of Engineering & Technology

*Website: www.sciencepubco.com/index.php/IJET*

***Research paper***

# An Investigational Study on Cloud Security Model and Data Privacy Schemes

**Chaithra M H[1]*, Dr. Vagdevi S[2]**

*[1]Assistant Professor, Dept of CSE, REVA University, Bangalore, India*
*[2]Professor & Head, Dept of Electrical & Electronics Engineering, GSSS Institute Of Engineering And Technology For Women*
*Mysore, Karnataka, India*
**Corresponding author E-mail: chaithra.mh14@gmail.com*

## Abstract

At present, cloud computing receiving more attention to the users as well as researchers. It is growing technology which showing more reliable development in the current processing world. It is increasingly popular by offering distinctive administrations like cloud facilitating, storage furthermore, servers and so on for various kinds of organizations as well as in scholastics. On the other hand, there are a few difficulties concerning distributed storage security and information protection. Security is as yet difficult in the distributed computing framework. Such difficulties incorporate loss of client's delicate information, spillage of information and revealing of clients mystery information. By considering these security and information protection issues inside the cloud foundation. This investigation for the most part audits the diverse security and protection difficulties, and arrangements. Additionally, this paper highlights the possible opportunities for storage security and data privacy in distributed computing environment

***Keywords***: *Cloud computing, Cloud security, Data privacy, Privacy preserving, Public auditing.*

## 1. Introduction

Cloud computing has reached to the popular level of acceptance that facilitates effortless and cost-effective services in the domain of information technology. It is a collection of a pool of end-devices connected through a network where sharing of resources takes place. Cloud computing provisions distributed computing environment that reduces the user's burden of physical installation as well as the overall cost for storage space, resource sharing, and processing power etc. Overall, it provides on-demand services by which user can share or access any kind of information from anywhere in the world at any time by using any device through internet connectivity [1] [2]. Generally, the customary idea to speak to the cloud framework incorporates 1) cloud benefit models (i.e. SAAS, PAAS, and IAAS), 2) organization models (i.e. Open, Private and Cross breed cloud) and 3) Fundamental qualities (Asset pooling, on interest administrations, Fast Versatility and so forth) [3].

Cloud technology is still growing very faster than expected. It has invited lots of users as a consumer towards achieving the business goal with increasing competitiveness by optimal resource utilization with low cost like data storage, backup, test & development, large data processing, etc.

As per the statistics of worldwide cloud-based online user, in 2013, 2.4 billions of user's were consumer of cloud technology and in 2018; about three.6 billion of clients are predicted to get entry to cloud services [4].

Cloud computing offers various services by serving their computing resources on the different level to many Agencies with an green, bendy and fee-effective manner. Therefore, those cloud offerings opens no. of security challenges and privacy worries between the cloud company and the cloud user [5]. In cloud computing, end users consume services Without knowing what procedures are involved, as the person has no concept of the physical location of the server and additionally the person's don't have any concept about what configuration concerned in processing of personal statistics. Thus, storing personal facts on a cloud server may want to generate a first-rate chance to user's privacy because the statistics saved in the cloud-database is simpler to control, and also easier to lose control of it. Whereas, security issues in cloud includes data security, data-backup & storage, network traffic system and files system. Therefore, data privacy and secure authentication is the significant factor in cloud environments [6]. There are various types of security protocols which makes the cloud services trustworthy & reliable and some of them are based on cryptographic concept and some are based on Non-cryptographic concept. The Cryptographic method refers to a technique that ensures the data protection by performing encryption as well as decryption operations. Basically this technique involves three algorithms viz; a) Symmetric-key set of rules, b) Asymmetric-key algorithm and c) Hashing algorithm. Symmetric key algorithm uses single secret key which performs both encryption and decryption operations to ensures the authentication and authorization. It contains algorithms like Advanced Encryption Standard, Data Encryption Standard, Ron Rivest Shamir Adleman-(RSA) and Blowfish algorithm. Asymmetric-key algorithm is also known as Public-key cryptographic set of rules which makes use of non-equal keys (i.E. Public key and personal key) for encryption operation. This algorithmic approach ensures the trustworthiness between the two parties. It contains encryption techniques like RSA and Diffie-Hellman Key Exchange. Whereas, the Hashing algorithm uses a cryptographic concept together with a hash function in which data numeric value is converted into fixed length compressed value. This set of rules may be very powerful to comfortable the password and to check the integrity of information. Hashing algorithm includes hash capabilities which includes Message Digest-5, Secure Hashing Algorithm-1(SHA-1), and SHA-2.While, non-cryptographic approach are those which do not depends on sharing of any key components. These techniques based on the Randomization, Anonymization and data hiding methods [7] [8].

Although, cloud computing gives numerous blessings its consumers, along side it has some demanding situations related to numerous safety attacks including Protocol assault, bandwidth assault, XML based totally DoS assault, Distributed denial of carrier (DDoS), and so forth out of them DDoS attacks are a very serious unwanted attempt, where an attacker can access all resources. As a result it affects the availability of cloud services with the intention to make the user unable to use of cloud resources and steal all information from the database. This attack occurs when an attacker compromises most of the agents (vulnerable machine) of the network where the target may be storage, main servers, web servers, CPU or other cloud network components. The major security challenges in the cloud seem to be as data segregation & protection and data leakage. So it is very important to understand security challenge and robust solutions to handle these challenges [9][10][11].

The proposed paper analyzes the key technologies of cloud computing and investigates the application in secure authentication and privacy preserving. The study mainly concentrates on aspects of privacy preserving and encryption based security approaches. The organization of the paper contains multi-fold patterns which are organized as comply with: The Section-II explores the model of cloud security and its related work. Section-III illustrates the existing approaches to cloud security. Section-IV describes the various privacy preserving method and their applications followed by solution techniques for privacy preserving in section-V. Section-VI highlights the different challenges over cloud security and data privacy. Section-VII defines some open research issues towards the cloud storage security and privacy. Finally, section-VIII describes the conclusion of the study.

## 2. Cloud Security Model

Cloud computing is an integrated technology and policies to protect data, infrastructure as well as services from possible attacks. The necessity of security in the cloud computing is the most essential thing which protect the data from the attackers. The following Figure-1 represents the cloud security architectural model. The security model composed of several components which are briefly explained in the following sub section [12].

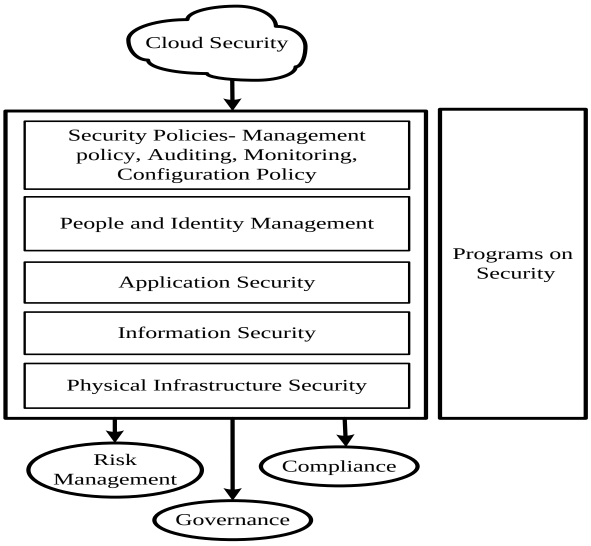
Cloud Security
Security Policies- Management policy, Auditing, Monitoring, Configuration Policy
People and Identity Management
Application Security
Information Security
Physical Infrastructure Security
Programs on Security
Risk Management
Compliance
Governance

**Fig. 1:** Security model for cloud-computing

### 2.1. Security Policies, Risk Management Etc

The primary task of the every organization is to identify and implement task and processor controls the organizational structure. In this Security governance is the set of policies, law, and technologies which are work within the organization and provides directions to achieve robust security [12]. Significant responsibilities of the organization are; to protect the organizational Touchy facts; recognize the criminal issues, records lifecycle management, portability, and interoperability. For effective risk-management, the organization should implement the secure framework and measures its performance by metrics computation process.

### 2.2. People and Id Management

In Cloud computing environment, only authorized person can enter and access the resources of the organization using ID federation method for security purpose. Here an only genuine person can log on to the system and access the data. Thus from this process can reduce the security issues appeared in the system.

### 2.3. Application Security

In this, the service provider should give protection to the user by following a secure development process. XML signature and XML encryption scheme can be applied to triumph over the all internet carrier assaults.

### 2.4. Information Security

Data and information security is the most significant aspect of the cloud, so standard encryption method must be applied to protect data privacy. At the same time, interruption prevention and detection system have to be designed for information security purpose.

### 2.5. Physical Infrastructure Security

Security of Physical infrastructure is one of the primary attributes in the security model. There are several security safeguards including Biometric Access-Control (BAC), CCTV (Close Control Television Monitoring) and door alarm. A Computer-based access control system (CAS) utilizes the badge-readers to allow only permitted persons to enter the controlled region.

Based on cloud security model, different researchers have proposed their scheme to improvise the cloud security level which is given as follows;

Zheng and Yonghui [13] introduced an Artificial Immune machine (AIS) primarily based cloud security version for the detection of viruses & malware attacks in the system instead of using antivirus software. The proposed model forms a combination of the local host-based detector with multiple detection machines in the cloud to detects the malware. The performance of the proposed scheme provides better malware detection rate.

In [14] Ashraf et al. presented a TSM (Transparency Service Model) for client data protection in cloud infrastructure by thump data information from the cloud provider. From this mechanism cloud provider can configures the services on cloud by offering service information about cloud database. The proposed system was evaluated efficiently using cloud provider information.

The research work of Tesfamicael et al. [15] examined the feasibility for the formation of a usable model to permit assessment of the layout model and alertness of trading Communication System (TCS). The proposed method adopted a OPNET concept which analyzed and showed the performance of TCS on cloud and may lead better performance rate.

The virtual security risk assessment model was proposed for the cloud using stochastic game nets in [16]. In this experimental study virtualization, security risk scenario and factors were evaluated by using graphical tools. For the analytical study proposed scheme was proved that system is more powerful to simulate complex and dynamic security disturbances in cloud service.

Ebrahim et al. [17] presented a new cloud safety version for facts protection & privacy the use of a combination of steganography and cryptography strategies. The proposed version consists of 3 phases like 1) Hash data the usage of SHA (Secure Hash Algorithm), 2) AES (Advanced Encryption Algorithm) to encrypt the data and 3) public key cryptography to encrypt the hash-code as well as a new key. LSB is formed here to embed all encrypted information. The analysis of proposed method provides the higher accuracy and better performance by calculating PSNR and comparing with other existed method.

Wei et al. [18] Explored a new mechanism of Belief Rule Base (BRB) version for cloud protection state prediction with the aid of referring large-scale monitoring records. The method carried towards quantitative and qualitative analysis of information in a parallel way. Additionally, have introduced ER algorithm to integrate many indicators with uncertain information so security state of cloud computing was found accurately. The proposed system analyzed and gives more accurate results.

Zhou et al. [19] concentrated on a data privacy problems and proposed a Service Level Agreement (SLA) model for se curity of cloud computing. To overcome these problem cloud computing along with Markov decision process theory utilized. With the evaluation of proposed method VDM (Violation Detection Model) was achieved good results in prediction effect.

## 3. Existing Approaches to Cloud Security

Cloud security defines the set of techniques, tactics and general protocol to supply data file with safety. It is a conversation of each bodily and logical protection attributes from all special carrier prototypes. Different approaches have proposed to increase the level of cloud infrastructure security.

Cloud security model introduces several techniques for example; RSA, DEC, ECC, SHA, PKI, and key management. These approaches are discussing based on a prior study in below section.

### 3.1. RSA Algorithm

The data security using RSA was analyzed in the work of Soumya and Prabha [20]. RSA is a public-key based Asymmetric Cryptographic approach and best suitable for data forwarding data on cloud and web-based environment. Several encryption & decryption technique is utilized for Cryptanalysis (i.e., Play fair cipher, mono-alphabetic cipher, and Hill cipher, etc.). The hacker is always trying to get the original text, so it's checking every possible key, to avoid this problem public key cryptography method is used. RSA algorithm is a deterministic encryption algorithm which secures data in clouds using both public and private key.

The facts protection for cloud computing the use of RSA and stegano-graphy turned into added in [20,21], which will increase the extent of cloud security by means of utilizing RSA encryption set of rules. Shereek et al. [22] introduced a hybrid data encryption method using RSA and Blowfish algorithm.

### 3.2. DES Algorithm

DES contains a single secret-key for both encrypting and decrypting the data. This algorithm encrypts the plain-texts as block-ciphers on 64-bit units with fixed number ciphers bit at a time. The key-length is 56 bits; actual inputs are 64 bits. However, some problems are appearing with DES algorithm- switching common secret-key over the unsecured internet, problem established if the contents are sent by the claimed–sender.

In cloud computing, DES algorithm was utilized for avoiding hacking of data from the attackers, even though this scheme is more used to consume less encryption time during algorithm implementation. In [24,25] authors have presented Cloud security model using DES algorithm to secure the channel between the user and cloud computing services. A multistage encryption method for cloud data security using DES was introduced in [26], and Bakhtiari et al. [27] presented secure, searchable data based DES algorithm for cloud computing.

### 3.3. ECC Algorithm

Elliptical Curve Cryptography (ECC) is a public-key encryption technique based at the elliptic-curve concept that may be implemented to draw a cryptographic key with smaller, quicker and higher efficiency. ECC is producing key via the homes of elliptic curve equation in place of any other traditional scheme of technology. This technique widely used in mobile by providing correspondent security with lesser computing power and network security. There are many advantages of ECC over RSA can observe such as shorter keys used which is stronger, low on CPU consumption, less memory usage, encrypted data size is smaller. This technique was used in security service like confidentiality in the cloud facility presented in work of Nithiya and Sidevi [28].

In [29, 30], authors have introduced an enhanced cloud security model with providing network security, integrity, and authentication. The research work of Kanna and Vasudevan [31] proposed a Hybrid cryptographic approach The usage of ECC set of rules for reinforcing the privateness of person facts within the cloud. Based on security, optimal resource allocation in cloud computing using ECC expressed in work of Nagalakshmi and Rajalakshmi [32].

### 3.4. SHA Algorithm

Secure Hash Algorithm (SHA) is a process of mapping of arbitrary messages length to n-bit hash code or used to calculate the hash-code for the secret data information to guarantee data integrity. It also provides a guarantee with 128 bits keys to overcoming collision attack and physical attack (i.e., Brute force attacks). This method is known with different forms of SHA-zero, SHA-1, SHA-2, and SHA-3. The SHA with a different number of rounds and output sizes which increases the complexity to break the algorithm as the quantity of rounds increases. SHA-2 gives more efficacy than SHA-1 since SHA-1 utilizes a higher number of packets with less number of processes. The passwords, usernames, bucket key are encrypted using this technique to protect against an attacker.

In cloud computing to achieve data privacy and data integrity, Hiremath and Kunte [33] introduced an SHA algorithm. Photo storage security in mobile cloud expressed in research work of Schwab et al. [34]. The secured cloud infrastructure is likewise checking the integrity of data, privacy, access control and authentication of the user, etc., for cloud service provider presented in work of Patil and Dharmik [35]. The work of Timothy and Santa [36] introduced new security method using SHA-1 with RSA method.

### 3.5. Key Management

The key-management with strong encryption is one of the core principles inside the cloud computing surroundings to shield or secure the saved information. The infrastructure of Cloud key-management sys-tem handles the all types of cryptographic keys in a cloud environment that facilitate all of cloud usability encryption, and it utilizes fewer improvement prices. CKMI (Cloud Management Key Infrastructure) incorporates CKM of server and client. CKMC formed in cloud applications and CKMS have interaction with CKMC utilizing cloud key management interoperability protocol, which communicates with SKMS (Symmetric key management device) and PKI (Public key infrastructure).

Key control infrastructure acts as the main role for safety objects like sending the particular identifier on ‘get' action so that right required key may be retrieved in any other case it’ll be back to the purchaser from the key management gadget. In Cloud computing surroundings, the work on KMI (key management infrastructure) presented in Lei et al. [37].

The multicast key management system provided to the individual user for securing cloud and here new key will be generating when a new user enters into the cloud is explained in work of Shriprasadh et al.[38]. The work of Wang et al. [39] expressed Key-management system for the safety of owner's data and information access control. Online key management based on character existed in surrounding of cloud introduced in work of Cheng et al. [40].

## 4. Privacy Preserving in a Cloud Environment

From the start of adoption of cloud computing methodology, privacy and safety have taken into consideration as a maximum significant challenge. It is real that few of the safety problems are older and less efficient. A lot of safety-related troubles will arise from disbursed gadget and internet, but actual state of affairs represents that superior techniques were to broaden. The evolution of cloud computing system and a large quantity of its users, costumes had pushed big evaluation this site and to research all types of threats that took place on it to locate advance solutions to layout a secure cloud version. There are several protection programs are available inside the cloud market that's stated conventional strategies to securing business enterprise facts systems.

However, privateness-keeping is also one of the widespread challenges within the present day computing world, with the growing demand for cloud computing system, the issues about keeping the privateness also being paid extended [41,42]. But imparting and guaranteeing privacy preserved information gaining access to in a cloud gadget is still in progress and wishes extra interest to attain the goal. There are distinct sorts of privateness-associated problems which behave like barrier are highlighted inside the table 1. Addressing all the ones troubles and growing a version which couldn't be compromised via attackers or intruders might mark the fulfillment of cloud computing. There are numerous traditional methods had been carried out to tackle privacy-associated problems. It is imperative that privateness must be preserved everywhere and each time.

**Table 1:** Privacy preserving issues in Cloud Environment

| Issues | Detail Description |
|---|---|
| In-Sufficient User Management | Authenticated User Lacks the Control on their Data in the Cloud, Particularly during Accessing or Processing in the Cloud. |
| Information Leakage | Leakage of Sensitive Information during Data Transmission Across the Network, it may be User ID or Important Files, etc. |
| Un-Authorized secondary storage | Chances of Accessing or Retrieving useful information. |
| Un-Manageable Data Proliferation | In cloud, Information is Unpredictable & Un-Manageable. |

Jiang et al. [43], have brought an anonymity based totally technique to accomplishing privateness in the cloud gadget. The proposed anonymity algorithm chargeable for processing the records and anonymizes some or all information before the freeing. When it is required, the cloud service company makes the usage of background information it has and integrates the detail records with nameless information to mine the specified facts. This anonymity approach isn't the same as any other traditional cryptographic method for keeping customers privateness because it gets rid of key-management, easy and flexible. But this method is suitable only for few offerings.

Greveker et al. [44], a proposed architecture for database storage in the cloud. This method preserves the consumer's non-public data and prevents the risks of each outside as well as internal assaults from the outsources records. In this system, from the person interface, the request is acquired via having access to the data from the database, that's forwarded in terms of RPC or XML request to the user engine and ultimately to the cloud storage.

Miao et al. [45] proposed privacy hold determine manipulate mechanism. According to this, each cloud person is connected with particular attributes, which makes a decision their get entry to rules. Moreover, the have a look at propounded a two-layer encryption model (one is base segment, and every other is a floor section). In this statistics, privateness is pre-served via presenting access control to the proprietor of the facts and rejecting the cloud-issuer to reap records about the records.

David et al. [46] added a rule-based authorization version for the cloud with the purpose of privateness retaining of person's information. Here, user's can outline their accessing privileges which guarantee the get admission to controlled of facts inside the cloud infrastructure. The proposed authorization model trusts the cloud-vendors & examines only threats which might be generated from outdoor.

In [47], Sayi et al. Have constructed a confidentiality retaining model for consumer's information. The privacy attributes are defined in phrases of a graph. The links and nodes define the limitations and confi-dentiality amongst corresponding nodes. Additionally, this look at illustrated a graph-coloring algorithm which performs the frag-mentation and putting fragmentation in a appropriate vicinity. The effectiveness of this technique can be improved by using modeling hyper-graph in preference to a 2-D graph.

Rahaman et al. [48], proposed a version of privateness-preserving for the cloud to achieve privateness. It was a layer-based totally method wherein customers' layer responsible for sending their request for the getting access to of cloud offerings. Whereas community layer accountable for updating the unique IPs correspond to the person request. Hence it ensures the customers privateness of IP address. The topmost layer of this structure is privateness preserves layer which has unique user cloud ID generator. The fundamental task is to preserve the person's privateness facts via executing the privacy check method. This procedure permits the user to specify the get admission to-control & data-transparency in the cloud infrastructure.

Adeela et al. [49], explored a idea of dynamic metadata exploitation in the cloud. By expanding know-how of metadata, the hackers can compromise the consumer’s privateness. So as an answer au-thors added a phenomenon of facts privacy maintenance method. In this technique, metadata needs to be stored in cloud garage and segregate the stored records. Then segregated data is incorporated as private, non-personal & partial personal based totally on the sensitivity of records.

Wang et al. [50] brought a method of privacy-keeping which performed through public auditing in the cloud. For the cloud infra-shape, there isn't appropriate to use traditional cryptographic techniques to acquire safety. The cause in the back of this became to facts-outsourcing. Thus, in this have a look at, they followed the 3rd birthday celebration auditing technique. The proposed auditing version changed into advanced the usage of four algorithms, i.e., key-gen, sing-gen, gen-evidence and verify-evidence algorithms. The first phase of implementation version uses first two algorithms which initialized the name of the game parameters and generates the established metadata. While in the 2nd segment of implementation device applied the other algorithms have been chargeable for the correctness of information in the cloud server. The following discern-three highlights the a few enormous methods of privacy retaining in cloud computing version.

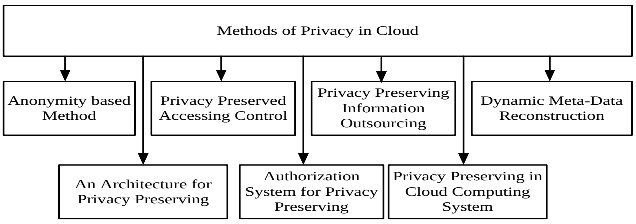
Methods of Privacy in Cloud
Anonymity based Method
Privacy Preserved Accessing Control
Privacy Preserving Information Outsourcing
Dynamic Meta-Data Reconstruction
An Architecture for Privacy Preserving
Authorization System for Privacy Preserving
Privacy Preserving in Cloud Computing System

**Fig 2:** Methods of Privacy-preserving in Cloud

## 5. Solution Techniques for Privacy Problems

The cloud database incorporates a big quantity of information files which does not offer a guarantee on facts consistency and facts integrity. Thus, the host doesn't have faith within the privacy of his/her information since the cloud database can misuse the information of users. For the safety & privacy concerns the consumer has to keep their records safety through third celebration auditor [51]. But the third celebration individual cannot assure consumer’s statistics privateness. For the statistics privateness and safety, the customer needs to encrypt their large statistics statistics before keeping into a cloud database. Some conventional techniques have a few obstacles.

In this check, have categorized the solution strategies for privateness troubles into three classes 1) Encryption Scheme, 2) Access-Control mechanism and three) Auditable Scheme.

Encryption Scheme: There are several encryption me-thods applied to hold the privateness of users statistics inside the cloud. Ruwei et al. [52] have designed a privacy-maintaining cloud storage version to clear up the privateness-related problems. The proposed model comprises the key management, facts-corporation structure, conversation between person participation and managing of updation of users getting access to regulations. This mechanism ensured the facts-consistency and decreases the encryption burden as well as information decryption manner. Also capable of take care of the range of keys, confidentiality, reduced storage area as well as processing time. Finally, the writer concluded that the proposed framework presents better protection and privacy for the user's records.

While within the look at of [53] brought a secret-sharing set of rules which recovers the key mechanism. This set of rules capable of retrieving the cipher textual content and solves the privateness trouble within the cloud storage with the help of encryption technique. It also reduces the workload of users all through the management of data files.

Fan et al. [54] proposed a mechanism of privateness seek method which incorporates "Revocable and Decryptable delegated searching for" each are based totally on symmetric encryption in the cloud database.

There are a few boundaries in encryption scheme like it improvises the weight with limits on the use of information. Such type of barriers can be solved shape having access to manage mechanism.

Access-Control Mechanism: This mechanism is espe-cially applied for the safety of customers facts inside the cloud infra-shape. This mechanism is answerable for identifying the person’ s authenticity with out knowing of customers ID earlier than preserving or storing the records [55]. Only legitimate or authenticated customers can capable of decrypt the information from cloud storage. It preserves the records privacy, handles the security in addition to maintains the name of the game statistics of the person.

Auditable Scheme: From this manner, providers can im-show their system services in addition to ca minimize the web burden. Generally, there are styles of auditing schemes 1) public auditing and personal auditing. Wang et al. [56] proposed a privacy-preserving model of public auditing for the motive to enhance their previous work via en-hancing the information garage safety power. Their experiment evaluation was carried out on an instance of "Amazon EC2" and showed that proposed model achieved the higher efficiency in information storage safety.

**Table 2:** Comparison of privacy-preserving schemes in cloud

| Methods | Detail | Usability of Cryptography |
|---|---|---|
| Anonymity based Approach | Anonymises the Data before Storing in the Cloud Database | No |
| Model for Cloud Storage Privacy Preserving | Defends both External and Internal Attacks | Yes |
| Access Control Mechanism | Defines the access Policies for users and Attains Access Control | Yes |
| Authorization System for Privacy Preserving | Rule-based Authorization Infrastructure | No |
| Data Outsourcing Method | Assures Privacy for data Fragmentation | No |
| Dynamic Re-Construction of Metadata | Performs segregation & meta-data re-construction | Yes |
| Preserving Cloud Privacy Model | Preserves users Information as well as user Identification | No |

From the above desk 2 can say that some researchers applied cryptographic strategies to gain privateness, and some different strategies stored them away and implemented opportunity methodologies to gain privateness. Thus, there may be a want for powerful privateness keeping version that solves the safety and privateness problems and guide the cloud users to make use of cloud-storage services for his or her purpose.

## 6. Challenges on Security and Privacy

### 6.1. Security Related Challenges

Security is the protection of touchy statistics form vulnera-ble attacks. There is several danger attributes which can be worried with cloud infrastructure are highlighted as under.

A. Multitenancy: Multitenancy approach, a unmarried program can run on multiple structures on the same time period, but it reasons the vulnerabilities in case of cloud-infrastructure [57].

B. Access manipulate: The touchy statistics documents within the cloud garage contain several threats. An attacker can hack the file which stored in the cloud garage and may be accessed and utilized later [58].

C. Availability: In cloud database, the person can shop their statistics documents which might be available for that particular user at any-time and everywhere, however in case of cloud failure or backup healing that records may delete. This re-sults inside the lack of self assurance among the customers [59] [60].

D. Trust: nonetheless there are lots of challenges associated with cloud storage machine. Still, there may be no faith dating some of the cloud customers and cloud companies. Users can’t trust on cloud carriers approximately their sensitive information to be preserved on cloud storage [61].

### 6.2. Privacy Related Challenges

Privacy means protection of transmitted data files forms passive attacks. The motive is to guarantee that users sensitive data/information not be disclosed or accessed by an unauthorized person.

Misusage of cloud database: cloud provider provides the unlimited network access, and limited storage cost or sometimes they offer a free trial that may result in different harms on cloud infrastructure [62, 63].

Malicious insider attacks: Basically, the cloud provider may not disclose their data access to resources which helps the hacker to access the data [64].

Data Proliferation: Several organizations involve data-proliferation but un-managed and uncontrolled by the data owner. Retailers are worried about the usage of duplicate data on several data centers. This causes the complexity to find that duplicate data or its backup files are not saved in certain authority; all such duplicate files are removed if such kind of request is made [63].

Dynamic-Provision: In cloud storage system, the user can store their private or secret data files, but there is no responsibility for protection of that file. Thus, there is a necessity of dynamic-provisioning of data in cloud system [65].

## 7. Open Research Issues

In this examine have discussed special security and privacy related methods and their programs. From the survey, a study has located some open studies challenges in cloud storage safety and its privacy are highlighted as underneath:-

A. Possibilities:- The look at [66] want sincere, cooperative service with cloud companies but we by no means one hundred% accept as true with on cloud carrier companies considering there are masses of demanding situations toward mi-susing of users secrete records files. So security of cloud garage device must be independent of provider vendors. The [67] pro-posed technique fails to use practically, and technique of [68] is most effective theoretical method so mythology need to be sensible sufficient to work. The designed framework have to solve all security and privacy-related troubles due to the fact several strategies [68-71] best centered and labored on specific demanding situations.

B. Possible techniques: - In [72], the proposed framework offering the greater protection and privacy of users sensitive statistics inside the cloud storage gadget the use of multitenant cloud surroundings. As a end result, this model stronger the safety stage which is offered through splitting statistics into multiple chunks of files and stores the ones documents into a couple of machines to beautify the safety as well as privateness. Formatting necessities is to apply this file as a template and genuinely type your textual content into it.

## 8. Conclusion

Nowadays, cloud computing is the key technology which acquireing more advancement and reputation for the users, organizations as well as authorities, and so on. This survey study offers an perception of different threats on cloud infrastructure with respect to protection & privateness of customers secrete data. Different procedures have proposed by means of researchers to tackle the problems exploiting special methodologies like cryptographic-based and non-cryptographic based which facilitates to lessen or solve the troubles over the cloud security and statistics privateness within the cloud environment. We have discussed cloud protection model observed by current approaches to reduce the cloud safety and records privateness troubles absolutely. Additionally, highlighted the related challenges towards cloud garage security and customers records privateness. Also, discover some open studies issues to work on.

## References

[1] S. Basu *et al.*, "Cloud computing security challenges & solutions-A survey," *2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC)*, Las Vegas, NV, 2018, pp. 347-356.

[2] Marinescu, Dan C. “Chapter-1 *Cloud computing: theory and practice*. Morgan Kaufmann," 2017. Science Direct. https://doi.org/10.1016/B978-0-12-812810-7.00001-7

[3] W. C. N. Kaura and A. Lal, "Survey paper on cloud computing security," *2017 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS)*, Coimbatore, 2017, pp. 1-6.

[4] Retrieved from ‘https://www.statista.com/statistics/321215/global-consumer-cloud-computing-users/.

[5] Sun, Yunchuan, et al. "Data security and privacy in cloud computing." *International Journal of Distributed Sensor Networks* 10.7 (2014): 190903.

[6] A. M. El-Zoghby and M. A. Azer, "Cloud computing privacy issues, challenges and solutions," *2017 12th International Conference on Computer Engineering and Systems (ICCES)*, Cairo, 2017, pp. 154-160.

[7] Chatterjee, Rishav, Sharmistha Roy, and U. G. Scholar. "Cryptography in Cloud Computing: A Basic Approach to Ensure Security in Cloud." *International Journal of Engineering Science* 11818 (2017).

[8] Rathore, Bhawani Singh, Anju Singh, and Divakar Singh. "A survey of cryptographic and non-cryptographic techniques for privacy preservation." *Int. J. Comput. Appl* 130 (2015): 13.

[9] Kang, Baoyuan, Jiaqiang Wang, and Dongyang Shao. "Attack on Privacy-Preserving Public Auditing Schemes for Cloud Storage." *Mathematical Problems in Engineering* 2017 (2017).

[10] Somani, Gaurav, et al. "DDoS attacks in cloud computing: Issues, taxonomy, and future directions." *Computer Communications* 107 (2017): 30-48.

[11] Q. Yan, F. R. Yu, Q. Gong and J. Li, "Software-Defined Networking (SDN) and Distributed Denial of Service (DDoS) Attacks in Cloud Computing Environments: A Survey, Some Research Issues, and Challenges," in *IEEE Communications Surveys & Tutorials*, vol. 18, no. 1, pp. 602-622, First quarter 2016.

[12] Al-Anzi, Fawaz S., Sumit Kr Yadav, and Jyoti Soni. "Cloud computing: Security model comprising governance, risk management, and compliance." Data Mining and Intelligent Computing (ICDMIC), 2014 International Conference on. IEEE, 2014.

[13] Zheng, Xufei, and Yonghui Fang. "An ais-based cloud security model." Intelligent Control and Information Processing (ICICIP), 2010 International Conference on. IEEE, 2010.

[14] Ashraf, Salman, et al. "Transparency service model for data security in cloud computing." Computing, Mathematics and Engineering Technologies (iCoMET), 2018 International Conference on. IEEE, 2018.

[15] Tesfamicael, Aklilu Daniel, et al. "Modeling for performance and security balanced trading communication systems in the cloud." (2017).

[16] Lv, Junjie, and JulingRong. "Virtualization Security Risk Assessment for Enterprise Cloud Services Based on Stochastic Game Nets Model." IET Information Security (2017).

[17] Ebrahim, Moshira A., Islam AM El-Maddah, and Hoda K. Mohamed. "Hybrid model for cloud data security using steganography." Computer Engineering and Systems (ICCES), 2017 12th International Conference on. IEEE, 2017.

[18] Wei, Hang, et al. "A New BRB Model for Cloud Security-state Prediction based on the Large-scale Monitoring Data." IEEE Access (2017).

[19] Zhou, Shengli, Lifa Wu, and CanghongJin. "A privacy-based SLA violation detection model for the security of cloud computing." China Communications 14.9 (2017): 155-165.

[20] AIT, Bangalore. "Cloud Computing: Data Security Using RSA."

[21] Pant, Vinay Kumar, Jyoti Prakash, and Amit Asthana. "Three-step data security model for cloud computing based on RSA and steganography." Green Computing and Internet of Things (ICGCIoT), 2015 International Conference on. IEEE, 2015.

[22] Shereek, Balkees Mohamed. "Improve Cloud Computing Security Using RSA Encryption with Fermat's Little Theorem." IOSR Journal of Engineering 4 (2014): 1.

[23] Bansal, VineyPal, and Sandeep Singh. "A hybrid data encryption technique using RSA and Blowfish for cloud computing on FPGAs." Recent Advances in Engineering & Computational Sciences (RAECS), 2015 2nd International Conference on. IEEE, 2015.

[24] Arora, Rachna, Anshu Parashar, and Cloud Computing Is Transforming. "Secure user data in cloud computing using encryption algorithms." International journal of engineering research and applications 3.4 (2013): 1922-1926.

[25] Arora, Rachna, Anshu Parashar, and Cloud Computing Is Transforming. "Secure user data in cloud computing using encryption algorithms." International journal of engineering research and applications 3.4 (2013): 1922-1926.

[26] Chennam, Krishna Keerthi, Lakshmi Muddana, and RajaniKanthAluvalu. "Performance analysis of various encryption algorithms for use in multistage encryption for securing data in the cloud." Recent Trends in Electronics, Information & Communication Technology (RTEICT), 2017 2nd IEEE International Conference on. IEEE, 2017.

[27] Bakhtiari, Majid, Majid Nateghizad, and Anazida Zainal. "Secure Search Over Encrypted Data in Cloud Computing." Advanced Computer Science Applications and Technologies (ACSAT), 2013 International Conference on. IEEE, 2013.

[28] Gampala, Veerraju, SrilakshmiInuganti, and Satish Muppidi. "Data security in cloud computing with elliptic curve cryptography." International Journal of Soft Computing and Engineering (IJSCE) 2.3 (2012): 138-141.

[29] Puri, Neha A., Ajay R. Karare, and Rajesh C. Dharmik. "Deployment of the application on Cloud and enhanced data security in

Cloud computing using ECC algorithm." Advanced Communication Control and Computing Technologies (ICACCCT), 2014 International Conference on. IEEE, 2014.

[30] Bansal, Akanksha, and Arun Agrawal. "Providing security, integrity, and authentication using ECC algorithm in cloud storage." Computer Communication and Informatics (ICCCI), 2017 International Conference on. IEEE, 2017.

[31] Kanna, G. Prabu, and V. Vasudevan. "Enhancing the security of user data using the keyword encryption and hybrid cryptographic algorithm in the cloud." Electrical, Electronics, and Optimization Techniques (ICEEOT), International Conference on. IEEE, 2016.

[32] Nagalakshmi, N., and S. Rajalakshmi. "Enabled security based on elliptic curve cryptography with optimal resource allocation schema in cloud computing environment." Computing, Communication and Information Systems (NCCCIS), 2015 IEEE Seventh National Conference on. IEEE, 2015.

[33] Hiremath, Shivarajkumar, and Sanjeev Kunte. "A novel data auditing approach to achieve data privacy and data integrity in cloud computing." Electrical, Electronics, Communication, Computer, and Optimization Techniques (ICEECCOT), 2017 International Conference on. IEEE, 2017.

[34] Schwab, David, et al. "A Secure Mobile Cloud Photo Storage System." Computer Communication and Networks (ICCCN), 2017 26th International Conference on. IEEE, 2017.

[35] Patil, Nilesh R., and Rajesh Dharmik. "Secured cloud architecture for cloud service provider." Futuristic Trends in Research and Innovation for Social Welfare (Startup Conclave), World Conference on. IEEE, 2016.

[36] Timothy, DivyaPrathana, and Ajit Kumar Santra. "A hybrid cryptography algorithm for cloud computing security." Microelectronic Devices, Circuits, and Systems (ICMDCS), 2017 International conference on. IEEE, 2017.

[37] Lei, Sun, Dai Zishan, and Guo Jindi. "Research on key management infrastructure in cloud computing environment." Grid and Cooperative Computing (GCC), 2010 9th International Conference on. IEEE, 2010.

[38] Sriprasadh, K., and O. Pandithurai. "A novel method to secure cloud computing through multicast key management." Information Communication and Embedded Systems (ICICES), 2013 International Conference on. IEEE, 2013.

[39] Wang, Yan, Zhi Li, and Yuxia Sun. "Cloud computing key management mechanism for cloud storage." (2015): 4-4.

[40] Cheng, Yingye, Hao Li, and Nan Zhang. "Character-based online key management in cloud computing environment." Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC), 2016 IEEE. IEEE, 2016.

[41] Gellman R (2009). WPF REPORT: Privacy in the clouds: Risks to privacy and confidentiality from cloud computing.

[42] Xiao Z, and Xiao Y. Security and Privacy in Cloud Computing, IEEE Communications Surveys & Tutorials, vol PP(99), 1–17.

[43] Wang J, Zhao Y et al. (2009). Providing Privacy preserving in cloud computing, International Conference on Test and Measurement, vol 2, 213–216.

[44] Greveler U, Justus b et al. (2011). A Privacy Preserving System for Cloud Computing, 11th IEEE International conference on Computer and Information Technology, 648–653.

[45] Zhou M, Mu Y et al. (2011). Privacy-Preserved Access Control for Cloud Computing, International Joint Conference of IEEE TrustCom-11/IEEE ICESS-11/FCST-11, 83–90.

[46] Chadwick D W, and Fatema K (2012). Privacy-preserving authorization system for the cloud, Journal of Computer and System Sciences, vol 78(5), 1359–1373.

[47] Sayi T J V R K M K, Krishna R K N S et al. (2012). Data Outsourcing in Cloud Environments: A Privacy Preserving Approach, 9th International Conference on Information Technology- New Generations, 361–366.

[48] Rahaman S M, and Farhatullah M (2012). PccP: A Model for Preserving Cloud Computing Privacy, International Conference on Data Science & Engineering (ICDSE), 166–170.

[49] Waqar A, Raza A et al. (2013). A framework for reservation of cloud users' data privacy using the dynamic reconstruction of metadata, Journal of Network and Computer Applications, vol 36(1), 235–248.

[50] Wang C, Wang Q et al. (2010). Privacy-Preserving Public Auditing for Storage Security in Cloud Computing, Proceedings IEEE INFOCOM'10.

[51] M.A. Shah, M. Baker, J.C. Mogul, and R. Swaminathan, "Auditing to Keep Online Storage Services Honest," Proc. 11th USENIX Workshop Hot Topics in Operating Systems (HotOS '07), pp. 1-6, 2007.

[52] Huang, R., Yu, S., Zhuang, W., & Gui, X. 2010. Design of privacy-preserving cloud storage framework. In Grid and CooperativeComputing (GCC), 2010 9th International Conference on (pp. 128-132). IEEE

[53] Huang, Z., Li, Q., Zheng, D., Chen, K., & Li, X. 2011, December. YI Cloud: Improving user privacy with secret key recovery in cloud storage. In Service Oriented System engineering (SOSE), 2011 IEEE 6th International Symposium on (pp. 268-272). IEEE.

[54] Fan, C. I., & Huang, S. Y. 2012. Controllable privacy preserving search based on symmetric predicate encryption in cloud storage.Future Generation Computer Systems.

[55] Ruj, S., Stojmenovic, M., & Nayak, A. 2012, May. Privacy Preserving Access Control with Authentication for Securing Data in Clouds. In Cluster, Cloud and Grid Computing (CCGrid),12th IEEE/ACM International Symposium on(pp. 556-563). IEEE.

[56] Wang C, Chow S S M et al. (2013). Privacy-Preserving Public Auditing for Secure Cloud Storage, IEEE Transactions on Computers, vol 62(2), 362–375.

[57] Munir, K., Palaniappan, S.: Security threats/attacks present in cloud environment. IJCSNS 12(12) (2012)

[58] Mahmood, Z.: Data Location and Security Issues in Cloud Computing. In: IEEE International Conference on Emerging intelligent Data and Web Technologies (2011)

[59] Attas, D., Batrafi, O.: Efficient integrity checking technique fro securing client data in cloud computing. IJECS-IJENS 11(5) (2011)

[60] Arockiam, L., Parthasarathy, et al.: Privacy in Cloud Computing: Survey. CS&IT (2012)

[61] Sharma, P., Sood, S.K., Kaur, S.: Security Issues in Cloud Computing. In: Mantri, A., Nandi, S., Kumar, G., Kumar, S. (eds.) HPAGC 2011. CCIS, vol. 169, pp. 36–45. Springer, Heidelberg (2011)

[62] Top Threats to the Cloud Computing V1.0, Cloud Security Alliance, http://www.cloudsecurityalliance.org/topthreats/2010

[63] Babu, J., Kishore, K., Kumar, K.E.: Migration from Single to Multi-Cloud Computing. International Journal of Engg. Research and Tech. 2(4) (April 2013)

[64] Munir, K., Palaniappan, S.: Secure Cloud Architecture. ACIJ 4(1) (2013)

[65] Chen, D., Zhao, H.: Data Security and Privacy Protection Issues in Cloud Computing. In: IEEE International Conference on Computer Science and Electronics Engineering (2012)

[66] Miranda, M., Pearson, S.: A Client-based Privacy Manager for cloud Computing. In: Proceeding of the Fourth International ICST Conference on Comm. and Middleware, COMSWARE 2009 (2009).

[67] Gentry, C.: Fully Homomorphic encryption using ideal lattices. In: STOC, pp. 169–178 (2009)

[68] Li, X., He, J., Zhang, T.: A Service-Oriented Identity Authentication Privacy Protection Method in Cloud computing. International Journal of Grid and Distributed Computing 6(1) (February 2013)

[69] Mishra, R., Dash, S., Mishra, D.: Privacy-preserving Repository for securing data across the Cloud. IEEE (2011)

[70] Stolfo, S.J., Salem, M.B., Keromytis, A.D.: Fog Computing: Mitigating Insider Data Theft Attacks in Cloud. In: IEEE CS Security and Privacy Workshop (2012)

[71] Gampala, V., Inuganti, S., Muppidi, S.: Data Security in Cloud Computing using Elliptic Curve Cryptography. International Journal of Soft Computing and Engg 2(3) (July 2012)

[72] Bohli, J.M., Gruschka, N., Jensen, M., Iacono, L.L., Marnau, N.: Security and Privacy- Enhancing Multi-cloud Architectures. IEEE Transactions on Dependable and Secure Computing 10(4) (July/August 2013)