International Journal of Data Informatics and Intelligent computing (IJDIIC)
Vol. 1, No. 2, December 2022, pp. 23~33
DOI: 10.59461/ijdiic.v1i2.33

A Review on Cloud Data Security Challenges and existing Countermeasures in Cloud Computing

Prabhdeep Singh[1], Ashish Kumar Pandey[2]
[1]School of Computer Applications, BBD University, Lucknow, India
[2]Computer Science and Engineering, Dr. R.M.L. Avadh University, Ayodhya, India

Article Info

Article history:

Received November 17, 2022
Revised December 13, 2022
Accepted December 16, 2022

Keywords:

Cloud computing (CC)
Privacy issues
Data security data encryption
Data obfuscation

ABSTRACT

Cloud computing (CC) is among the most rapidly evolving computer technologies. That is the required accessibility of network assets, mainly information storage with processing authority without the requirement for particular and direct user administration. CC is a collection of public and private data centers that provide a single platform for clients throughout the Internet. The growing volume of personal and sensitive information acquired through supervisory authorities demands the usage of the cloud not just for information storage and for data processing at cloud assets. Nevertheless, due to safety issues raised by recent data leaks, it is recommended that unprotected sensitive data not be sent to public clouds. This document provides a detailed appraisal of the research regarding data protection and privacy problems, data encrypting, and data obfuscation, including remedies for cloud data storage. The most up-to-date technologies and approaches for cloud data security are examined. This research also examines several current strategies for addressing cloud security concerns. The performance of each approach is then compared based on its characteristics, benefits, and shortcomings. Finally, go at a few active cloud storage data security study fields.

Corresponding Author:

Ashish Kumar Pandey
Computer Science and Engineering
Dr. R.M.L. Avadh University
Ayodhya
India
Email: ashishkpandey9@gmail.com

1. INTRODUCTION

Consumers can store data remotely in that cloud for a variety of applications using the new concept known as CC, which has abundant computing power [1]. Microsoft Azure, Amazon's Elastic Compute Cloud, and other third-party cloud computing platforms all provide data support, computational administration, and internet services [2, 3]. They aren't always cost-effective, but also can provide a high degree of flexibility, allowing network operators to gradually move their information to the cloud. Organizations acknowledge the benefits and importance of sharing data wealth across several datasets. The amount of confidential and valuable information recorded and maintained in the digital library through multiple government & non-governmental entities is continually expanding [4].

Over the latest days, a variety of data mining algorithms have been used on CC to aid in analysis. Such strategies have been used to extract hidden data from huge databases and present this in the development of special hypotheses, patterns, and themes [5, 6]. Nevertheless, the private details of any people must be secured throughout data mining for reasons of security. Several businesses are moving at least a few of their computer technology towards the cloud, including everything from information storage through e-mail and certain other productivity tools. The primary factors supporting this transition include lower prices, without the need for upkeep, nearly infinite processing capabilities, and improved availability. However, security & privacy concerns remain major challenges to a more rapid move to the cloud [7].

Unrestricted data store capacity, accessible, secure, as well as effective document availability including offline recovery, and low price of use are all profits of cloud storing [8]. In real situations, cloud storage may be classified into the following classes [9, 10]: public cloud storage, personal cloud storage, private cloud storage, mixed cloud storage, and mutual cloud storage. Enterprises outsource data storage to cloud storage providers in the public cloud, eliminating the need to construct architecture and operate servers. Just authorized persons have access to the data. [11] Medium & small industries are harassed by the gains of public cloud that contain adaptability, scalability, and cost benefits. Personal cloud often termed mobile cloud storage, seems to be a subset of the public cloud, and it varies in that it offers public cloud services to particular customers.

Enterprises must establish cloud storage facilities and hire skilled staff to administer and manage servers in the private cloud [12]. It assures that the private cloud is higher safety than the public cloud and that the organization keeps control over its data. Nevertheless, the cost increases considerably. This storage approach is well-suited to big industries with a bunch of valuable & sensitive information. A mixed cloud merges the gains of both public & private clouds [13]. Private clouds may be employed to accumulate expensive and critical information, whereas public clouds could be used to keep additional data. The status of this storage option is rising. Mutual cloud, being a relatively new cloud storage format in the latest days, is well-suited to the financial and health sectors. [14] Mutual cloud delivers cloud services to a group of enterprises in a certain area. Naturally, those industries share comparable issues or have the desire to team up on certain tasks. Sever & infrastructure management is performed in-house or outsourced to a 3rd person via mutual cloud participants.

Although cloud storage has been around for a long time, this is still vital throughout the IoT, smart cities, and electronic business. The significance of data protection and privacy preservation for cloud storage remains high, prompting us to write this report. Give a complete analysis of the research on issues related to data privacy and security, data encryption techniques, and solutions for cloud storage systems. The following are the article's central themes:

- To analyze data privacy and security challenges as well as strategies with cloud storage systems in depth.
- A summary of data encryption technology including protection strategies is provided. The security needs have already been highlighted them.
- Go through a few typical data protection research concerns concerning cloud storage before you wrap up.

2. DATA PROTECTION NEEDS REGARDING CLOUD STORAGE

Data Confidentiality: Data confidentiality means preventing uninvited entities from actively attacking consumer information and providing that the collected dataset by the data receiver was consistent with the data given by the transmitter. [15] That would be to say; just authenticated users have access to and get the information. Consider your checking account [18]. Users must be able to receive it, and so should workers at the banks who are assisting them with a payment, and no one else can. Data confidentiality is irreversibly destroyed once it has been acquired by others.

Data Integrity: Data integrity assigns to the data's consistency, or truth that it can't be altered with or substituted at will [16, 17]. For instance, while purchasing on Amazon, anybody might change the items in the account without the owner's consent. Data integrity concerns could be extremely dangerous to our privacy.

Data Availability: Data availability relates to the capability to get information in the cloud at any moment, i.e., users can access, upload, or modify information in the cloud whenever they need it [19]. Access Control on a Fine-Grained Structure [20]. Transferring information in such a dynamic community in a safe way [21].

Completely Data Deletion: [22] Rather than being duped by malevolent cloud providers, customers may erase the information transferred to the cloud platform and keep the data already demolished when they no longer utilize cloud services.

Privacy Protection: Although customers appreciate the ease of cloud storage, cloud storage companies have collected critical information such as personal identification and position for the company [23]. Privacy security techniques are employed to ensure that such data remain private in the face of interested opponents and malevolent cloud provider agents.

It is becoming increasingly hard to protect the information in the cloud when data centralization & quantity grow [24]. As a result, cloud providers and academics would be concerned for a long period as to how to guarantee that customers with their digital materials aren't revealed. Nevertheless, throughout the information age, present data security solutions would no longer match the data security needs, and safety concerns will increasingly become a hurdle inhibiting the advancement of digitalization. In truth, information storage assurance in cloud storage involves both static and dynamic data security [25]. Static data security refers to the protection of static data on a cloud storage system, whereas dynamic storage safety refers to the validity and privacy of the data when it is being transmitted.

Because data are transported over an Internet protocol in the public cloud, security issues that present on conventional networks, like data loss, data breaches, data manipulation, denial of service, etc, impact secure data storage. Customers' information could be dispersed across several servers inside the cloud storage, so each server could be accessed by different customers, raising the danger of illegal access. Complex encryption techniques are not pleasant to individuals with limited resources, therefore ensuring that they can work according to their gadgets is a real concern [26]. Furthermore, the likelihood of a side-channel assault on a user's device must be extremely high.

2.1. Problem statement

Secret information may be gleaned from a distributed system's cache using "side-channel attacks," as discussed in the related paper. This kind of attack often involves the attacker accessing the L3 cache. Information might be stolen without the victim's awareness. The current defenses are insufficient since they do not prevent assaults in real-time. If the hypervisor is breached, then sensitive information stored in guest virtual machines will be exposed. The results presented motivate more research into the field to develop more effective countermeasures. The hypervisor is a critical component in making virtualization a reality. However, as shown, hypervisor vulnerability leads to a variety of attacks, including remapping and duplicate mapping, both of which may result in the loss of sensitive data. Live VM migration is the cutting-edge technology at the heart of cloud computing's potential for superior resource management. However, this opens the door to a wide variety of assaults, such as multi-resource denial-of-service attacks (which were studied in). As a result, there needs to be more research was done that takes a more all-encompassing approach to secure virtual machines from threats.

3. PRESENT SAFETY SOLUTIONS

The security of data becomes compromised once it is transferred to the cloud. Encryption is indeed a useful tool for ensuring data protection [28]. The objective of encrypting data would be to use techniques to convert a plaintext file or information into a sequence of unknown code, which would be known as ciphertext. Once someone hijacks the garbled message, he or she will be unable to decipher the unique content, successfully protecting the data's anonymity and preventing tampering [27]. Users with access may decode the data using the private key associated with that as well, and change or alter the ciphertext. Figure 1 depicts the data security process in a cloud environment.

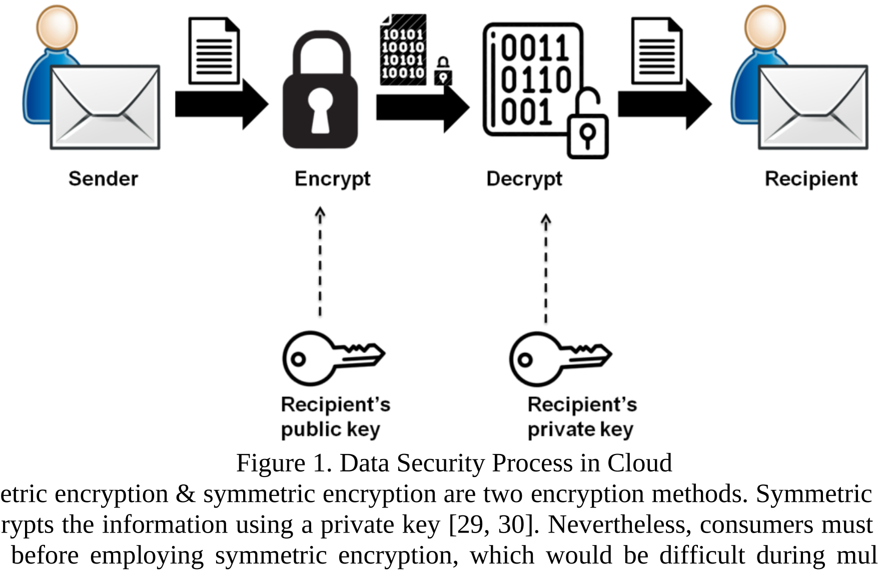

Figure 1. Data Security Process in Cloud

Asymmetric encryption & symmetric encryption are two encryption methods. Symmetric encryption encrypts and decrypts the information using a private key [29, 30]. Nevertheless, consumers must first select a consensus key before employing symmetric encryption, which would be difficult during multi-user file transfers. Asymmetric encryption often referred to as public key encryption, seems to be more efficient in contrast. Pair of keys are used in public key encryption [31]. The public key is employed to encode the data and it can be exchanged with others, whereas the private key has been used to decipher the ciphertext. We'll go through some encryption mechanisms which are commonly used in cloud storage systems under this part. Table 1 depicts the strategies with benefits and limitations.

3.1. Identity-based Encryption (IBE)

IBE is indeed a public key technology in which a private key generator produces a master key pair as well as a master private key, with the master public key being generated using the customer's specific data [32]. By obtaining the private key associated with their identification from the private key generator, the user accesses the file. Not only does the Private Key Generator produce private keys, and that also verifies the identity of the user [33]. The fundamental disadvantage of IBE is that it requires faith in the private key generator, which contains all private keys and should be kept available.

3.2. Role-based model

Before saving information in the cloud, the data holder encodes the information locally and afterward stores the encoded information in the cloud [34, 35]. Data consumers are unable to easily access data stored in the cloud. Responsibilities and roles are allocated to every user. The responsibilities and qualifications are used to allocate roles. The authorized persons have certain roles that grant them access to the information. Various tasks were assigned to the customers, but every role has permission to access them. A role manager's job is really to provide a role to a customer and subsequently withdraw that role if the customer leaves the company. If the Cloud Provider, customers, and others are not allocated the correct roles, they will not be permitted to see the information. If an illegal customer is discovered, the data holder may remove the role.

3.3. Attribute-based encryption (ABE)

The data holder encoded the information in their local computer before placing this in the cloud, as well as the data user decoded it [36]. A combination of features is considered user identification inside an attribute-based encryption process and is used during encryption and decryption processes. The trusted agent creates keys for both the data holder and the consumer. It produces a key based on the customer's properties. The customer's public key & master key would be generated by the trustworthy agent. The data owner really must encrypt the message with the customer's public key, as well as the customer's private key will be used to decrypt the message.

This approach has two benefits: 1) it reduces internet connection expense, and 2) it provides fine-grained permissions [37]. The data holder should be using the authenticated user public key to encrypt the message, which is a drawback of this approach. The access policy was split into 2 structures based on attribute-based encryption: key policy attributes-based encryption as well as ciphertext-policy attributes-based encryption.

3.4. Key policy-ABE (KP-ABE)

The ciphertext is typically related to several characteristics in key policy-ABE; the Private Key, which would be granted by a trustworthy source, and related to an authentication scheme that looks like a tree and represents the identity of the user [38]. However, if the access policy throughout the private key matches the characteristics as in ciphertext, then the user will receive that data.

The customer key was issued by a trustworthy source, defined as such, encrypted data is labeled with a variety of features and certain types of encrypted information may be decoded using access rules. The disadvantage of the KP-ABE technique would be that the data holder has no idea who could decode the information. That's not suited for certain applications since the data user wishes to believe the key provider. An additional drawback is the lack of scalability when it comes to interacting with various degrees of attribute authority. To address this problem, we're switching to ciphertext policy–attribute encryption.

3.5. Ciphertext policy-based ABE (CP-ABE)

The private key gets related to several characteristics in CP-ABE, as well as a ciphertext is constructed with an access structure to determine the encrypting policy [39]. The ciphertext could only be decrypted if indeed the characteristics inside the private key match the access tree given within the ciphertext. The authority manages attribute maintenance & key exchange throughout the CP-ABE framework. The data holder establishes the access policy as well as encrypts data using it. Every client receives a security code based on their characteristics. In this case, the data holder has the final say over the encryption policy.

3.6. Hierarchical Attribute-based Encryption (HABE)

Hierarchical-IBE (HIBE) & CP-ABE are combined in HABE. It supports complete deputation with fine-grained attribute access control. One-to-many encryption is supported [37]. A customer and most of their close relatives may decode an encrypted message with their private keys. Inside the HIBE scheme, HABE has the feature of hierarchical key generation, while in the CP-ABE scheme; it has the feature of adaptable network access.

3.7. Hierarchical attribute-set-based Encryption (HASBE)

Regarding cloud services, the HASBE system is used to manage accessibility [40]. HASBE is a CP-ASBE modification, or perhaps an ASBE method with such a hierarchy organization of users of the system, for scalable, adaptable, and fine-grained data access. Every data source seems to have several characteristics connected with that as well, but every customer has an expressive access structure assigned to them. To cope with customer revocation more effectively than previous systems, HASBE leverages multiple value allocations for access expiry. By employing their unique private key, the customer may decrypt the message. Those domain authorities keep track of consumers' approval of the right key. The higher-level authority offers a master key to govern data held by the lower-level authority.

Imposing data-attribute-based access controls on the one hand, and allowing the data holder to transfer almost all of the computational tasks needed in fine-grained access control towards untrustworthy servers without revealing the underlying data files on another. Achieve this using method that combines proxy re-encryption, lazy re-encryption, and linking ABE. By relating an allocation algorithm to ASBE, the HASBE approach fully incorporates a hierarchy organization of scheme users. Because of various value allocations of characteristics, HASBE preserves compound characteristics, allowing for quick user revocation.

Numerous ABE-based approaches have difficulty implementing complicated access policies. The trusted authority is responsible for formulating and disseminating system variables including root master keys, and also approving top-level domain authority. The key was distributed by domain authority to sub-domain authority or customer. A key format is provided to every customer that provides the characteristic linked with the decryption key. The downside of this strategy is that determining a unique access pattern for every customer requires a significant amount of processing.

3.8. Multi-authority

Numerous authorities issued the characteristics to customers, and the data holder shared the data defined over characteristics from various authorities utilizing access control policy [41]. Multi-authority CP-ABE seems to be more important for information access control. Customers' characteristics could be changed dynamically using this strategy. Additional characteristics could be assigned to a customer, or existing characteristics could well be canceled, and access requests must be adjusted accordingly. Every data holder divides the information into various sections before encoding it, and every section is encrypted with content keys employing symmetric encryption algorithms. The owner next creates access policies for characteristics from several attribute authorities & encodes the content keys following the policies. Once the information has been encoded, the ciphertext is sent to the cloud service. The service has the choice of accessing information, as well as the Customer may decrypt the message if but only if the customer characteristics meet the ciphertext's access control policy.

Table 1. Techniques with their benefits and limitations

S. No.	Solutions	Description	Benefits	Limitations
1.	IBE [32, 33]	IBE develops a public key for every party based on the identification. The private key is generated by a trusted 3rd party. The master public key is generated by the public key generator, and everybody can determine the private key by incorporating the master public key as well as the identification policy, which allows the consumer to decrypt the text. This strategy is beneficial when pre-distribution of an authorized secret key becomes impossible but key distribution among customers is not required.	• Makes the encoding procedure less complicated. • There are no certificates required. • There is no need to register ahead of time. • Because keys have an expiration date, they do not have to be canceled. When a key is adjusted inside a classical public-key system, it should be canceled.	• There must be safe communication between the customer and the private key generator. • Because PKG retains all private keys and should stay accessible, it requires a high degree of confidence. • Because encrypted data is just decoded through one known user, there is no advanced information sharing.
2.	ABE [36, 37]	As per characteristics, the attribute authority creates a	• Cut down on the amount of cost it	For data encryption, the data holder must

		public key as well as a master key. The encryption is done using a public key as well as a collection of meaningful characteristics by the data holder. A data holder decodes the encrypted information using his private key, which he receives from authority and afterward obtains the information they required.	takes for people to communicate. - Offer fine-grained access control. - ABE's collusion resistance is indeed a vital security thing.	employ the public key of every authenticated person.
3.	KP-ABE [38]	Data are encrypted & stored with the help of particular attributes, but only customers who have all of those attributes can decode them. Ciphertexts are accompanied by several descriptive characteristics inside the KP-ABE method, as well as the trustworthy attribute authority delivers a private key to the customer that retains a policy that defines which types of ciphertexts the key may decode.	- The customer cancellation key is simple to manage. - It is made for one-to-many interaction. - Accomplish fine-grained access control. - Greater management over customers than the ABE method.	The data holder has no control over who can decode the information. Since the data holder must accept the key sender, this is not appropriate for certain applications.
4.	CP-ABE [39]	Access formation upon ciphertext is called ciphertext policy. This approach will make information private even though the memory server was untrustworthy. Whenever a data holder encodes a communication in the CP-ABE method, the ciphertext contains a specified access policy that dictates who could decode the encrypted information.	The drawback of KP-ABE was addressed in CP-ABE, thus access control throughout the actual world is supported.	The user combines all attributes in a single set issued in their keys to satisfy policies.
5.	Role-based model [34, 35]	The data controller encodes the information in the cloud using a defined encryption policy & grants access to people with specific roles. There are different types of roles to which customers are allocated, but every role has its permissions.	Greater effective provision, better effective access policy management, and less worker downtime are all reported benefits of this approach. ABE was simple to put up but difficult to handle, but this is mitigated by the use of a role-based encryption approach.	To verify the partial sorting relationship between all these keys, an effective cryptographic methodology is needed.
6.	HASBE [40]	The data holder encrypts the data before sending this to the cloud. The owner may modify the policies of the files by changing the end date. The permissions are provided by the domain authority, as well as the domain authority controls the data holders.	- Lower investment cost. - The new service start-up time has been reduced.	- Lesser operating and preservation expenses. - Failure improvement is a lot simpler.

7.	Multi-authority [41]	This strategy creates a centralized private key and a centralized secret key for such customers. A Central Authority (CA) as well as multiple attribute authorities (AAs) makes up the whole system. Those attribute authorities are in charge of their characteristics. The strategy's major parts include master attribute authorities & consumers. The master's responsibility seems to be to provide private user keys. The customer is authorized by the Attribute Authority, and the customer is given a private attribute key that could be used to decrypt the message. By using an encryption mechanism, the user creates an encrypted message.	• Authorities handle various attribute domains. • Single-authority expressivity, effectiveness, and safety are not inferior. • Nothing can decode ciphertext alone. • The system's advantages include collusion resistance, efficiency, robustness, and adaptability. • The authorities operate autonomously. • Thus, the malfunctions of one authority do not impact the operation of others. This increases system resilience.	The CA may decode each ciphertext, reducing customer privacy and information security. Handling dispersed authorities has an expense.

4. DATA OBFUSCATION APPROACHES

Obfuscation is a way of making information incomprehensible. It's like encryption, and it employs arithmetic or program language [42]. Using an algorithm as well as a key, encryption converts viewable ordinary plain text into unintelligible information. Obfuscated information may be operated without de-obfuscation, while encrypted messages must be decoded first. This method is now widely used for cloud storage data protection. Data obfuscation is divided among categories based on the conversion subject. It removes remarks & style, but sometimes scrambles identifiers.

The next types of control-flow conversions alter the program's control flow whilst keeping the computational capability [43]. Aggregation, rescheduling, and repetitive computing are common transformations. The aggregation conversion combines unrelated computations. Inline/outline approaches and transparent predicates, including loop unrolling are used in an execution. Transparent predicates were helpful for obfuscation because these introduce new ways towards the control flow graph, which a static analysis might not have been able to infer. The two sides of a basic block could be connected by a predicate that always tests to be true.

In this case, the rescheduling operation randomly arranges the expressions, statements, and loops whilst preserving locality. This might be used with the inline & outline approaches. It introduces unnecessary statements and duplicate parameters which do not alter the program's control flow, including such dead-code or extended loop circumstances. This also hides control-flow concepts by converting reducible flow graphs into non-reducible flow diagrams. Also, certain virtual machine codes can use object-level code patterns without high-level features like table interpretation. Code parallelization & introducing fake activities are also important techniques.

In the third category of transformations, the information itself would be changed (Data Obfuscation). Approaches affecting saving, encryption, aggregation, and sorting. An artificial storing type in both dynamic and static information. Using unusual encoding techniques. The colon can be used to divide parameters, promote scalars to objects, transform static data to processes, and change variable life periods. Convert the data into objects or arrays by rearranging, dividing, collapsing, or combining them. Furthermore, convert scalar variables to arrays and objects; change object inheritance relationships. The attacker is also confused by rearranging arrays as well as objects elements like instance variables or formal variables.

Preventive Transformations are the last category. Comparatively, protective transformations restrict automatic analytical techniques by embedding a fake program within the real program, for instance [44]. The first category is focused on preventive conversion that exploits existing de-compiler/de-obfuscator flaws. This is a security game implementation. Generic inherent preventive transforms aim no particular resources.

Exaggerating data dependencies in loops & control flow. Separate from software approaches, many physical obfuscation strategies function by modifying address spaces, rearranging registers, or replacing machine-level instructions.

5. CLOUD SECURITY CONCERNS AND REMEDIES

Before this part, detailed information regarding cloud security was provided as above mentioned. Table 2 depicts the concerns with cloud security & remedies among various risks of security and table 3 depicts the approaches to protect cloud infrastructure among various risks of security. Figure 2 depicts the security challenges within cloud computing.

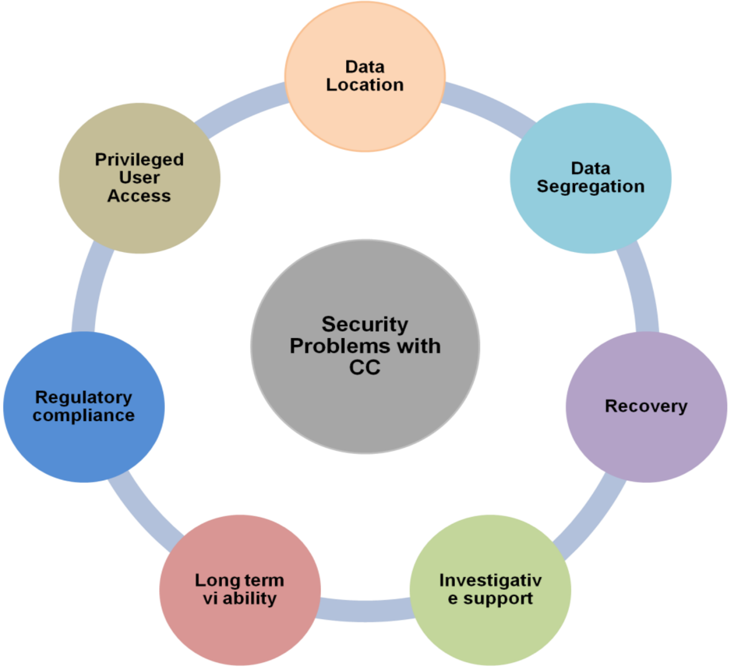

Figure 2. Security problems in cloud computing

Table 2. Concerns with cloud security & remedies [45]

S. No.	Security risk	Remedies
1.	Information outflow	Application programming interface (API) access management must be strictly enforced. Encoding must guarantee the integrity of data while in transmission. Information security must be considered both during planning and construction.
2.	Cloud computing corruption	Improved facility enabling coordination and tracking of debit card scams, facility enabling maintaining public blacklists for own network blocks.
3.	Anxious Interfaces & APIs	Analyze the security strategy of the interfaces properly. Verify that the encoded transfer includes effective access controls & authorization.
4.	Spiteful participants	Supply chain management must be carefully enforced, so as part of formal contracts, human resource needs must be specified. To keep overall security policies and ensure compliance accessibly, it is necessary to maintain openness. It's time to figure out how to notify people when a security incident occurs.
5.	Problems with common technology	When set up, safety must be applied. Environmental action must be constantly supervised. For management and operations, strong authentication & control access must be encouraged. Patching & risk mitigation must be governed by service-level agreements (SLAs). Threat assessments & setup checks must be performed.
6.	Hijacking of account/service	The exchange of account credentials among service providers and customers must be restricted. Wherever practical, two-factor secure authentication

		mechanisms must be used. The illegal activity must be caught as quickly as possible. Security rules & SLAs from cloud providers must be properly known.

Table 3. Approaches to protecting cloud infrastructure [46]

S. No.	Security risk	Solutions
1.	To ensure communication security	Tunneling, including the exploit of virtual circuits.
2.	To keep the servers safe	Distinct servers, storing hashed data, duplication, and a server load limit are all examples of intrusion detection systems (IDSs).
3.	To keep the customer safe	Signatures in the internet age, each writer needs a one-time password and verification. Dispersed Storing, Regional Servers, and Local Disk Short Term Backup
4.	To construct a safe cloud	The cloud infrastructure must be constructed safely, incorporating various characteristics based on the level of protection. Mixing a one-time password as well as a digital signature allows for two-factor verification.

Account information, material, and server data confidentiality must all be protected for cloud technology to be safe [47, 48]. Security aspects always tends to apply in cloud storage data servers as mobile communications are also involved in the cloud applications [49, 50, 51, 52]. Information is stolen both during transfer and while being stored on the server. Cloud computing comes with several safety concerns. This step includes a review of all conceivable cloud security concerns and remedy options.

6. CONCLUSION

A detailed assessment of data protection and privacy preservation for cloud services are provided in this study. First and foremost, cloud technology and cloud storage will continue to be the majority, based on their great contribution throughout the digital world, corporate digitalization, IoT, and certain other industries. Analyze the data protection needs regarding cloud storage and then examine the current safety solutions also. Furthermore, data obfuscation approaches were described for cloud storage. Cloud security concerns and remedies were illustrated as tabular formation regarding security risks.

REFERENCES

[1] Tabrizchi, H. and Kuchaki Rafsanjani, M., 2020. A survey on security challenges in cloud computing: issues, threats, and solutions. The journal of supercomputing, 76(12), pp.9493-9532.

[2] Shakarami, A., Ghobaei-Arani, M., Masdari, M. and Hosseinzadeh, M., 2020. A survey on the computation offloading approaches in mobile edge/cloud computing environment: a stochastic-based perspective. Journal of Grid Computing, 18(4), pp.639-671.

[3] Bokhari, M.U., Makki, Q. and Tamandani, Y.K., 2018. A survey on cloud computing. In Big Data Analytics (pp. 149-164). Springer, Singapore.

[4] Basu, S., Bardhan, A., Gupta, K., Saha, P., Pal, M., Bose, M., Basu, K., Chaudhury, S. and Sarkar, P., 2018, January. Cloud computing security challenges & solutions-A survey. In 2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC) (pp. 347-356). IEEE.

[5] Sarkar, A., Bhattacharya, A., Dutta, S. and Parikh, K.K., 2019. Recent trends of data mining in cloud computing. In Emerging Technologies in Data Mining and Information Security (pp. 565-578). Springer, Singapore.

[6] Rambabu, M., Gupta, S. and Singh, R.S., 2021. Data mining in cloud computing: survey. In Innovations in Computational Intelligence and Computer Vision (pp. 48-56). Springer, Singapore.

[7] Sahmim, S. and Gharsellaoui, H., 2017. Privacy and security in internet-based computing: cloud computing, internet of things, cloud of things: a review. Procedia computer science, 112, pp.1516-1522.

[8] Li, P., Li, J., Huang, Z., Gao, C.Z., Chen, W.B. and Chen, K., 2018. Privacy-preserving outsourced classification in cloud computing. Cluster Computing, 21(1), pp.277-286.

[9] Nachiappan, R., Javadi, B., Calheiros, R.N. and Matawie, K.M., 2017. Cloud storage reliability for big data applications: A state of the art survey. Journal of Network and Computer Applications, 97, pp.35-47.

[10] Yang, P., Xiong, N. and Ren, J., 2020. Data security and privacy protection for cloud storage: A survey. IEEE Access, 8, pp.131723-131740.

[11] Attaran, M. and Woods, J., 2019. Cloud computing technology: improving small business performance using the Internet. Journal of Small Business & Entrepreneurship, 31(6), pp.495-519.

[12] Wang, J., Zhang, W., Shi, Y., Duan, S. and Liu, J., 2018. Industrial big data analytics: challenges, methodologies, and applications. arXiv preprint arXiv:1807.01016.

[13] Vijayakumar, K., Suchitra, S. and Shri, P.S., 2019. A secured cloud storage auditing with empirical outsourcing of key updates. International Journal of Reasoning-based Intelligent Systems, 11(2), pp.109-114.

[14] Li, X., Kumari, S., Shen, J., Wu, F., Chen, C. and Islam, S.K., 2017. Secure data access and sharing scheme for cloud storage. Wireless Personal Communications, 96(4), pp.5295-5314.

[15] Thiel, F. and Wetzlich, J., 2019. The European metrology cloud: impact of european regulations on data protection and the free flow of non-personal data. In 19th International Congress of Metrology (CIM2019) (p. 01001). EDP Sciences.

[16] Chen, Y., Li, L. and Chen, Z., 2017, December. An approach to verifying data integrity for cloud storage. In 2017 13th International Conference on Computational Intelligence and Security (CIS) (pp. 582-585). IEEE.

[17] Tian, J. and Jing, X., 2020. Cloud data integrity verification scheme for associated tags. Computers & Security, 95, p.101847.

[18] El Makkaoui, K., Beni-Hssane, A. and Ezzati, A., 2019. Speedy Cloud-RSA homomorphic scheme for preserving data confidentiality in cloud computing. Journal of Ambient Intelligence and Humanized Computing, 10(12), pp.4629-4640.

[19] Liu, J., Shen, H., Chi, H., Narman, H.S., Yang, Y., Cheng, L. and Chung, W., 2020. A low-cost multi-failure resilient replication scheme for high-data availability in cloud storage. IEEE/ACM Transactions on Networking, 29(4), pp.1436-1451.

[20] Qi, S., Lu, Y., Wei, W. and Chen, X., 2020. Efficient data access control with fine-grained data protection in cloud assisted IIoT. IEEE Internet of Things Journal, 8(4), pp.2886-2899.

[21] Koulouzis, S., Martin, P., Zhou, H., Hu, Y., Wang, J., Carval, T., Grenier, B., Heikkinen, J., de Laat, C. and Zhao, Z., 2020. Time-critical data management in clouds: Challenges and a Dynamic Real-Time Infrastructure Planner (DRIP) solution. Concurrency and Computation: Practice and Experience, 32(16), p.e5269.

[22] Yang, C., Chen, X. and Xiang, Y., 2018. Blockchain-based publicly verifiable data deletion scheme for cloud storage. Journal of Network and Computer Applications, 103, pp.185-193.

[23] Akremi, A. and Rouached, M., 2021. A comprehensive and holistic knowledge model for cloud privacy protection. The Journal of Supercomputing, 77(8), pp.7956-7988.

[24] Mann, Z.Á., Kunz, F., Laufer, J., Bellendorf, J., Metzger, A. and Pohl, K., 2021. RADAR: Data protection in cloud-based computer systems at run time. IEEE Access, 9, pp.70816-70842.

[25] Kumar, G., 2019. A review on data protection of cloud computing security, benefits, risks and suggestions. PDF). United International Journal for Research & Technology, 1(2), p.26.

[26] Russo, B., Valle, L., Bonzagni, G., Locatello, D., Pancaldi, M. and Tosi, D., 2018. Cloud computing and the new EU general data protection regulation. IEEE Cloud Computing, 5(6), pp.58-68.

[27] Masood, A., Lakew, D.S. and Cho, S., 2020. Security and privacy challenges in connected vehicular cloud computing. IEEE Communications Surveys & Tutorials, 22(4), pp.2725-2764.

[28] Mukherjee, S., 2019. Cloud-based Security Solutions. Available at SSRN 3408882.

[29] Abroshan, H., 2021. A hybrid encryption solution to improve cloud computing security using symmetric and asymmetric cryptography algorithms. International Journal of Advanced Computer Science and Applications, 12(6).

[30] Lozupone, V., 2018. Analyze encryption and public key infrastructure (PKI). International Journal of Information Management, 38(1), pp.42-44.

[31] Maqsood, F., Ahmed, M., Mumtaz, M. and Ali, M., 2017. Cryptography: a comparative analysis for modern techniques. International Journal of Advanced Computer Science and Applications, 8(6), pp.442-448.

[32] Unal, D., Al-Ali, A., Catak, F.O. and Hammoudeh, M., 2021. A secure and efficient Internet of Things cloud encryption scheme with forensics investigation compatibility based on identity-based encryption. Future Generation Computer Systems, 125, pp.433-445.

[33] Wei, J., Chen, X., Wang, J., Hu, X. and Ma, J., 2019, September. Forward-secure puncturable identity-based encryption for securing cloud emails. In European Symposium on Research in Computer Security (pp. 134-150). Springer, Cham.

[34] Rahunathan, L., Tamilarasi, A. and Sivabalaselvamani, D., 2018. Efficient and Secure Interoperable Healthcare Information System Using Keyword Searchable and Role-Based Access Control in Cloud Environment. Journal of Computational and Theoretical Nanoscience, 15(4), pp.1176-1181.

[35] Sultan, N.H., Varadharajan, V., Zhou, L. and Barbhuiya, F.A., 2020. A role-based encryption scheme for securing outsourced cloud data in a multi-organization context. arXiv preprint arXiv:2004.05419.

[36] Zhang, Y., Deng, R.H., Xu, S., Sun, J., Li, Q. and Zheng, D., 2020. Attribute-based encryption for cloud computing access control: A survey. ACM Computing Surveys (CSUR), 53(4), pp.1-41.

[37] Huang, K., 2021. Accountable and revocable large universe decentralized multi-authority attribute-based encryption for cloud-aided IoT. IEEE Access, 9, pp.123786-123804.

[38] Zhu, H., Wang, L., Ahmad, H. and Niu, X., 2017. Key-policy attribute-based encryption with equality test in cloud computing. IEEE Access, 5, pp.20428-20439.

[39] Ramu, G., Reddy, B.E., Jayanthi, A., and Prasad, L.V., 2019. Fine-grained access control of EHRs in cloud using CP-ABE with user revocation. Health and Technology, 9(4), pp.487-496.

[40] Ezhilarasi, T.P., Sudheer Kumar, N., Latchoumi, T.P. and Balayesu, N., 2021. A secure data sharing using IDSS CP-ABE in cloud storage. In Advances in Industrial Automation and Smart Manufacturing (pp. 1073-1085). Springer, Singapore.

[41] Challagidad, P.S. and Birje, M.N., 2020. Efficient multi-authority access control using attribute-based encryption in cloud storage. Procedia Computer Science, 167, pp.840-849.

[42] Enireddy, V., Somasundaram, K., Prabhu, M.R. and Babu, D.V., 2021, October. Data Obfuscation Technique in Cloud Security. In 2021 2nd International Conference on Smart Electronics and Communication (ICOSEC) (pp. 358-362). IEEE.

[43] Suguma, R. and Raja, K., 2018. Data Security and Data Privacy in Cloud Computing Environment using Data Obfuscation Technique. International Journal of Advanced Studies in Computers, Science and Engineering, 7(3), pp.24-29.

[44] Naik, C., Siddhartha, M., Martin, J.P. and Chandrasekaran, K., 2019, October. Location Privacy Using Data Obfuscation in Fog Computing. In TENCON 2019-2019 IEEE Region 10 Conference (TENCON) (pp. 1286-1291). IEEE.

[45] Saxena, R. and Gayathri, E., 2021, October. A study on vulnerable risks in security of cloud computing and proposal of its remedies. In Journal of Physics: Conference Series (Vol. 2040, No. 1, p. 012008). IOP Publishing.

[46] Alghofaili, Y., Albattah, A., Alrajeh, N., Rassam, M.A. and Al-rimy, B.A.S., 2021. Secure Cloud Infrastructure: A Survey on Issues, Current Solutions, and Open Challenges. Applied Sciences, 11(19), p.9005.

[47] Mishra, S., Sharma, S.K. and Alowaidi, M.A., 2021. Analysis of security issues of cloud-based web applications. Journal of Ambient Intelligence and Humanized Computing, 12(7), pp.7051-7062.

[48] Wulf, F., Strahringer, S. and Westner, M., 2019, July. Information security risks, benefits, and mitigation measures in cloud sourcing. In 2019 IEEE 21st Conference on Business Informatics (CBI) (Vol. 1, pp. 258-267). IEEE.

[49] S. Saxena, D. Yagyasen, C. N. Saranya, R. S. K. Boddu, A. K. Sharma and S. K. Gupta, "Hybrid Cloud Computing for Data Security System," 2021 International Conference on Advancements in Electrical, Electronics, Communication, Computing and Automation (ICAECA), 2021, pp. 1-8, doi: 10.1109/ICAECA52838.2021.9675493.

[50] Eshrag Refaee, Shabana Parveen, Khan Mohamed Jarina Begum, Fatima Parveen, M. Chithik Raja, Shashi Kant Gupta, Santhosh Krishnan, "Secure and Scalable Healthcare Data Transmission in IoT Based on Optimized Routing Protocols for Mobile Computing Applications", Wireless Communications and Mobile Computing, vol. 2022, Article ID 5665408, 12 pages, 2022. https://doi.org/10.1155/2022/5665408

[51] Rajesh Kumar Kaushal, Rajat Bhardwaj, Naveen Kumar, Abeer A. Aljohani, Shashi Kant Gupta, Prabhdeep Singh, Nitin Purohit, "Using Mobile Computing to Provide a Smart and Secure Internet of Things (IoT) Framework for Medical Applications", Wireless Communications and Mobile Computing, vol. 2022, Article ID 8741357, 13 pages, 2022. https://doi.org/10.1155/2022/8741357

[52] N. Thangarasu, R. Rajalakshmi, G. Manivasagam, & V. Vijayalakshmi. (2022). Performance of re-ranking techniques used for recommendation method to the user CF- Model. International Journal of Data Informatics and Intelligent Computing, 1(1), 30–38. https://doi.org/10.5281/zenodo.7108931

BIOGRAPHIES OF AUTHORS

Prabhdeep Singh is an assistant Professor at School of Computer Applications department, Babu Banarasi Das University, Lucknow. He pursued B.Tech from Saroj Institute of Technology and Management, Lucknow (U.P.T.U.) and M.Tech CMJ University , Shillong. He is also pursuing Ph.D. (Part Time) from Amity School of Engineering & Technology, Lucknow. He has over 13 years of experience in technical education inclusive one year as a software engineer. He has published numerous research papers in international journals. He has also published two patents. He can be contacted at email: prabhdeepcs@gmail.com

Dr. Ashish Kumar Pandey is an assistant professor in the department of CSE, Institute of Engineering & Technology, Ayodhya. He pursued B.Tech from Dr. R.M.L. Avadh University, Ayodhya. He has completed M.Tech and PhD from Integral University, Lucknow. He has also done Master of Business Management in Marketing and HR from Dr. Abdul Kalam Technical University (former GBTU), Lucknow. He has over 13 years of experience in technical education. He has published various research papers in international journals and at international conferences. He has also published one patent. He can be contacted at email: ashishkpandey9@gmail.com