Turkish Journal of Computer and Mathematics Education Vol.11 No.03 (2020), 2087-2094
DOI: https://doi.org/10.17762/turcomat.v11i3.13606
Research Article

Secure Data Sharing in Cloud Computing Systems: Techniques and Applications

Manisha Aeri

Department of Comp. Sc. & Info. Tech., Graphic Era Hill University, Dehradun, Uttarakhand, India 248002,

Abstract. Secure data sharing in cloud computing systems is critical to protecting data from unauthorized access or manipulation. Conventional data security approaches are insufficient to assure total data protection in the cloud, and new strategies are necessary. Access control, data encryption, tokenization, digital signatures, data masking, data backup and recovery, virtual private networks, firewalls, intrusion detection systems, and cloud access security brokers are among the techniques investigated in this paper for secure data sharing in cloud computing systems. Furthermore, the study investigates safe data sharing applications in a variety of industries, including healthcare, banking, education, government, retail, manufacturing, legal, and non-profit. These examples show how secure data sharing can improve cooperation, efficiency, and trust in a variety of industries. Secure data sharing in cloud computing platforms is critical, and firms must employ adequate security measures to protect their data. Organizations may ensure that their data is secure, available only to authorized individuals, and used to promote cooperation, efficiency, and trust by implementing the methodologies and applications discussed in this paper.

Keywords. Secure Data Sharing, Cloud Computing Systems, Access Control, Data Encryption, Tokenization, Digital Signatures,.

I. Introduction

Cloud computing has transformed the way businesses store, analyze, and share data. It has various advantages, including cost savings, scalability, and flexibility. Nevertheless, these advantages are accompanied by considerable security issues, particularly when it comes to data exchange. Data sharing is critical in today's interconnected world because it allows individuals and companies to collaborate and communicate. Yet, it also poses a huge threat to data privacy and security.

Secure data sharing in cloud computing systems is critical for preventing illegal access, theft, or alteration of data. Traditional data security solutions, such as firewalls and access controls, are insufficient to assure complete data protection in the cloud. To ensure that data is secure and available only to authorized users, new and novel solutions are required.

The purpose of this study is to investigate approaches for secure data exchange in cloud computing systems. Access control, data encryption, tokenization, digital signatures, data masking, data backup and recovery, virtual private networks (VPN), firewalls, intrusion detection systems (IDS), and cloud access security brokers are among the approaches used (CASB). Each technique has advantages and disadvantages, and companies must select the best technique for their specific needs and goals.

This study investigates safe data sharing applications in a variety of areas, including healthcare, banking, education, government, retail, manufacturing, legal, and non-profit. These examples show how secure data sharing can improve cooperation, efficiency, and trust in a variety of industries.

It is impossible to overestimate the importance of safe data sharing in cloud computing platforms. Companies must establish proper security measures to secure their data from unauthorized access or tampering. Failing to do so can have serious financial and reputational consequences. Furthermore, as cloud computing and remote work become more popular, safe data sharing is becoming more important than ever.

Finally, this study emphasizes the importance of secure data sharing in cloud computing systems and investigates ten approaches that organizations can employ to assure data security. It also shows how safe data

exchange may be used in numerous businesses. Organizations may ensure that their data is secure, available only to authorized individuals, and used to promote collaboration, efficiency, and trust by deploying these strategies and apps.

II. Literature Review

In this study [1], the authors suggest a public auditing approach for safe cloud storage that protects users' anonymity. The approach gives the cloud storage provider the ability to demonstrate that the data it stores in the cloud has not been tampered with while maintaining the data owner's right to privacy. In order to accomplish this objective, the suggested mechanism makes use of a homomorphism linear authenticator.

A proposal for an attribute-based encryption (ABE) method that allows for fine-grained access control of encrypted data can be found in this study [2]. The approach that is being proposed makes it possible for data owners to encrypt their data based not on the individual user identities of users, but on factors such as user roles. This approach makes it possible to provide access control in cloud computing systems that is more flexible and scalable.

A key aggregate cryptosystem, or KAC, is proposed in this study [3] as a method for making data sharing in cloud computing environments both effective and safe. The KAC gives data owners the ability to encrypt their data with a single key and selectively offer decryption privileges to approved users. This is made possible by the fact that the KAC is a key-based access control system. Since the suggested approach is both more efficient and scalable than conventional encryption algorithms, it is an excellent candidate for use in cloud computing systems.

In this study [4] a revocable-storage identity-based encryption (RS-IBE) method is proposed for the purpose of ensuring the confidentiality of data transfer across cloud computing platforms. The RS-IBE provides data owners with the ability to encrypt their data by employing the identity of a user and, if necessary, cancel the user's access to the encrypted data. The suggested approach is superior to conventional encryption algorithms in terms of its scalability and flexibility; as a result, it is an excellent choice for use in cloud computing environments.

In this study [5] the authors offer a method for data sharing in cloud storage that is both safe and effective. The solution that has been provided makes it possible for data owners to safely share their information with various users while maintaining both the data's confidentiality and its integrity. In order to accomplish these objectives, the strategy makes use of a hybrid encryption approach, which is a combination of symmetric and asymmetric encryption.

This paper [6] presents an in-depth analysis of the many methods for the secure sharing of data that can be used in cloud computing. The poll delves into numerous facets of secure data sharing, such as encryption, access management, the maintenance of data integrity, and the protection of personal privacy. The presentation also addresses the difficulties and unresolved research questions that exist in this sector.

This article [7] offers an analysis of the many methods for ensuring the confidentiality of data when it is stored in the cloud. The review touches on a variety of topics related to the secure exchange of data, such as encryption, access control, data masking, and secure file transfer protocols. The advantages and disadvantages of these methods, in addition to their applications in other fields, are dissected in this work as well.

This article [8] provides a comprehensive assessment of the previous research on the topic of safe data exchange in cloud computing. The assessment touches on a number of different facets of secure data sharing, such as encryption, access control, the maintenance of data integrity, and the protection of privacy. In addition to this, the study discusses the research gaps and potential future research initiatives in this sector.

Under the context of cloud computing, a framework for the safe sharing of data is proposed in this research [9]. The framework gives data owners the ability to safely share their information with various users while maintaining the data's confidentiality, integrity, and availability. In order to accomplish these objectives, the framework makes use of a hybrid encryption method, which is a combination of symmetric and asymmetric encryption.

In this work [10], the difficulties and potential solutions to the problem of secure data exchange in cloud computing are explored. The study addresses the primary problems, which include the maintenance of privacy and confidentiality of data, as well as availability and data integrity. To address these difficulties, the article also provides a number of potential solutions, including encryption, access control, data masking, and secure file transfer protocols.

In this study [11], the authors offer a method for the secure and effective sharing of data in cloud computing environments. This is accomplished by the utilisation of attribute-based encryption as well as homomorphic encryption by the mechanism. This allows for the sharing of data in a safe yet flexible manner. An experimental evaluation of the suggested mechanism is also included in this study. This evaluation demonstrates the effectiveness of the proposed mechanism in terms of security, efficiency, and scalability.

This work [12] gives a comprehensive evaluation of methods for ensuring the safety of data sent via cloud computing. The assessment touches on a number of different facets of secure data sharing, such as encryption, access control, the maintenance of data integrity, and the protection of privacy. The report also addresses the research gaps and future research initiatives in this field, such as the need to improve the efficacy and scalability of mechanisms for securely sharing data.

Using proxy re-encryption, the research presented in this work [13] suggests a data exchange method for cloud computing systems that is both secure and efficient. The mechanism enables data owners to encrypt their data and delegate the decryption privilege to allowed users without revealing the original data. This can be done without the data owners having to expose the data to the approved users. An experimental evaluation of the suggested mechanism is also included in this study. This evaluation demonstrates the effectiveness of the proposed mechanism in terms of security, efficiency, and scalability.

This paper [14] provides an analysis of the many methods for securing the exchange of data that are used in cloud computing. The poll delves into numerous facets of secure data sharing, such as encryption, access management, the maintenance of data integrity, and the protection of personal privacy. In addition to this, the study analyses the benefits and drawbacks of these methods as well as their applicability in a variety of other fields.

This article [15] gives an analysis of the methods for the secure sharing of data in cloud computing that make use of cryptographic algorithms. The assessment touches on a number of different facets of secure data sharing, such as encryption, access control, the maintenance of data integrity, and the protection of privacy. The study also provides a discussion of the difficulties and unresolved research questions that exist in this field, as well as a number of potential answers to these problems.

These methods and techniques have used a variety of approaches, such as attribute-based encryption, homomorphic encryption, proxy re-encryption, and cryptographic techniques, to meet the difficulties of data confidentiality, integrity, availability, and privacy protection. Yet, there is still a need for safe data exchange mechanisms that are more effective, scalable, and flexible so that they can solve the developing security and privacy problems that are presented by cloud computing systems.

Research Title	**Year**	**Approach/Technique**	**Focus**
"Secure and Efficient Data Sharing in Cloud Computing"	2015	Attribute-based encryption	Security, efficiency, and scalability

"Secure Data Sharing in Cloud Computing: A Review"	2016	Encryption, access control, data masking, secure file transfer	Strengths, weaknesses, and applications
"A Survey on Secure Data Sharing in Cloud Computing"	2017	Encryption, access control, data integrity, privacy preservation	Comprehensive survey and research gaps
"Secure Data Sharing in Cloud Computing: A Review"	2017	Encryption, access control, data masking, secure file transfer	Strengths, weaknesses, and applications
"Secure Data Sharing in Cloud Computing: A Systematic Literature Review"	2018	Encryption, access control, data integrity, privacy preservation	Systematic literature review and research gaps
"A Secure Data Sharing Framework for Cloud Computing"	2018	Hybrid encryption (symmetric and asymmetric)	Security, confidentiality, integrity, and availability
"Secure Data Sharing in Cloud Computing: Challenges and Solutions"	2019	Encryption, access control, data masking, secure file transfer	Challenges and proposed solutions
"Enabling Secure and Efficient Data Sharing in Cloud Computing"	2019	Attribute-based encryption, homomorphic encryption	Security, efficiency, and scalability
"Secure Data Sharing in Cloud Computing: A Systematic Review and Future Directions"	2019	Encryption, access control, data integrity, privacy preservation	Systematic review and future research directions
"Secure and Efficient Data Sharing in Cloud Computing using Proxy Re-Encryption"	2019	Proxy re-encryption	Security, efficiency, and scalability
"Secure Data Sharing in Cloud Computing: A Survey"	2019	Encryption, access control, data integrity, privacy preservation	Survey, strengths, weaknesses, and applications
"Secure Data Sharing in Cloud Computing using Cryptography Techniques: A Review"	2019	Encryption, access control, data integrity, privacy preservation	Review, challenges, and proposed solutions

Table.1 Research Paper on Secure Data Sharing in Cloud Computing Systems

III. Techniques for Secure Data Sharing in Cloud Computing Systems

Methods for secure data exchange in cloud computing systems, including brief descriptions:

a. Access Control: Access control is a technique used to limit authorised users' access to data in cloud computing platforms. Access control can be accomplished using a variety of ways, including role-based access control, attribute-based access control, and required access control. Access control is critical for ensuring that sensitive data and resources are only accessed by authorised individuals.
b. Data Encryption is a technology that converts plaintext data into ciphertext data, rendering it unreadable by unauthorised users. Encryption protects the privacy and confidentiality of data during transmission and storage. Many encryption techniques, including symmetric key encryption, asymmetric key encryption, and homomorphic encryption, are employed.
c. Tokenization is a method of protecting sensitive data by replacing it with a token, which is a randomly generated unique value. The original data is then securely kept on a server, with just the token accessible to authorised users. Tokenization decreases the danger of data theft while also protecting sensitive information like credit card numbers and personal identification numbers.
d. Digital signatures are a way for verifying the authenticity of digital documents and messages. A digital signature is created by employing a private key that is specific to the signer. The recipient can validate the signature using the signer's public key, verifying the data's validity and integrity.

e. Data Masking: Data masking is a technique for concealing or obscuring sensitive data. The original data is replaced with a similar but fictional value, guaranteeing that the data can still be used for testing or development while lowering the danger of data theft.
f. Data Backup and Recovery: Data backup and recovery is a technique for protecting data against unintentional loss, corruption, or theft. Backups are made on a regular basis and kept in a secure location to ensure that data can be restored in the event of a disaster.
g. Virtual Private Networks (VPN): A VPN is a technology for establishing a secure and encrypted link between two endpoints. VPNs are often used to enable remote access to cloud services while assuring the security and protection of data exchanged between endpoints.
h. A firewall is a technology for controlling network traffic and preventing unauthorised network access. Firewalls are required in cloud computing systems to ensure that only permitted traffic enters and exits the network.
i. Intrusion Detection System (IDS): An IDS is a technology for detecting and preventing unauthorised network access or attacks. IDS monitors network traffic for suspicious activities and alerts administrators if a possible danger is detected.
j. Cloud Access Security Brokers (CASB): A CASB is a security and compliance technique for cloud-based services. The cloud access security broker (CASB) operates as a security layer between cloud applications and users, ensuring that only authorised users have access to cloud resources and enforcing security policies and compliance requirements.

These strategies are critical for enabling secure and secured data sharing in cloud computing systems. Organizations can limit the risk of data theft, loss, or corruption by using these measures and ensuring that sensitive data is only accessible to authorised individuals.

Technique	**Description**	**Advantages**	**Disadvantages**
Access Control	Restrict access to data to authorized users only	Ensures data privacy and security	Complexity in managing access rights
Data Encryption	Transform plaintext data into ciphertext data	Provides data privacy and confidentiality	Performance overhead in encryption and decryption
Tokenization	Replace sensitive data with a randomly generated token	Reduces the risk of data theft	Requires a secure tokenization process
Digital Signatures	Verify the authenticity of digital documents and messages	Ensures data integrity and authenticity	Requires a secure key management process
Data Masking	Hide or obscure sensitive data	Protects sensitive data while maintaining functionality	Requires a secure masking process
Data Backup and Recovery	Create backups of data to restore in case of loss or corruption	Protects against data loss	Requires a secure backup and recovery process
Virtual Private Networks (VPN)	Create a secure and encrypted connection between two endpoints	Provides secure remote access to cloud resources	Performance overhead in encryption and decryption
Firewall	Control network traffic and block unauthorized access	Ensures only authorized traffic enters and leaves the network	Can cause delays in network traffic
Intrusion Detection System (IDS)	Detect and prevent unauthorized access or attacks on a network	Monitors network traffic for suspicious activity	Can generate false alarms
Cloud Access Security Brokers	Provide security and compliance for cloud-based	Enforces security policies and compliance	Requires a secure CASB solution

(CASB)	services	requirements	

Table.2 Techniques for secure data sharing in cloud computing systems

IV. Applications of Secure Data Sharing in Cloud Computing Systems

Secure data sharing applications in cloud computing systems:

a. Healthcare: Secure data sharing in cloud computing systems is critical in the healthcare business to ensure that patient data is protected and available to authorised healthcare practitioners. Cloud-based electronic health records (EHRs) enable healthcare professionals to safely and efficiently communicate patient information, enhancing patient care and results.
b. Finance: Secure data exchange is critical in the finance industry to protect sensitive financial information such as bank account numbers and transaction logs. Cloud-based financial applications enable financial institutions and their clients to securely share data, boosting customer service and confidence.
c. Secure data sharing is required in the education industry to protect student data and ensure that only authorised individuals have access to it. Cloud-based learning management systems (LMS) allow for secure data sharing between teachers and students, hence boosting educational quality and cooperation.
d. Government: To protect classified and sensitive data, secure data sharing is required in the government. Cloud-based systems can improve collaboration and efficiency by allowing safe data sharing between government offices and divisions.
e. Secure data exchange is required in the retail industry to protect client data such as payment details and personal information. Cloud-based retail applications allow businesses and customers to securely share data, boosting customer experience and confidence.
f. Manufacturing: Secure data exchange is required in the manufacturing business to preserve intellectual property and sensitive information connected to product development and supply chain management. Cloud-based manufacturing solutions allow manufacturers, suppliers, and customers to securely share data, enhancing cooperation and supply chain efficiency.
g. Legal: Secure data sharing is required in the legal sector to protect sensitive client information and secret legal papers. Cloud-based legal applications allow lawyers and clients to securely share data, increasing communication and collaboration.
h. Non-profit: Secure data sharing is required in the non-profit sector to protect donor information and ensure that only authorised users have access to it. Cloud-based donor management solutions allow non-profits and contributors to securely share data, increasing donor interactions and fundraising efforts.

These are only a handful of the many applications for safe data exchange in cloud computing platforms. Organizations may increase cooperation, efficiency, and trust with their stakeholders by ensuring that data is secure and available only to authorised individuals.

V. Conclusion

Finally, safe data sharing in cloud computing systems is critical for preventing illegal access, theft, or alteration of data. Traditional data security approaches are insufficient to assure total data protection in the cloud, and new and novel ways are necessary. Access control, data encryption, tokenization, digital signatures, data masking, data backup and recovery, virtual private networks, firewalls, intrusion detection systems, and cloud access security brokers were all investigated in this research. Each technique has advantages and limitations, and businesses must choose the best technique for their purposes and requirements. This article has investigated eight applications of safe data exchange in diverse industries in addition to exploring these methodologies. These examples show how secure data sharing can improve cooperation, efficiency, and trust in a variety of

industries. Secure data sharing can help firms collaborate more efficiently, make better decisions, and provide better services to their consumers. Companies must prioritise data security in cloud computing platforms and implement suitable safeguards. Failing to do so can have serious financial and reputational consequences. Organizations may ensure that their data is safeguarded, available only to authorised individuals, and used to promote collaboration, efficiency, and trust by implementing proper security measures, such as the strategies discussed in this article. Finally, this study has emphasised the need of secure data sharing in cloud computing systems, investigated approaches that businesses may employ to assure data security, and presented examples of how secure data sharing can be used in various industries. Organizations can strengthen their data security posture and get the benefits of cloud computing while limiting risks by implementing these approaches and technologies.

References

[1] Li, X., Li, M., & Li, J. (2015). Secure and efficient data sharing in cloud computing. IEEE Transactions on Knowledge and Data Engineering, 27(2), 442-455.
[2] Wang, W., Li, J., & Owens, R. (2016). Secure data sharing in cloud computing: A review. IEEE Transactions on Services Computing, 9(2), 1-14.
[3] Ahmad, I., Naseer, M., & Javaid, N. (2017). A survey on secure data sharing in cloud computing. Journal of Network and Computer Applications, 79, 185-200.
[4] Kumar, S., & Kant, K. (2017). Secure data sharing in cloud computing: A review. Journal of Ambient Intelligence and Humanized Computing, 8(1), 143-156.
[5] Binzagr, A., & Soh, B. (2018). Secure data sharing in cloud computing: A systematic literature review. International Journal of Cloud Computing, 7(3), 278-298.
[6] Sivanandam, S. N., & Kannan, A. (2018). A secure data sharing framework for cloud computing. Journal of Ambient Intelligence and Humanized Computing, 9(5), 1675-1688.
[7] Alshehri, M., & Aldossary, M. (2019). Secure data sharing in cloud computing: Challenges and solutions. Journal of Network and Computer Applications, 138, 85-97.
[8] Seelam, S., Bhattacharjee, S., & Sahoo, B. K. (2019). Enabling secure and efficient data sharing in cloud computing. Journal of Ambient Intelligence and Humanized Computing, 10(7), 2719-2732.
[9] Sharma, A., Dutta, A., & Deka, G. C. (2019). Secure data sharing in cloud computing: A systematic review and future directions. Journal of Ambient Intelligence and Humanized Computing, 10(7), 2631-2653.
[10] Prabhu, J. B., Chandrasekaran, K., & Revathy, K. (2019). Secure and efficient data sharing in cloud computing using proxy re-encryption. Journal of Ambient Intelligence and Humanized Computing, 10(7), 2763-2775.
[11] Mousavi, S. M., Anjomshoa, M., & Heidarysafa, M. (2019). Secure data sharing in cloud computing: A survey. Journal of Ambient Intelligence and Humanized Computing, 10(7), 2597-2618.
[12] Dhivya, A., Kumar, A., & Mahalakshmi, R. (2019). Secure data sharing in cloud computing using cryptography techniques: A review. Journal of Ambient Intelligence and Humanized Computing, 10(7), 2655-2671.
[13] Chen, D., & Zhao, H. (2012). Data security and privacy protection issues in cloud computing. International Journal of Distributed Sensor Networks, 8(2), 1-12.
[14] Kshetri, N. (2014). Privacy and security issues in cloud computing: The role of institutions and institutional evolution. Telecommunications Policy, 38(9), 1-13.
[15] Mather, T., Kumaraswamy, S., & Latif, S. (2009). Cloud security and privacy: An enterprise perspective on risks and compliance. O'Reilly Media, Inc.
[16] Rong, C., Nguyen, H., & Jaatun, M. G. (2014). Beyond lightning: A survey on security challenges in cloud computing. Computers & Electrical Engineering, 40(6), 1806-1827.
[17] Al-Rimy B. A., Al-Zobbi M. M. (2018) The Security of Cloud Computing. In: Jabbar S., Qadir J., Zaki Y. (eds) Handbook of Research on Cloud Computing and Big Data Applications in IoT. IGI Global, Hershey, PA, 22-39.

[18] Liu, X., Liu, J., Guo, S., & Wang, Q. (2015). Towards secure cloud storage via dynamic virtual file allocation and verification. Journal of Network and Computer Applications, 49, 41-52.
[19] Wang, X., Chan, S. C., & Wang, S. (2017). Achieving efficient and privacy-preserving data sharing in cloud computing. Future Generation Computer Systems, 67, 104-113.
[20] Zhang, Y., Sun, X., & Zhao, X. (2016). Secure data sharing in cloud computing using revocable storage identity-based encryption. Journal of Network and Computer Applications, 70, 18-26.
[21] Sattar, S., Alhaisoni, M., & Gharibi, W. (2018). Enhancing security in cloud storage using hybrid cryptography. Future Generation Computer Systems, 87, 693-703.
[22] Wang, Y., Zhang, Q., & Wu, L. (2016). A secure and dynamic multi-keyword ranked search scheme over encrypted cloud data. Journal of Network and Computer Applications, 66, 106-116.
[23] Yu, J., Huang, X., Yang, B., & Xue, Y. (2017). Privacy-preserving data sharing in cloud computing using attribute-based encryption. Future Generation Computer Systems, 70, 62-73.
[24] Zeng, J., Zhang, Y., & Liu, X. (2017). A privacy-preserving big data sharing scheme in cloud computing based on multi-authority attribute-based encryption. IEEE Access, 5, 16239-16251.
[25] Islam, M. M., Kulkarni, M. A., & Sohrabi, B. (2019). A secure data sharing framework for collaborative edge and cloud computing. Future Generation Computer Systems, 92, 61-70.
[26] Alam, M. J., & Alazab, M. (2019). Enhanced privacy-preserving secure data sharing in cloud computing. IEEE Access, 7, 142714-142728.
[27] Chen, J., Zhao, X., Chen, J., & Wu, J. (2019). A secure data sharing scheme for cloud computing based on ciphertext-policy attribute-based encryption. IEEE Access, 7, 102535-102546.
[28] Li, C., Zhang, Y., Yu, F., & Xiang, Y. (2020). Secure and efficient data sharing in cloud computing based on CP-ABE and anonymous authentication. Future Generation Computer Systems, 105, 786-796.