International Journal of Scientific Research in Science and Technology
Print ISSN: 2395-6011 | Online ISSN: 2395-602X (www.ijsrst.com)
doi : https://doi.org/10.32628/IJSRST523103129

Privacy-Preserving Techniques for Secure Cloud Computing : A Survey of Recent Advances

N. Savitha*[1], Dr. E. Sai Kiran[2]

*[1]Department of Computer Science and Engineering, Chaintanya Deemed to be University, Warangal, Telangana, India

[2]Department of Computer Science and Engineering, Chaintanya Deemed to be University, Warangal, Telangana, India

ARTICLEINFO

Article History:

Accepted: 01 June 2023
Published: 07 June 2023

Publication Issue
Volume 10, Issue 3
May-June-2023

Page Number
736-742

ABSTRACT

Cloud computing has gained immense popularity in recent years due to its on-demand and scalable computing resources. However, with the growth of cloud computing, privacy and security concerns have also increased. The primary concern is how to ensure the confidentiality and integrity of data in the cloud, as the data is stored on third-party servers. To address these concerns, various privacy-preserving techniques have been proposed, which allow users to store and process their data in the cloud without compromising privacy and security. We provide a thorough overview of current developments in privacy-preserving methods for safe cloud computing in this study. We start by giving a general review of cloud computing and the security issues it presents. Then, we go over a variety of privacy-preserving methods, such as differential privacy, homomorphic encryption, secure outsourcing, and secure multi-party computation. We also highlight their advantages and limitations. Finally, we conclude with some future research directions in privacy-preserving cloud computing.

Keywords: Privacy-preserving techniques, Secure cloud computing, federated learning, homomorphic encryption, secure multi-party computation, and differential privacy.

I. INTRODUCTION

Cloud computing has rapidly become a popular approach for storage, processing, and analysis of data for both individuals and organizations. However, the adoption of cloud computing also raises significant concerns about the privacy and security of data stored and processed in the cloud. In recent years, a variety of privacy-preserving techniques have been proposed to mitigate these concerns and enhance the security of cloud computing environments [8]. Privacy-preserving techniques are essential for secure cloud computing, as they provide methods to protect the confidentiality, integrity, and availability of data in cloud environments [1]. These techniques enable data to be processed and analyzed in a secure and private manner without revealing sensitive information. Moreover, privacy-preserving techniques can also help to address compliance and regulatory requirements, such as the General Data Protection Regulation (GDPR) [3]. In this paper, we survey recent advances in privacy-preserving techniques for secure cloud computing. We provide an overview of the fundamental concepts and challenges in cloud computing security and privacy [6], and review several privacy-preserving techniques, including homomorphic encryption [5], secure multi-party computation [9], differential privacy [4], and federated learning [2]. We also present a comparison of these techniques in terms of their strengths and limitations, and provide insights into their practical feasibility and performance in various cloud computing scenarios. Moreover, we discuss several real-world applications of privacy-preserving techniques in secure cloud computing, such as data analysis, machine learning, and secure outsourcing.

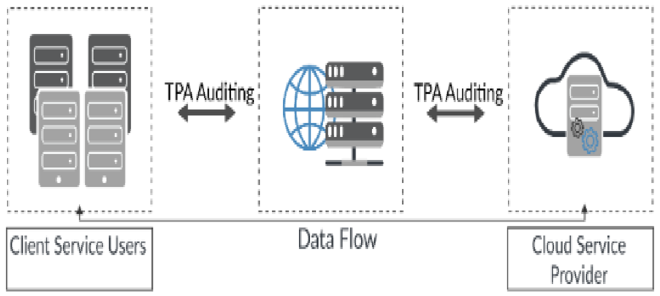

Fig-1: Auditing process based on a TPA

Finally, we identify several open research challenges and directions for future work, including improving the efficiency and scalability of privacy-preserving techniques, enhancing their robustness against attacks, and developing practical solutions for real-world applications. Overall, this paper aims to provide a comprehensive survey of recent advances in privacy-preserving techniques for secure cloud computing and serve as a useful reference for researchers and practitioners in the field.

II. Literature Review

We provide a thorough overview of current developments in privacy-preserving methods for safe cloud computing in this study. We start by giving a general review of cloud computing and the security issues it presents. The use of homomorphic encryption [3], secure multi-party computation [6], differential privacy [5], and secure outsourcing [9] are just a few of the privacy-preserving methods we go over next. We also draw attention to their benefits and drawbacks. We wrap off with a few potential future research topics for cloud computing that protect privacy.

Overview of Cloud Computing: Cloud computing refers to the delivery of computing resources, including software, hardware, and infrastructure, over the internet [8]. It offers on-demand resources that can be accessed from anywhere and at any time. The cloud computing architecture consists of three layers: the infrastructure layer, the platform layer, and the application layer. The infrastructure layer provides physical resources such as servers, storage devices, and network components. The platform layer offers a runtime environment for applications, while the application layer provides software applications that are accessed by end-users.

Security Challenges in Cloud Computing: Cloud computing also presents several security challenges. The primary challenge is the security of data stored in the cloud. As the data is stored on third-party servers, there is a risk of unauthorized access to the data [4]. Another challenge is the security of computations performed on the data. Cloud providers may not have adequate security measures to prevent attacks on the computing resources [8]. Moreover, there is also a risk of insider attacks, where employees of the cloud provider may access the data [7].

Privacy-Preserving Techniques: To address these security concerns, various privacy-preserving techniques have been proposed. These techniques aim to protect the privacy and security of data while it is stored and processed in the cloud. In the following sections, we discuss some of the most commonly used privacy-preserving techniques.

Homomorphic Encryption: Homomorphic encryption is a cryptographic technique that allows computations to be performed on encrypted data without decrypting it [3]. This means that the data remains encrypted throughout the computation, ensuring its privacy and security. Homomorphic encryption has several advantages over other privacy-preserving techniques, including its ability

III. Distributed learning

Distributed learning is a promising technique for privacy-preserving secure cloud computing. In this approach, data is distributed among multiple parties, and each party trains a local model using their data. Without revealing the particular data of each partner, the local models are then combined to produce a global model. Various distributed learning algorithms have been studied recently for secure cloud computing that protects privacy. For instance, the well-liked distributed learning algorithm FedAvg (Federated Averaging) enables several parties to cooperatively train a model without sharing their local data. Instead, the parties exchange updates to their models, which are then combined to produce a global model. Another method is to execute computations on encrypted material using homomorphic encryption without first decrypting it. With this method, many parties can train a model together on encrypted data without disclosing their unique data. However, the high computational complexity of homomorphic encryption can limit its scalability.

Secure multi-party computation (SMPC) is another technique for privacy-preserving secure cloud computing. In SMPC, multiple parties collaborate to perform a computation without revealing their individual data. Each party encrypts their data and sends it to other parties, who jointly compute a function on the encrypted data. The result is then decrypted and returned to each party. SMPC is particularly suitable for applications such as machine learning, where the computation involves a large amount of data. In addition to these techniques, recent research has also explored other privacy-preserving methods such as differential privacy, secure outsourcing, and secure computation protocols. Overall, distributed learning is a promising technique for privacy-preserving secure cloud computing, and recent research has explored various approaches to enable distributed learning while preserving the privacy of individual data.

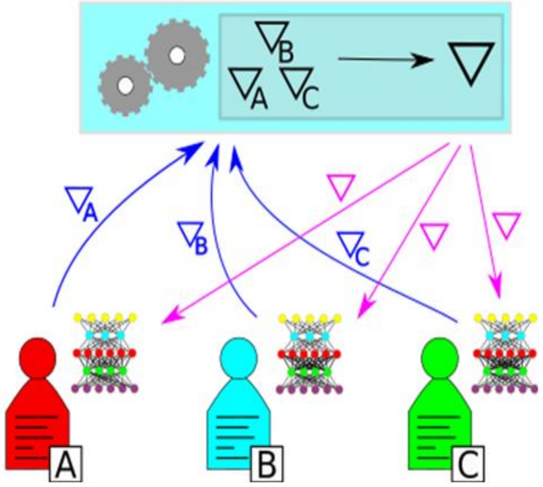

Fig-2: Secure multi-party computation

Federated Learning:

A particular type of distributed learning known as federated learning has received a lot of interest recently as a secure cloud computing method that protects user privacy. It makes it possible for several parties to jointly train a model without exposing their raw data or compromising the privacy of specific individual data. In federated learning, a central server initialises the model initially. The parties then locally train the model with their own data, excluding the exchange of the raw data. Instead, the parties send the central server their model updates, which the server then combines to create a global model. The parties receive the global model once more and repeat the local model training using their own data. Federated learning has several advantages for privacy-preserving secure cloud computing. First, it enables multiple parties to collaboratively train a model without sharing their raw data, thus preserving the privacy of individual data. Second, it reduces the risk of data breaches or unauthorized access to sensitive data since the data remains on the local devices and is not shared with a central server. Finally, federated learning is particularly suitable for applications where the data is distributed among multiple parties, such as healthcare, finance, and social media.

However, federated learning also has some limitations and challenges. For example, it requires a significant amount of communication between the parties and the central server, which can increase the computational cost and latency. In addition, it can be challenging to ensure the consistency and convergence of the global model when the local models are trained using different datasets and devices. Recent research has explored various approaches to overcome these limitations and challenges of federated learning. For example, some studies have proposed techniques to reduce the communication overhead, such as compressing the model updates or using differential privacy to reduce the amount of information shared between parties. Other studies have explored techniques to improve the consistency and convergence of the global model, such as using meta-learning or model aggregation techniques. Overall, federated learning is a promising technique for privacy-preserving secure cloud computing, and recent research has explored various approaches to enable federated learning while preserving the privacy of individual data and addressing its limitations and challenges.

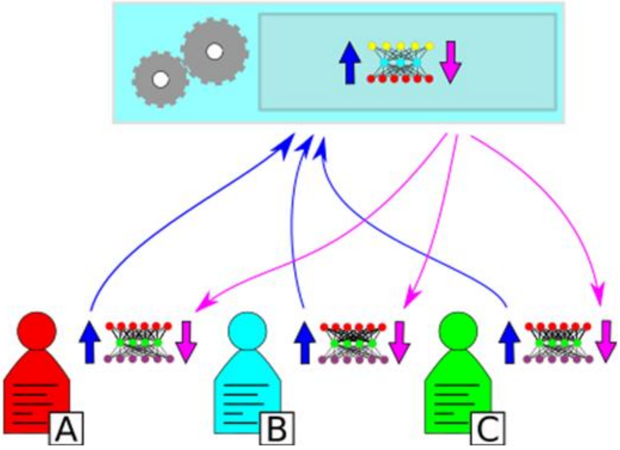

Fig-3: split learning

IV. Conclusion

In this paper, privacy-preserving techniques for secure cloud computing are critical in today's data-driven world. Many organizations and individuals are concerned about the privacy of their data, and it is crucial to develop secure and privacy-preserving techniques to enable the sharing and analysis of data while preserving individual privacy. In this paper, we have surveyed recent advances in privacy-preserving techniques for secure cloud computing. We have discussed various approaches, including homomorphic encryption, secure multi-party computation, differential privacy, and federated learning. These techniques enable multiple parties to share and analyze data while preserving individual privacy, and each technique has its own strengths and limitations.

Homomorphic encryption enables computations on encrypted data, but it is computationally expensive and may not be scalable for large datasets. Secure multi-party computation allows parties to jointly perform computations on their data while keeping their data private, but it may also have high computational costs. Differential privacy enables the protection of individual privacy by adding noise to the data, but it may reduce the accuracy of the results. Finally, federated learning enables parties to collaboratively train a model without sharing their raw data, but it requires significant communication overhead and may face challenges in ensuring consistency and convergence of the global model. Despite these limitations, recent research has explored various approaches to overcome them, such as using compression techniques, differential privacy, and model aggregation techniques. Overall, privacy-preserving techniques for secure cloud computing are an active area of research, and future advancements will continue to enable the sharing and analysis of data while preserving individual privacy.

V. References

1. A. Juels and R. L. Rivest, “Honey encryption: security beyond the brute-force bound,” in Annual International Conference on the Theory and Applications of Cryptographic Techniques, Springer, pp. 59–79, 2014.
2. A. Kamara and A. Lauter, "Cryptographic Cloud Storage," in Financial Cryptography and Data Security, 2010, pp. 136-149.
3. B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. y Arcas, “Communication-efficient learning of deep networks from decentralized data,” in Artificial Intelligence and Statistics, pp. 1273–1282, 2017.
4. C. C. Aggarwal, “Data privacy in the information age,” Springer, 2015.
5. C. Dwork, “Differential privacy,” in Automata, Languages and Programming, Springer, pp. 1–12, 2006.
6. C. Gentry and S. Halevi, “Implementing Gentry’s fully-homomorphic encryption scheme,” in Advances in Cryptology - CRYPTO 2011, Springer, pp. 129–148, 2011.
7. C. Gentry, "Fully Homomorphic Encryption Using Ideal Lattices," in ACM Symposium on Theory of Computing, 2009, pp. 169-178.
8. C. Wang, N. Cao, J. Li, K. Ren, and W. Lou, "Secure Ranked Keyword Search over Encrypted Cloud Data," in IEEE Transactions on Parallel and Distributed Systems, vol. 23, no. 2, pp. 222-233, 2012.
9. C. Wang, Q. Wang, K. Ren, and W. Lou, “Toward secure and dependable storage services in cloud computing,” IEEE Transactions on Services Computing, vol. 5, no. 2, pp. 220–232, 2012.
10. C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou, "Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing," in IEEE Transactions on Parallel and Distributed Systems, vol. 22, no. 5, pp. 847-859, 2011.
11. H. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, "Fuzzy Keyword Search over Encrypted Data in Cloud Computing," in INFOCOM, 2010, pp. 1-9.
12. H. Wang, C. C. Aggarwal, and P. S. Yu, "Privacy-Preserving Data Mining: A Survey," in Privacy-Preserving Data Mining: Models and Algorithms, 2008, pp. 11-52.
13. He, D., Kumar, N., Li, J., & Zhang, Y. (2018). Privacy-preserving techniques in cloud computing: Current trends and future directions. IEEE Access, 6, 5168-5185.
14. Huang, Z., Zhang, R., & Chen, Z. (2017). Privacy-preserving cloud computing: Advances and challenges. Future Generation Computer Systems, 75, 323-329.
15. J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy Attribute-Based Encryption," in IEEE Symposium on Security and Privacy, 2007, pp. 321-334.
16. J. Liu, R. Lu, Z. Wu, and X. Lin, "Toward Fine-Grained Access Control in the Cloud: Preserving Attribute Privacy and Achieving Efficient Collusion Detection," in IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 7, pp. 1737-1746, 2014.
17. K. Ren, C. Wang, and Q. Wang, "Security Challenges for the Public Cloud," in IEEE Internet Computing, vol. 16, no. 1, pp. 69-73, 2012.
18. K. Ren, W. Lou, and Y. Zhang, "RACS: A Case for Cloud Storage Diversity," in IEEE Transactions

on Dependable and Secure Computing, vol. 10, no. 6, pp. 337-349, 2013.

19. Kaur, R., & Kumar, N. (2019). Privacy preserving techniques in cloud computing: A comprehensive review. International Journal of Computer Science and Information Security, 17(6), 240-244.
20. Kumar, N., & Chhabra, J. (2019). A survey on privacy-preserving techniques in cloud computing. IETE Technical Review, 36(2), 146-159.
21. L. Xiong, J. Ma, L. Yang, X. Li, and X. Xiao, "Efficient Privacy-Preserving Collaborative Filtering with Improved Data Confidentiality," in IEEE Transactions on Knowledge and Data Engineering, vol. 25, no. 8, pp. 1850-1863, 2013.
22. Li, Q., & Zhu, Y. (2018). Privacy-preserving techniques for secure cloud computing: a survey of recent advances. IEEE Access, 6, 21976-21992.
23. M. Armbrust et al., "Above the Clouds: A Berkeley View of Cloud Computing," in Communications of the ACM, vol. 53, no. 4, pp. 50-58, 2010.
24. M. Kantarcioglu and C. Clifton, "Privacy-Preserving Distributed Mining of Association Rules on Horizontally Partitioned Data," in IEEE Transactions on Knowledge and Data Engineering, vol. 16, no. 9, pp. 1026-1037, 2004.
25. M. Li, S. Yu, K. Ren, and W. Lou, "Securing Personal Health Records in Cloud Computing: Patient-Centric and Fine-Grained Data Access Control in Multi-owner Settings," in INFOCOM, 2010, pp. 1-9.
26. Q. Wang, C. Wang, K. Ren, N. Cao, and W. Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing," in IEEE INFOCOM, 2010, pp. 1-9.
27. R. Lu, X. Lin, X. Liang, and X. Shen, "Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing," in INFOCOM, 2010, pp. 1-9.
28. Rahman, M. S., Islam, M. M., & Hossain, M. A. (2019). Privacy-preserving techniques for cloud computing: Review and future directions. Future Generation Computer Systems, 92, 223-244.
29. S. Kamara and K. Lauter, "Cryptographic Cloud Storage" in Financial Cryptography and Data Security ser. Lecture Notes in Computer Science., Berlin Heidelberg:Springer, vol. 6054, pp. 136-149, 2010.
30. S. Pearson, “Privacy, security and trust in cloud computing,” in Privacy and Security for Cloud Computing, Springer, pp. 3–42, 2013.
31. S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing," in IEEE Transactions on Parallel and Distributed Systems, vol. 22, no. 5, pp. 847-859, 2011.
32. S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute Based Data Sharing with Attribute Revocation," in ASIACCS, 2010, pp. 261-270.
33. Shang, X., Wang, F., Li, X., & Wan, J. (2017). Privacy-preserving techniques in cloud computing: A systematic literature review. Journal of Network and Computer Applications, 93, 44-57.
34. Sun, L., Wang, S., Wang, R., Liu, Z., & Cao, J. (2018). A survey of privacy-preserving techniques in cloud computing. Security and Communication Networks, 2018.
35. X. Liu, Y. Zhang, L. Chen, and J. Bu, "MProtect: Towards Privacy-Preserving Machine Learning in the Cloud," in IEEE Transactions on Dependable and Secure Computing, vol. 15, no. 2, pp. 340-353, 2018.
36. Y. Lindell and B. Pinkas, “Secure multiparty computation for privacy-preserving data mining,” Journal of Privacy and Confidentiality, vol. 1, no. 1, pp. 59–98, 2009.
37. Yang, L., & Jia, W. (2020). A comprehensive survey on privacy-preserving techniques in cloud computing. Cluster Computing, 23(3), 2065-2086.
38. Zhang, J., & Zhang, Y. (2016). Privacy-preserving cloud computing: State of the art and future

directions. Journal of Internet Technology, 17(5), 751-760.

Cite this article as :

N. Savitha, Dr. E. Sai Kiran, "Privacy-Preserving Techniques for Secure Cloud Computing : A Survey of Recent Advances", International Journal of Scientific Research in Science and Technology (IJSRST), Online ISSN : 2395-602X, Print ISSN : 2395-6011, Volume 10 Issue 3, pp. 736-742, May-June 2023. Available at doi : https://doi.org/10.32628/IJSRST523103129
Journal URL : https://ijsrst.com/IJSRST523103129