ISSN: 2633-4828 Vol. 5 No.4, December, 2023

International Journal of Applied Engineering & Technology

LITERATURE REVIEW ON PRIVACY PRESERVATION OF DATA IN THE CLOUD USING IOMT

Sowjanya Addu[1] and Dr. Arpit Jain[2]
[1] Research Scholar and [2]Professor, Department of CSE, KL Deemed to be University, Guntur, Andhra Pradesh, India
[1]sowji.affable@gmail.com and [2]dr.jainarpit@gmail.com

ABSTRACT
Every day, vast amounts of data are collected and analyzed in our information-driven world. Cloud computing has emerged as the most popular model for supporting large and complex data. It provides the possibility of developing accurate machine learning models. Moreover, it was challenging to explore the possibility of extending the suggested basis where the parties will not follow the honest-but-curious security model and satisfy the patient's and medical professionals' specifications and offers data gathering without compromising privacy policy. Although it is still difficult to avoid many aspects in the medical literature, such as emotion, communication, violence. Leveraging cloud services to meet remote storage needs is exciting. The challenge is the need for reliable and efficient storage and secure data transfer network bandwidth. Although it is difficult to create a better personal protection system to collect information at the request of users and protect the owner's information.

Keywords: Privacy preservation, Cloud Security, Internet of Things, IoMT, IoHT, Inference, linking, Cloud services.

INTRODUCTION
The Cloud computing sector offers a large amount of support to the global environment in various areas like education, medicine, and business.Security is an important part of international services. The first of these is how to ensure that ID card, name, address and other information are not leaked during the application process. This is to prevent personal privacy from being compromised by malicious information. The second is how to make better data requests. Loss of personal information is unacceptable to any person or organization, especially in the medical field. Data security and privacy preservation in cloud storage environments based on cryptography mechanisms. For this, various kinds of techniques, like cryptography, differential privacy, k-anonymity, etc., are used to preserve the data for privacy reasons before transferring it to the cloud platforms. Data encryption and decryption becomes better technique for getting information secrecy and respectability.

Privacy in Cloud Storage
Recently, numerous services in the cloud, such as healthcare, online marketing, banking & payment, and social media, rely heavily on the utilization of personal information. These privacy-sensitive data are stored in distant locations across the globe. This development raises concerns regarding privacy in the cloud, including how users' privacy is perceived and safeguarded. In response to these growing privacy concerns, various technologies have been proposed, and governments worldwide are working on establishing legal frameworks to protect privacy. However, there still exist gaps between current practices and proposed solutions, conflicts of interests, and disagreements on requirements and concepts.

Defining Privacy
Privacy entails the freedom from any form of interference. Privacy control empowers individuals to maintain a certain level of intimacy. It serves as a safeguard for the proper use of personal information belonging to cloud users. Breaches of privacy can lead to significant troubles for cloud users. The American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA) define privacy as "the right and obligation of individuals and organizations regarding the collection, use, retention, and disclosure of personal information."

Privacy Concerns in Cloud Storage

When assessing privacy risks in the context of cloud storage, it is crucial to recognize that privacy threats vary depending on the specific cloud scenario. The papers [2][3] highlight several privacy issues, including lack of user control, inadequate training and expertise, unauthorized secondary usage, complexity of regulatory compliance, addressing restrictions on transborder data flow, litigation, legal uncertainty, compelled disclosure to the government, data security, disclosure of breaches, data accessibility, location of data, and data transfer and retention

LITERATURE SURVEY

Aminifar, A., Shokri, M., Rabbi, F., Pun, V.K.I. and Lamo, Y [1] developed high-quality and contributed a better healthcare system in the long term. Aminifar, A., Shokri, M., Rabbi, F., Pun, V.K.I. and Lamo, Y [1] suffered from scalability and high communication overhead.

Mondal, A. Goswami, RT[2] increased the security of Web services due to the use of high-performance systems. Mondal, A. and Goswami, R.T [2] It is not widely used due to translation complexity and computation time.

Ahamad, D., Hameed, S.A. and Akhtar, M [3] solves the multi-objective privacy problem with rapid integration and proves effective. Ahamad, D., Hameed, S.A. and Akhtar, M [3] The accuracy of the treatment appears to be low.

Mansour, H.O., Siraj, M.M., Ghaleb, F.A., Saeed, F., Alkhammash, E.H. Maarof, M.A[4] A more efficient and more complete method of ensuring confidentiality for electronic data. Protecting privacy in this way is not effective. Sathya, A. and Raja, S.K.S [5] show interest in using their methods in personal protection of sensitive data in the medical field, thus contributing to larger data. This method solves the problem of users updating simultaneously. Çamikara, M.A.P., Bertok, P., Halil, İ., Liu, D., and Çamtepe, S [6] rare comparison method for the operation of distribution centers gives good results. In this way the use of time is affected by the number of attributes. Singh, AK Gupta, R., [7] Efficacy pattern of well-established data shows that PPMD is safer, more effective and more effective. This solution uses higher memory. Wang, K., Li, J. and Wu, W [8] method has advantages such as fast learning, less interference and computational efficiency. Due to data privacy and security concerns, organizational standards cannot be updated easily and regularly.

This section reviews the literature on various existing techniques for privacy-privacy key generation based on the new hybrid RMDL-CNN in the cloud.

The above research data was organized and analyzed according to the previous year's publication.

RELATED WORK

The Internet of Things has supported the development of the Internet of Things (IoHT) and IoMT in Healthcare, which helps reduce and monitor health problems across a wide range of diseases. In [13], the authors aimed to provide home patient identification services using weather patterns to solve multiple problems. [14] discussed the development of a new healthcare system that meets the academic, commercial and needs of IoT. The authors describe a heart monitor that sends messages to the patient's relatives via a smart bracelet. [15] explores various IoT applications, technologies, and methods and highlights the importance of IoT in healthcare. The paper also highlights the importance of avoiding distributed attacks and presents an intelligent IoT model to improve healthcare systems and e-health while mitigating IoT attacks. [16] proposed a physical sensor network that can transmit high-quality and continuous data to IoT-based public systems, highlighting the role of communication in the development of IoT applications in therapy. The authors also mention the necessary safety constraints to increase the safety of the planning process, including the next moving equipment. As the exchange of audiovisual data from different cloud services increases, good security is needed to ensure greater security, reduce the quality of interference and less competition.

PROPOSED SYSTEM

The primary intention of the research is to develop a New Hybrid Random Multimodal Deep Learning Fused Convolutional Neural Network (RMDLFCNN) based key generation for privacy preserved data in cloud.

Security Parametres are:

- Trust Factors
- Encryption
- Kronecker product
- Secret key

Here the implementation of the proposed method will be used by the Python tool.

The performance will be evaluated under the metrics of accuracy and utility.

Federated Learning (FL), also known as collaborative learning, is a machine learning approachs main aspect to tackle the challenges of data governance and privacy by enabling algorithms to be trained collectively without the need to exchange the actual data.

The proposed Internet of Medical Things (IoMT) model consists of three stages: data acquisition, data storage, and application stages. The data acquisition stage involves three main processes: sensor-based data collection, encryption of the acquired data, and computation of the storage key value for secure storage of the encrypted data on the cloud.

In the second stage of the IoMT model, the encrypted data is stored on the cloud using B+ file organization. The data is organized based on the attached key, ensuring efficient storage and retrieval.

The third stage of the proposed model is the application stage, where authorized doctors, patients visiting other healthcare centers, and registered research institutions are granted access to the cloud-based information. This allows for seamless information sharing and collaboration.

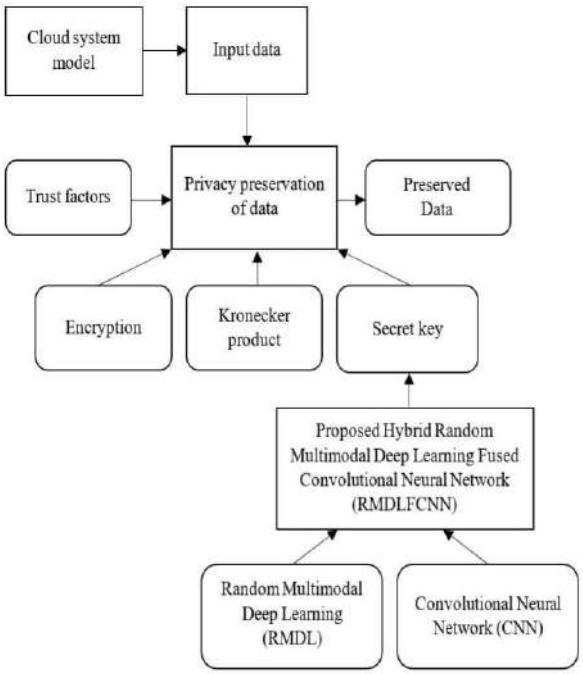

Figure 1. Block Diagram of the proposed RMDLFCNN

The IoMT Model is Built on Several Premises:

1. Each healthcare center has its own cloud for storing patient information, and these clouds are interconnected.
2. Patients are equipped with wireless sensors that transmit data to a central sensor connected to the healthcare cloud where the patient is registered.
3. The central sensor is equipped with encryption and decryption applications, among other functionalities.
4. Patient information is stored in a central database through the cloud network.
5. A timestamp named "T" is included in every message sent and received, ensuring data accuracy.
6. Private communication between clients on the IoMT platform is not possible. Communication is limited to the healthcare center and the clients.

These premises form the foundation of the proposed IoMT model, enabling secure and efficient healthcare data management and access.

Challenges:

Existing techniques face the following challenges:

- Develop accurate machine learning models in [1]. It was difficult to consider extending the suggested basis if the parties do not adhere to the honest but curious security model.
- In[5], it meets the needs of the patients and medical professionals and provides data collection without violating privacy policy. However, it was difficult to prevent multiple attacks like inference, linking and impersonation in the healthcare database.
- In a study mentioned in [6], the enhancement of efficiency for the quantity of attributes was not observed in the DISTPAB. Additionally, it proved to be challenging to accomplish, and it was not able to explore the vertical federated learning approach in situations where the distributed clients possess distinct feature spaces.
- Cloud services for remote storage are becoming increasingly popular. However, the need for cost-effective storage solutions and secure data transmission network bandwidth remains a challenge.

Researchers have identified these issues and have developed alternative approaches to address the privacy concerns surrounding cloud data. However, many of these existing techniques have been found to have shortcomings. Searchable encryption (SE) has emerged as a viable solution to the data privacy problem in the cloud environment. However, SE presents an additional challenge in the multiuser setting, where each user may have access to encrypted data segments stored by different users. Multiuser searchable encryption schemes enable users to search through multiple data segments based on search rights granted by the segment owners. In this setting, privacy requirements extend beyond the confidentiality of the data segments to include the privacy of the queries, protecting against impostors and potentially malicious cloud service providers (CSPs). Nevertheless, existing searchable encryption techniques, such as Fully Homomorphic Encryption (FHE) implementations, involve computationally intensive operations that render the schemes impractical. Practical FHE is still a distant goal, and efforts to enhance its performance remain an active area of research. This research work proposes a secure Internet of Medical Things (IoMT) model that incorporates an efficient cloud data privacy-preserving technique to safeguard sensitive medical information stored in the cloud. The proposed scheme utilizes a hybrid-based encryption/decryption scheme called Hybrid Modified Caesar Cryptosystem (HMCC). In HMCC, the existing stream Caesar cipher is modified into a block cipher to enhance data security. Additionally, Elliptic Curve Diffie-Hellman (ECDH) is employed for secret key sharing, and an Elliptic Curve Digital Signature Algorithm (ECDSA) is applied for digital signing and signature verification.

METHODOLOGY

Cloud computing is one of the hottest topics in the current information technology (IT) field. As more and more important data is transferred to third-party cloud service providers, concerns have arisen about the reliability of these service providers. To ensure data privacy, users are advised to encrypt sensitive data before storing it in the cloud. Traditional encryption methods have limitations.

Traditional encryption terms say that if the key owner wants to access private data stored in the cloud, all encrypted data from the cloud server, decrypt it, and then search for the necessary information must be downloaded. This method is not very useful, especially when the encrypted data is large or the user accesses the cloud storage from a mobile phone. Additionally, the key is sent to the cloud server for decryption and search, but this poses a serious security risk since the cloud server can access the key.

To overcome these challenges, various models for the integrity of data archives have been proposed. One such model is the Provable Data Ownership (PDP) model, which uses an RSA-based homomorphic linear verifier to verify that data is trustless. However, this model still has the disadvantage of sending information to external auditors and therefore affecting privacy. Another model, called the Proof of Retrieval (PoR) model, uses checkpoints and error-correcting codes to ensure the availability and storage of data. However, this method only works on encrypted devices. An improvement to the PoR protocol was proposed to guarantee confidentiality of control and use the BLS signature. Unfortunately, this system also has a lack of self-protection.

Thus, TPA (Third Party Auditor) based methods emerged to ensure the integrity of online storage. The main aim of this approach is to provide solutions that allow efficient and secure access to cloud storage while preserving privacy.

Encryption Techniques

Encryption techniques are used to ensure privacy in cloud computing as discussed in previous articles [10] [11]. Method [10] proposed a privacy-preserving cloud storage framework to solve the privacy security problem. The framework is built around information standards, trends and governance, collaboration with partners, changes to user rights, and support for working on dynamic data. It also uses interactive process and elimination as the key derivation algorithm. This framework ensures confidentiality of information, solves the problem of low key derivation performance, reduces encryption and decryption efforts, simplifies the management of many keys, saves storage space for the owner, minimizes the operating system and ensures privacy. security is available to many users, data subjects and service providers. But technology is needed to reduce the burden of encryption on the owner and work on the ciphertext.

As mentioned in the document [10][11], encryption technology is used to ensure confidentiality in cloud computing. Method [10] proposed a special cloud storage protection framework to solve the privacy security problem. Here, the framework includes data organization, trends and creation of management structure, collaboration with partners, handling of changes in user rights and support for dynamic data processing. It uses interpolation and elimination method as key derivation algorithm. This framework ensures confidentiality of information, solves the problem of key ineffectiveness, reduces the burden of encryption and decryption, facilitates the management of multiple keys, saves storage space for the owner, reduces processing time, and provides excellent privacy security. . Used for multiple users, profile owners and service providers. But technology is needed to reduce the burden of encryption on the owner and work on the ciphertext.

Privacy Preservation in the Proposed IoMT Model

The cloud does not disclose the patient's identity, and to prevent unauthorized access, health records of the patients are stored on the cloud after encryption. To make this easy to search through the encrypted data, the encrypted data are stored on the cloud using B+ tree file organization, in which the information is stored using (key, value) pair form.

CONCLUSION

Development of accurate machine learning models is made possible by it. Furthermore, research into the potential of the proposed disclosure process in situations where parties do not comply with the fair but knowing security standard has proven to be a difficult task. It meets the specific needs of patients and doctors while ensuring that data is stored without compromising privacy. Although there are difficulties in preventing various attacks such as emotion, communication, personalization on medical records. There is growing interest in using cloud services for remote storage needs. However, cloud service providers still face the challenge of providing reliable and affordable storage and secure data connections. In addition, sharing the collected data among users and creating appropriate security mechanisms to protect the data from more than one owner also causes problems. It has the ability to improve the quality of education. Furthermore, research into the potential of the proposed disclosure process in situations where parties do not comply with the fair but knowing security standard has proven to be a difficult task.

REFERENCES

[1] https://ieeexplore.ieee.org/document/9676691

[2] https://www.sciencedirect.com/science/article/abs/pii/S0141933120308644

[3] https://www.sciencedirect.com/science/article/pii/S131915782030495X

[4] https://www.hindawi.com/journals/wcmc/2021/7154705/

[5] https://link.springer.com/article/10.1007/s11277-021-08278-6

[6] https://www.sciencedirect.com/science/article/abs/pii/S0140366421000773

[7] https://arxiv.org/abs/2212.12534

[8] https://www.hindawi.com/journals/scn/2022/2913293/

[9] https://www.academia.edu/36810974/Review_Paper_on_Privacy_Preservation_Techniques_in_Cloud

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

[11] Jayalatchumy, D., Ramkumar, P., &Kadhirvelu, D. 2010, November. Preserving Privacy through Data Control in a Cloud Computing Architecture Using Discretion Algorithm. In Emerging Trends in Engineering and Technology (ICETET), pp. 456-461

[12] https://www.researchgate.net/publication/368932585_Securing_Critical_User_Information_over_the_Internet_of_Medical_Things_Platforms_Using_a_Hybrid_Cryptography_Scheme

[13] Chavan, P.; More, P.; Thorat, N.; Yewale, S.; Dhade, P. ECG-Remote patient monitoring using cloud computing. Imp. J. Interdiscip.Res. 2016,2, 368–372

[14] Arbat, H.; Choudhary, S.; Bala, K. IoT smart health band. Imp. J. Interdiscip. Res. 2016,2, 300–311.43.Islam,

[15] S.R.; Kwak, D.; Kabir, M.H.; Hossain, M.; Kwak, K.S. The internet of things for health care: A comprehensive survey. IEEEAccess 2015,3, 678–708.

[16] Huiyeh, K.A. secure IoT-based healthcare system with body sensor networks. IEEE Access 2016,4, 10288–10299

[17] Gohel, M., & Gohil, B. 2012. A New Data Integrity Checking Protocol with Public Verifiability in Cloud Storage. Trust Management VI, 240-246.

[18] Wang, Q., Wang, C., Ren, K., Lou, W., & Li, J. 2011. Enabling public auditability and data dynamics for storage security in cloud computing. Parallel and Distributed Systems, IEEE Trans. on, 22(5), 847-859.

[19] Ateniese, G., Burns, R., Curtmola, R., Herring, J., Khan, O., Kissner, L., ... & Song, D. 2011. Remote data checking using provable data possession. ACM Transactions on Information and System Security (TISSEC), 14(1), 12.

[20] Hao, Z., Zhong, S., & Yu, N. 2011. A privacy-preserving remote data integrity checking protocol with data dynamics and public verifiability. Knowledge and Data Engineering, IEEE Transactions on, 23(9), 1432-1437.

[21] Wang, C., Chow, S., Wang, Q., Ren, K., & Lou, W. 2010. Privacy-preserving public auditing for secure cloud storage.

[22] Zhu, Y., Hu, H., Ahn, G. J., & Yau, S. S. 2011. Efficient audit service outsourcing for data integrity in clouds. Journal of Systems and Software.

[23] B. Cui, Z. Liu, and L. Wang, "Key-Aggregate Searchable Encryption (KASE) for Group Data Sharing via Cloud Storage," IEEE Transactions on Computers, vol.65, no.8, pp. 2374–2385, Aug. 2016.

[24] H. Deng, Z. Qin, Q. Wu, Z. Guan, and Y. Zhou, "Flexible attribute-based proxy re-encryption for efficient data sharing," Information Sciences, vol. 511, pp. 94–113, Feb. 2020.

[25] "Digital Economy Report," United Nations, 2019.

[26] C. Dong, K. Yang, J. Qiu, and Y. Chen, "Outsourced revocable identitybased encryption from lattices," Transactions on Emerging Telecommunications Technologies, vol. 30, n. 11, pp. e3529, Nov. 2019.

[27] Y. Dodis, Y. T. Kalai and S. Lovett, "On cryptography with auxiliary input," in Proc. 41st Annual ACM Symposium on Theory of Computing, 2009, pp. 621–630.

[28] L. Du, K. Li, Q. Liu, Z. Wu, and S. Zhang, "Dynamic multi-client searchable symmetric encryption with support for boolean queries," Information Sciences vol. 506, pp. 234–257, Jan. 2020.

[29] S. Dziembowski, "Intrusion-resilience via the bounded-storage model," in Proc. TCC, Berlin, Germany: Springer, 2006, vol. 3876, pp. 207–224.

[30] E. Makkaoui, K. Ezzati, A. Beni-Hssane, and S. Ouhmad, "Fast CloudâA ¸SPaillier homomorphic schemes for protecting confidentiality of ˇ sensitive data in cloud computing," in J Ambient Intell Human Comput, to be published. (DOI: 10.1007/s12652-019-01366-3)

[31] T. Elgamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," IEEE Transactions on Information Theory, vol. 31, no. 4, pp. 469–472, Jul. 1985.

[32] Fully Homomorphic Encryption: Cloud Security. Accessed on Feb. 2020. [Online]. Available: https://www.sciencedirect.com/topics/computerscience/fully-homomorphic-encryption

[33] Z. Fu, X. Wu, C. Guan, X. Sun and K. Ren, "Toward Efficient MultiKeyword Fuzzy Search Over Encrypted Outsourced Data With Accuracy Improvement," IEEE Transactions on Information Forensics and Security, vol. 11, no. 12, pp. 2706–2716, Dec. 2016.

[34] Gartner: Gartner Forecasts Worldwide Public Cloud Revenue to Grow 17% in 2020. Accessed on Feb. 2020. [Online].Available: https://www.gartner.com/en/newsroom/press-releases/2019-11-13-gartner-forecasts-worldwide-public-cloud-revenue-to-grow-17-percentin-2020

[35] C. Ge, W. Susilo, L. Fang, J. Wang and Y. Shi, "A CCA-secure key-policy attribute-based proxy re-encryption in the adaptive corruption model for dropbox data sharing system," Designs, Codes and Cryptography, vol. 86 n. 11, pp. 2587–2603, Nov. 2018.