Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 05, May-2023

Safeguarding the Confidentiality of Electronic Health Records: State of Art

Deepali Awasthi
Noida Institute of Engineering and Technology

Shagun Chauhan
Noida Institute of Engineering and Technology

Dr. Hitesh Singh
Associate Professor
Noida Institute of Engineering and Technology

Swati Lohiya
Noida Institute of Engineering and Technology

Mahima Kaushik
Noida Institute of Engineering and Technology

Dr. Vivek Kumar
Professor
Noida Institute of Engineering and Technology

Abstract*— The increased demand for data availability in every industry is driving individuals to exchange and store data on centralized platforms such as clouds so that the intended audience may access it. To facilitate data exchange and storage in the medical industry, organizations and patients are building cloud platforms. However, the most pressing issue that everyone faces is data protection and security. Here, we describe many techniques that are available to protect the system and meet the requirement for data privacy preservation in the medical industry. Some algorithms are Zero-Knowledge Proof, Principal Component Analysis and Random Projection, Generative Adversarial Networks, blockchain and cloud computing, Quasi-Identifier Recognition, Q-learning Neural Network, digital signature, and others.

Keywords— ***Medical record, Cloud computing, blockchain, privacy-preservation, GANs, algorithm, digital signature.***

I INTRODUCTION

1. Introduction

Electronic health records (EHRs) have transformed the way healthcare professionals manage patient data. EHRs provide an efficient and secure way to store and share patient information, enabling healthcare providers to deliver better patient care. However, the widespread use of EHRs also poses new challenges, particularly when it comes to safeguarding the confidentiality of patient information.

In this article, we will explore the importance of confidentiality in electronic health records and the threats that EHRs face. We will also provide best practices for safeguarding the confidentiality of EHRs to ensure patient privacy is protected.

2. The Importance of Confidentiality in Electronic Health Records

Confidentiality is a critical component of healthcare. Patients expect that their medical information will be confidential. The unauthorized disclosure of patient information can have serious consequences, including damage to the patient's reputation, financial harm, and even physical harm. Electronic health records contain sensitive information such as patient medical history, diagnoses, medications, and lab results. It is essential to maintain the confidentiality of this information to protect patient privacy and prevent potential harm.

3. Common Threats to Electronic Health Records Confidentiality

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 05, May-2023

Electronic health records face several threats to their confidentiality. These include:

a) Unauthorized Access: One of the most significant threats to EHR confidentiality is unauthorized access. Healthcare providers must implement strict access controls in order to make that only authorized personnel can access patient information.

b) Insider Threats: Employees with authorized access to EHRs can pose a significant threat to confidentiality. It is essential to monitor employee access to patient information to detect and prevent any unauthorized activity.

c) Hacking: EHRs are vulnerable to hacking attacks, and cybercriminals can use stolen patient information for identity theft or other fraudulent activities.

d) Physical Theft: Physical theft of EHRs, such as laptops or mobile devices, can also compromise patient information.

4. Best Practices for Safeguarding Electronic Health Records Confidentiality

To protect the confidentiality of electronic health records, healthcare providers should follow best practices such as:

a) Implementing Access Controls: Access controls should be in place to make sure that only authorized personnel can get access to patient information. This includes password protection, multi-factor authentication, and user roles and permissions.

b) Regular Employee Training: Regular employee training should be conducted to ensure that employees are aware of the importance of EHR confidentiality and understand their role in safeguarding patient information.

c) Regular Auditing: Regular auditing of EHR access logs monitors any unauthorized access or activity.

d) Encryption: All patient data should be encrypted both in transit and at rest to prevent unauthorized access.

e) Physical Security: Physical security measures, such as locking up laptops and mobile devices when not in use, can prevent physical theft of EHRs.

f) Disaster Recovery and Business Continuity Planning: Healthcare providers should have a disaster recovery and business continuity master plan in place to make that patient information is not compromised at the time of a disaster.

Safeguarding the confidentiality of electronic health records is critical to protecting patient privacy and preventing potential harm. Healthcare providers must implement strict access controls, employee training, regular auditing, encryption, physical security, and disaster recovery and business continuity planning to ensure that patient information remains confidential. By following best practices for EHR confidentiality, healthcare providers can maintain patient trust and deliver better patient care.

II LITERATURE REVIEW

Feng et al. [1] developed a blockchain-based privacy protection and sharing scheme that uses zero-knowledge proof to safeguard sensitive data in wireless communication and mobile computing. Ratra et al. [2] presented a big data privacy preservation method in healthcare that reduces the dimensionality of the data using principal component analysis and random projection while still maintaining privacy. Yin and Yang [3] suggested a privacy preservation technique based on Generative Adversarial Networks (GANs) to safeguard mobility data by generating a synthetic dataset with similar properties to the original data. Huang and Lee [4] introduced a medical data privacy protection technique that employs blockchain and cloud computing to store encrypted medical data securely and ensure data integrity and confidentiality.

Mansour et al. [5] proposed a Quasi-Identifier recognition algorithm for protection of cloud data that identifies sensitive data and reduces the risk of reidentification in cloud computing. Zhang et al. [6] proposed a blockchain-based privacy-preserving e-health system that maintains data confidentiality, integrity, and availability while protecting sensitive healthcare data. Anand et al. [7] presented a privacy-preserving module using Gaussian mutation-based firebug optimization in cloud computing that preserves the privacy of data by minimizing the risk of reidentification and optimizing the accuracy of data analysis. Kanwal et al. [8] provided a taxonomy of privacy preservation in e-health cloud and highlighted the need for efficient privacy-preserving methods in this area. Chenthara et al. [9] discussed the security and privacy challenges of e-health solutions in cloud computing, emphasizing the importance of secure and privacy-preserving e-health solutions. Yuvaraj et al. [10] proposed a data privacy preservation method that balances the trade-off between privacy and utility by using deep adaptive clustering and elliptic curve digital signature algorithm to preserve privacy while maintaining data usefulness.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 05, May-2023

Rubai, S. M. [11] proposed a hybrid heuristic-based key generation protocol for privacy preservation of data in cloud computing that aims to generate unique keys for each user to preserve data privacy in cloud environments. Xu et al. [12] presented an energy-efficient cloudlet management approach for privacy preservation in metropolitan area networks that manages cloudlets efficiently to reduce power consumption and preserve privacy. Aminifar et al. [13] proposed randomized tree algorithm for privacy preservation in distributed structured health data that shares data between different parties while preserving privacy.

Bedi and Goyal [14] suggested an Extended Fully Homomorphic Encryption (EFHE)-based approach for privacy preservation in medical data in cloud IoT to provide secure and privacy-preserving access to patient's medical data in cloud IoT environments. Kathamuthu et al. [15] proposed a deep Q-learning-based neural network with privacy preservation technique for secure data transmission in IOT healthcare applications to improve data security and privacy. Ren and Zhang [16] proposed a new data model for protection of medical images using a combination of watermarking and encryption techniques to protect the privacy of medical images. Cano and Cañavate-Sanchez [17] proposed a dual signature ECDSA-based approach for preserving patient's data privacy in the Internet of Medical Things (IoMT) to ensure secure and private communication between IoMT devices and healthcare systems.

Shen et al. [18] discussed the challenges and opportunities of integrating, modeling, and simulating large-scale biomedical data in the period of big data and translational medicine. They provided an overview of the various types of biomedical data, the various data sources, and the techniques used for data integration, modeling, and simulation. Park and Lee [19] proposed a privacy-preserving k-nearest neighbor (k-NN) algorithm for medical diagnosis in e-health cloud that

III CONCLUSION AND FUTURE WORK

Our work's main focus is on emphasizing the necessity for privacy-preservation methods when we transfer EHR data to the cloud. This satisfies the security, integrity, and validity requirements for confidentiality, according to the theoretical analysis of the methodologies. We discussed privacy strategies together with their benefits, drawbacks, and relevance to the taxonomy of different data kinds. Medical data manipulation requires a crucial protective method to guarantee data privacy. In general, encryption techniques are recommended to alleviate privacy concerns, but their effectiveness must be increased without compromising the secrecy of data. In order to significantly increase the level of privacy and the usefulness of, we are working to close the gap in selecting the ideal mix of privacy methods and privacy models. We anticipate improving this prototype through meticulous simulations of scalability and comparisons with various potential configurations as health data increases every year.

IV COMPARATIVE ANALYSIS

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 05, May-2023

TITLE	TECHNOLOGY	ALGORITHM	FUTURE WORK	SPECIFICATION	LIMITATION
Based on Zero-Knowledge Proof, Blockchain Data Privacy Protection and Sharing Scheme [1]	Blockchain	Zero-Knowledge Proof	safe exchange of data without a third-party server and the realisation of a completely decentralised data sharing scheme.	accomplish data sharing secrecy and accuracy, as well as data sharing validity and consistency	It cannot guarantee the data's accuracy and consistency. .
Big Data Privacy Preservation Using Principal Component Analysis and Random Projection in Healthcare [2]	Big Data and machine learning	Random Projection, Principal Component Analysis	—	the suggested technique outperforms traditional techniques in terms of runtime, accuracy, efficiency, mean absolute error, kappa statistic measure, and F-measurer, even after the perturbation	It works on large set of data
Privacy-Preserving Density Distribution Using GANs on Mobility Data[3]	GANs, Machine learning, Deep learning	Generative Adversarial Networks (GANs)	—	On data usefulness and privacy-preservation, the strategy outperforms the alternatives.	—
A Blockchain and Cloud Computing-Based Medical Data Privacy Protection Scheme[4]	Blockchain, Cloud computing	Attribute-based encryption and proxy reencryption	Improving the consensus method, fine-grained management of cloud data, and reducing duplicate data storage overhead	It can not only do cloud data integrity testing but also perform broader security encryption computing.	—
A Quasi-Identifier Recognition Algorithm for Cloud Data Privacy Preservation Based on Risk Reidentification[5]	Cloud Computing,	quasi-identifier recognition algorithm	—	Alogirthm tested on real dataset and result demonstrated that it reduces privacy leakage and manintain data utility.	—
Blockchain-based privacy-preserving e-health solution for cloud-based healthcare data[6]	Blockchain, Cloud computing, E-health	pairing-based cryptography, blockchain	—	Present the system model, threat model, and security aim, followed by the suggested system's design specifics.The technology generates tamper-proof records from patients' EHRs using pairing-based encryption, which are then incorporated into legitimate transactions and posted to the blockchain.	—

TITLE	TECHNOLOGY	ALGORITHM	FUTURE WORK	SPECIFICATION	LIMITATION
In cloud computing, a privacy-preserving system based on Gaussian mutations is used to optimise firebugs. [7]	cloud computing, privacy preservation, optimization	The firefly method is based on Gaussian mutations.	——	suggested a privacy protection architecture employing gaussian mutation based firefly algorithm. The trials are carried out utilising three distinct healthcare datasets: HPD, Medical MIMIC-III, and MHEALTH.	data hiding and data restoration operations are considered as two significant operations of the proposed framework
Taxonomy, privacy standards, feasibility analysis, and prospects for privacy protection in the e-health cloud [8]	E-health, cloud computing, privacy preservation	SKE hybrid cloud, ABE encryption, CP-ABE.	Identification and mitigation of privacy leaks for cloud-based EHRs in real-world dataset settings also require thorough examination.	did a thorough investigation to undertake an in-depth review of privacy protecting approaches in e-health cloud	——
The problems of e-health solutions in cloud computing in terms of security and privacy [9].	Cloud computing, data privacy, EHR, and security	Attribute Based Encryption (ABE), KP-ABE, and CP-ABE are all types of encryption.	——	Studies must focus on efficient complete security measures for EHR, as well as approaches to safeguard the integrity and confidentiality of patients' information.	——
Deep adaptive clustering and the elliptic curve digital signature technique are used to protect data privacy and strike a balance between privacy and utility. [10]	cloud computing, cryptography	Deep Adaptive Clustering (DAC) with Elliptic Curve Digital Signature Algorithm (ECDSA) privacy	——	The utility is carried out by clustering the input datasets with DAC, and the privacy is protected by ECDSA.	——
Energy-Efficient Cloudlet Management for Wireless Metropolitan Area Network Privacy Preservation [12]	Cloud Computing	VM MigrationTechnique (Virtual Machine)	to consider both cloudlet load balancing and cloudlet energy usage.	to minimise cloudlet energy usage while maintaining privacy in WMAN.	——
Extremely Randomised Trees for Distributed Structured Health Data with Privacy Preservation [13]	Artificial Intelligence , Machine Learning	k-PPD-ERT ALGO (Extremely Randomized Trees) ,	to investigate the possibilities of extending the suggested framework to situations in which the parties do not adhere to the honest-but-curious security model	We present a scalable privacy-preserving framework for distributed machine learning based on the very randomised trees technique, which has a linear overhead in terms of the number of participants and can accommodate missing information.	Such approaches do not give enough privacy protection.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 05, May-2023

TITLE	TECHNOLOGY	ALGORITHM	FUTURE WORK	SPECIFICATION	LIMITATION
Using Extended Fully Homomorphic encryption to protect the privacy of personalised medical data in the cloud IoT [14],	Cloud Computing , IOT	Fully Homomorphic encryption	using hybrid encryption techniques to improve data privacy and security	Long-term privacy-preserving for encrypted data is achieved through the proposed encryption model and p The suggested encryption architecture achieves long-term privacy preservation for encrypted data while also providing efficient, safe, and reliable cloud-IoT applications.	When compared to alternative encryption procedures, the fault tolerant paradigm has a high system complexity.
Deep Q-Learning-Based Neural Network with Privacy Preservation Method for Secure Data Transmission in Internet of Things (IoT) Healthcare Application [15]	IOT , Deep Learning , Cryptography	Deep Q-learning-based neural network with privacy preservation method (DQ-NNPP)	nonoptimized data searching in a deep-learning concept to improve security.	The proposed DQNNPP architecture overcomes the challenges of security and privacy threats. The paper presents a new approach called ciphertext-policy attribute-based privacy preservation (CPABPP), which utilizes private, public, and master keys to develop a patient-centric access control system in electronic medical sectors. This approach ensures both security and privacy by combining the advantages of different key types.	more training time is required for complex DNNs in the core clouds compared to existing traditional methods
A New Data Model for the Privacy Protection of Medical Images [16]	IoMT(Internet of Medical Things), Artificial Intelligence	SVM (Support Vector Machines) , PCA (Principal Component Analysis)	To address the issue of noise interference in VC image restoration, we leverage the advancements in deep neural networks for image denoising. Consequently, we propose a denoising neural network specifically designed.	Additionally, the paper introduces an efficient and key-free data protection model based on virtual channels (VC) for transmitting medical data and storing templates.	Takes time to perform complex cryptographic operations and the communicating parties need to perform more steps to make an encrypted channel
Preserving Data Privacy in the Internet of Medical Things Using Dual Signature ECDSA [17]	IoMT(Internet of Medical Things), Cryptography, Artificial Intelligence	Elliptic curve digital signature algorithm (ECDSA) , AES(Advanced Encryption Standard)	——	focused on confidentiality, how to protect the anonymity of the object that generates the data, that data confidentiality can be added as another security layer depending on the energy and computational restrictions of the IoMT source device.	necessity of using physical smart cards and the congestion that could appear in case of a high number of IoMT devices
Integration, Modelling, and Simulation of Biomedical Data in the Age of Big Data and Translational Medicine [18]	Big Data	——	——	——	——
Privacy Preserving k-Nearest Neighbor for Medical Diagnosis in e-Health Cloud [19]	Cloud Computing , Machine Learning	k-nearest neighbor (kNN) , Case-based reasoning (CBR)	construct the privacy preserving and efficient protocols for other data mining techniques other than kNN to apply MPC.	It provides privacy of medical diagnosis dataset outsourced from multiple data owners as kNN result and hides the data access pattern. as the number of data, the length of data, or k increase, the number of rounds of PE-FTK does not increase.	number of rounds and the running time increases little as the number of data or k increases.

TITLE	TECHNOLOGY	ALGORITHM	FUTURE WORK	SPECIFICATION	LIMITATION
Sharing Information and Protecting Privacy in an Electronic Nursing Record Management System [20]	Blockchain	End-to-End Memory Neural Network	A comparison demonstrates that our approach outperforms others in terms of functional completeness, processing power, and CPU occupancy.	The consensus method offers a simplified consensus process and facilitates quick connections, rapid synchronisation, and effective information sharing across ENR nodes..	The ENR management system is overly reliant on a centralised process
Healthchain: A unique framework for preserving the privacy of electronic health records through the use of blockchain technology [21].	Blockchain	SHA-256	future work could focus on improving the scalability and efficiency of Healthchain, as well as exploring the potential for integrating other emerging technologies like artificial intelligence and the internet of things.	A unique framework for maintaining the privacy of electronic health records utilising blockchain technology. However, the authors emphasise that significant hurdles remain, including scalability and integration with existing health information systems.	Further testing on real-world data would be needed to validate its effectiveness.
Privacy protection in e-healthcare environments: current state and future directions [22].	E-Healthcare	RBAC, IABA	To protect sensitive data, such as Secure Multiparty Computation (SMC) and Differential Privacy. Additionally, the paper calls for more research on how to improve patient trust and engagement in e-healthcare systems.	It examines the legal and regulatory frameworks around healthcare privacy, such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States.	There are no specific methods or strategies for preserving privacy in e-healthcare..
Cloud security in EHR design for Indian healthcare services [23]	Cloud computing, Electronic Health Record (EHR)	Elgamal algorithm	Improving the security of cloud-based EHR systems through improved authentication and access control measures, as well as data privacy through encryption and anonymization approaches.	A safe cloud-based EHR solution for use in Indian healthcare. To maintain the security and privacy of patient data, the proposed system includes safeguards such as encryption, authentication, and access restriction.	It may not be applicable to healthcare services in other regions or countries.
PSMPV stands for patient-controlled and multi-level privacy-protecting cooperative validation in distributed M-Healthcare cloud computing. [24]	Distributed M-Healthcare, Cloud computing	Signature algorithm	increasing the planned PSMPV system's scalability and efficiency, as well as investigating the feasibility of using blockchain technology to improve security and privacy in distributed M-Healthcare systems	PSMPV solution for distributed cloud computing environments in M-Healthcare. To maintain the security and privacy of patient data, the proposed system includes mechanisms such as patient self-control and multi-level privacy protection.	It may not be applicable to all M-Healthcare cloud computing environments
DDoS attacks in SDN and cloud computing environments: a survey [25].	Cloud computing and software-defined networking (SDN).	The NetFPGA stqage design is built on an openFlow switch.	enhancing security by creating more effective and efficient DDoS detection and mitigation strategies in SDN and cloud computing settings, as well as investigating the possibility for applying machine learning and AI-based approaches.	A review of distributed denial of service (DDoS) attacks in cloud computing and software-defined networking (SDN) systems. The review examines numerous forms of DDoS assaults, their effects on SDN and cloud computing systems, and various detection and mitigation approaches.	the survey may not be comprehensive or up-to-date, as the field of DDoS attacks and defense is rapidly evolving.

TITLE	TECHNOLOGY	ALGORITHM	KEY WORDS	FUTURE WORK	SPECIFICATION	LIMITATION
Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology [26]	Blockchain technology, Electronic Health Records (EHRs)	Consensus quorumChain	Blockchain technology, Privacy-preserving, Access control, Interoperability	improving the scalability and efficiency of the proposed Ancile framework, as well as exploring the potential for integrating artificial intelligence (AI) and machine learning (ML) techniques to enhance privacy and security.	framework includes measures such as patient-controlled access and fine-grained authorization to ensure the privacy and security of EHRs.	specific algorithms or techniques used for the Ancile framework. Additionally, the proposed framework may face scalability and performance issues when dealing with large volumes of EHRs.
Healthcare in Cloud Using Multi-Level Privacy-Preserving Patient Self-Controllable Algorithm [27]	Cloud computing, Privacy-preserving algorithm	Multi-Level Privacy-Preserving Patient Self-Controllable Algorithm	Healthcare, Cloud computing, Privacy-preserving, Patient self-control, Multi-level, Algorithm	——	multi-level privacy-preserving patient self-controllable algorithm for healthcare in cloud computing environments. The algorithm aims to protect patient privacy and confidentiality while enabling patients to control the access and use of their healthcare data in cloud environments.	——
Privacy-Aware Access Control with Trust Management in Web Service [28]	Web service, trust management, access control	Access control management	Privacy, Access control, Trust management, Web service	focus on improving the efficiency and scalability of the proposed privacy-aware access control framework, as well as exploring the potential for integrating additional trust management models and techniques.	framework for web services that incorporates trust management mechanisms. The proposed framework includes measures such as policy-based access control and privacy preservation to ensure the privacy and security of web services.	the proposed framework may face performance and efficiency issues when dealing with large numbers of users and web services.
Ethereum: A Secure Decentralised Generalised Transaction Ledger [29]	Blockchain, decentralized computing	Ethash Algorithm	Ethereum, Blockchain, Decentralized computing, Transaction ledger, Security	focus on improving the scalability, security, and usability of Ethereum, as well as exploring its potential applications beyond financial transactions, such as in the areas of identity verification and supply chain management.	Ethereum, a decentralized computing platform and transaction ledger based on blockchain technology. Ethereum allows developers to create and deploy decentralized applications, or "smart contracts", that can be executed automatically and securely without the need for intermediaries.	important to note that the technology is still relatively new and undergoing rapid development, which may lead to security and scalability issues. Additionally
Data Security and Privacy Management in Healthcare Applications and Clinical Data Warehouse Environment [30]	Healthcare Applications, Clinical Data Warehouse, Data Security, Privacy Management	Meteor, EDW, SIA	Healthcare Applications, Clinical Data Warehouse, Data Security, Privacy Management	the authors recommend the development of standards and guidelines for the use of such techniques to ensure that they are widely adopted and effectively implemented.	presents a case study of a clinical data warehouse implementation and discusses the security and privacy measures that were employed to protect patient data	——

V Conclusion

In conclusion, safeguarding the confidentiality of electronic health records (EHRs) is critical in maintaining patient privacy and preventing potential harm. The state of the art in EHR confidentiality involves implementing strict access controls, regular employee training, regular auditing, encryption, physical security, and disaster recovery and business continuity planning. By following these best practices, healthcare providers can ensure that patient information remains confidential, prevent unauthorized access or activity,

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 05, May-2023

and maintain patient trust. As EHRs continue to play a vital role in healthcare, it is essential to remain vigilant and stay up-to-date with the latest technologies and best practices to protect the confidentiality of electronic health records.

VI REFERENCES

[1] Feng, T., Yang, P., Liu, C., Fang, J., & Ma, R. (2022). Blockchain Data Privacy Protection and Sharing Scheme Based on Zero-Knowledge Proof. *Wireless Communications and Mobile Computing*, *2022*.
[2]Ratra, R., Gulia, P., Gill, N. S., & Chatterjee, J. M. (2022). Big Data Privacy Preservation Using Principal Component Analysis and Random Projection in Healthcare. *Mathematical Problems in Engineering*, *2022*.
[3] Yin, D., & Yang, Q. (2018). GANs based density distribution privacy-preservation on mobility data. *Security and Communication Networks*, *2018*.
[4] Huang, L., & Lee, H. H. (2020). A medical data privacy protection scheme based on blockchain and cloud computing. *Wireless Communications and Mobile Computing*, *2020*.
[5] Mansour, H. O., Siraj, M. M., Ghaleb, F. A., Saeed, F., Alkhammash, E. H., & Maarof, M. A. (2021). Quasi-Identifier recognition algorithm for privacy preservation of cloud data based on risk reidentification. *Wireless Communications and Mobile Computing*, *2021*.
[6] Zhang, G., Yang, Z., & Liu, W. (2022). Blockchain-based privacy preserving e-health system for healthcare data in cloud. *Computer Networks*, *203*, 108586.=
[7] Anand K., Vijayaraj, A., & Vijay Anand, M. (2022). Privacy preserving framework using Gaussian mutation based firebug optimization in cloud computing. *The Journal of Supercomputing*, *78*(7), 9414-9437.
[8] Kanwal, T., Anjum, A., & Khan, A. (2021). Privacy preservation in e-health cloud: taxonomy, privacy requirements, feasibility analysis, and opportunities. *Cluster Computing*, *24*(1), 293-317.
[9] Chenthara, S., Ahmed, K., Wang, H., & Whittaker, F. (2019). Security and privacy-preserving challenges of e-health solutions in cloud computing. *IEEE access*, *7*, 74361-74382.
[10] Yuvaraj, N., Praghash, K., & Karthikeyan, T. (2022). Data Privacy Preservation and Trade-off Balance Between Privacy and Utility Using Deep Adaptive Clustering and Elliptic Curve Digital Signature Algorithm. *Wireless Personal Communications*, *124*(1), 655-670.
[11] Rubai, S. M. (2022). Hybrid heuristic-based key generation protocol for intelligent privacy preservation in cloud sector. *Journal of Parallel and Distributed Computing*, *163*, 166-180.
[12] Xu, X., Huang, R., Dou, R., Li, Y., Zhang, J., Huang, T., & Yu, W. (2018). Energy-efficient cloudlet management for privacy preservation in wireless metropolitan area networks. *Security and Communication Networks*, *2018*.
[13] Aminifar, A., Shokri, M., Rabbi, F., Pun, V. K. I., & Lamo, Y. (2022). Extremely Randomized Trees With Privacy Preservation for Distributed Structured Health Data. *IEEE Access*, *10*, 6010-6027.
[14] Bedi, P., & Goyal, S. B. (2022). Privacy preserving on personalized medical data in cloud IoT using Extended Fully Homomorphic Encryption.
[15] Kathamuthu, N. D., Chinnamuthu, A., Iruthayanathan, N., Ramachandran, M., & Gandomi, A. H. (2022). Deep Q-Learning-Based Neural Network with Privacy Preservation Method for Secure Data Transmission in Internet of Things (IoT) Healthcare Application. *Electronics*, *11*(1), 157.
[16] Ren, L., & Zhang, D. (2022). A New Data Model for the Privacy Protection of Medical Images. *Computational Intelligence and Neuroscience*, *2022*.
[17] Cano, M. D., & Cañavate-Sanchez, A. (2020). Preserving data privacy in the internet of medical things using dual signature ECDSA. *Security and Communication Networks*, *2020*.
[18] Shen, B., Teschendorff, A. E., Zhi, D., & Xia, J. (2014). Biomedical data integration, modeling, and simulation in the era of big data and translational medicine. *BioMed research international*, *2014*.
[19] Park, J., & Lee, D. H. (2018). Privacy preserving k-nearest neighbor for medical diagnosis in e-health cloud. *Journal of healthcare engineering*, *2018*.
[20] Li, Q., Yu, H., & Li, W. (2022). Information Sharing and Privacy Protection of Electronic Nursing Record Management System. *Scientific Programming*, *2022*.
[21] Chenthara, S., Ahmed, K., Wang, H., Whittaker, F., & Chen, Z. (2020). Healthchain: A novel framework on privacy preservation of electronic health records using blockchain technology. *Plos one*, *15*(12), e0243043.
[22] Sahi, M. A., Abbas, H., Saleem, K., Yang, X., Derhab, A., Orgun, M. A., ... & Yaseen, A. (2017). Privacy preservation in e-healthcare environments: State of the art and future directions. *Ieee Access*, *6*, 464-478.
[23] Deshmukh, P. (2017). Design of cloud security in the EHR for Indian healthcare services. *Journal of King Saud university-computer and information sciences*, *29*(3), 281-287.
[24] Shaikh, N. S., & Raut, S. Y. (2016). International journal of engineering sciences & research technology PSMPV: Patient self-controllable and multi-level privacy-protecting cooperative validation in distributed M-Healthcare cloud computing. *Int. J. Eng. Sci. Res. Technol.*, *5*(7), 909-916.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 05, May-2023

[25] Dong, S., Abbas, K., & Jain, R. (2019). A survey on distributed denial of service (DDoS) attacks in SDN and cloud computing environments. *IEEE Access*, *7*, 80813-80828.
[26] Dagher, G. G., Mohler, J., Milojkovic, M., & Marella, P. B. (2018). Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. *Sustainable cities and society*, *39*, 283-297.
[27] imrana Fatima, S., & Siddiqui, S. HEALTHCARE IN CLOUD USING MULTI-LEVEL PRIVACY-PRESERVING PATIENT SELF-CONTROLLABLE ALGORITHM.
[28] Li, M., Sun, X., Wang, H., Zhang, Y., & Zhang, J. (2011). Privacy-aware access control with trust management in web service. *World Wide Web*, *14*, 407-430.
[29] Wood, G. (2014). Ethereum: A secure decentralized generalized transaction ledger. *Ethereum project yellow paper*, *151*(2014), 1-32.
[30] Puppala, M., He, T., Yu, X., Chen, S., Ogunti, R., & Wong, S. T. (2016, February). Data security and privacy management in healthcare applications and clinical data warehouse environment. In *2016 IEEE-EMBS International Conference on Biomedical and Health Informatics (BHI)* (pp. 5-8). IEEE.
[31] Pussewalage, H. S. G., & Oleshchuk, V. A. (2016). Privacy preserving mechanisms for enforcing security and privacy requirements in E-health solutions. *International Journal of Information Management*, *36*(6), 1161-1173.
[32] Wang, W., Chen, L., & Zhang, Q. (2015). Outsourcing high-dimensional healthcare data to cloud with personalized privacy preservation. *Computer Networks*, *88*, 136-148.
[33] Abbas, A., & Khan, S. U. (2014). A review on the state-of-the-art privacy-preserving approaches in the e-health clouds. *IEEE journal of Biomedical and health informatics*, *18*(4), 1431-1441.
[34] Anwar, M., Joshi, J., & Tan, J. (2015). Anytime, anywhere access to secure, privacy-aware healthcare services: Issues, approaches and challenges. *Health Policy and Technology*, *4*(4), 299-311.
[35] Yu, S., Wang, C., Ren, K., & Lou, W. (2010, March). Achieving secure, scalable, and fine-grained data access control in cloud computing. In *2010 Proceedings IEEE INFOCOM* (pp. 1-9). Ieee.
[36] Masud, M. A. H., Huang, X., & Islam, M. R. (2014). A Novel Approach for the Security Remedial in a Cloud-based E-learning Network. *Journal of Networks*, *9*(11), 2934.
[37] Younis, Y. A., Kifayat, K., & Merabti, M. (2014). An access control model for cloud computing. *Journal of Information Security and Applications*, *19*(1), 45-60.
[38] Zhang, E., Li, M., Yiu, S. M., Du, J., Zhu, J. Z., & Jin, G. G. (2021). Fair hierarchical secret sharing scheme based on smart contract. *Information Sciences*, *546*, 166-176.
[39] Feldman, P. (1987, October). A practical scheme for non-interactive verifiable secret sharing. In *28th Annual Symposium on Foundations of Computer Science (sfcs 1987)* (pp. 427-438). IEEE.
[40] Zhang, E., Peng, J., & Li, M. (2018). Outsourcing secret sharing scheme based on homomorphism encryption. *IET Information Security*, *12*(1), 94-99.
[41] Keshta, I., & Odeh, A. (2021). Security and privacy of electronic health records: Concerns and challenges. *Egyptian Informatics Journal*, *22*(2), 177-183.
[42] Singh, S., Rathore, S., Alfarraj, O., Tolba, A., & Yoon, B. (2022). A framework for privacy-preservation of IoT healthcare data using Federated Learning and blockchain technology. *Future Generation Computer Systems*, *129*, 380-388.
[43] Ramesh, D., Mishra, R., Atrey, P. K., Edla, D. R., Misra, S., & Qi, L. (2023). Blockchain based efficient tamper-proof EHR storage for decentralized cloud-assisted storage. *Alexandria Engineering Journal*, *68*, 205-226.
[44] Varghese, B., & Buyya, R. (2018). Next generation cloud computing: New trends and research directions. *Future Generation Computer Systems*, *79*, 849-861.
[45] Liu, J., Li, X., Ye, L., Zhang, H., Du, X., & Guizani, M. (2018, December). BPDS: A blockchain based privacy-preserving data sharing for electronic medical records. In *2018 IEEE Global Communications Conference (GLOBECOM)* (pp. 1-6). IEEE.
[46] Chen, S. W., Chiang, D. L., Liu, C. H., Chen, T. S., Lai, F., Wang, H., & Wei, W. (2016). Confidentiality protection of digital health records in cloud computing. *Journal of medical systems*, *40*, 1-12.
[47] Huang, L. C., Chu, H. C., Lien, C. Y., Hsiao, C. H., & Kao, T. (2009). Privacy preservation and information security protection for patients' portable electronic health records. *Computers in Biology and Medicine*, *39*(9), 743-750.
[48] Chenthara, S., Ahmed, K., Wang, H., & Whittaker, F. (2019). Security and privacy-preserving challenges of e-health solutions in cloud computing. *IEEE access*, *7*, 74361-74382.
[49] Yi, X., Miao, Y., Bertino, E., & Willemson, J. (2013, December). Multiparty privacy protection for electronic health records. In *2013 IEEE Global Communications Conference (GLOBECOM)* (pp. 2730-2735). IEEE.
[50] Li, P., Guo, S., Miyazaki, T., Xie, M., Hu, J., & Zhuang, W. (2016). Privacy-preserving access to big data in the cloud. *IEEE Cloud Computing*, *3*(5), 34-42.
[51] Zhang, R., & Liu, L. (2010, July). Security models and requirements for healthcare application clouds. In *2010 IEEE 3rd International Conference on cloud Computing* (pp. 268-275). IEEE.
[52] Ahmed, M., & Barkat Ullah, A. S. (2018). False data injection attacks in healthcare. In *Data Mining: 15th Australasian Conference, AusDM 2017, Melbourne, VIC, Australia, August 19-20, 2017, Revised Selected Papers 15* (pp. 192-202). Springer Singapore.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 05, May-2023

[53] AbuKhousa, E., Mohamed, N., & Al-Jaroodi, J. (2012). e-Health cloud: opportunities and challenges. *Future internet*, *4*(3), 621-645.

[54] Calvillo-Arbizu, J., Román-Martínez, I., & Roa-Romero, L. M. (2014, June). Standardized access control mechanisms for protecting ISO 13606-based electronic health record systems. In *IEEE-EMBS International Conference on Biomedical and Health Informatics (BHI)* (pp. 539-542). IEEE.

[55] Khalid, N., Qayyum, A., Bilal, M., Al-Fuqaha, A., & Qadir, J. (2023). Privacy-preserving artificial intelligence in healthcare: Techniques and applications. Computers in Biology and Medicine, 106848.

[56] Durham, E., Xue, Y., Kantarcioglu, M., & Malin, B. (2012). Quantifying the correctness, computational complexity, and security of privacy-preserving string comparators for record linkage. Information Fusion, 13(4), 245-259.