iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** III **Month of publication:** March 2023

DOI: https://doi.org/10.22214/ijraset.2023.49781

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue III Mar 2023- Available at www.ijraset.com

A Review on Privacy Preserving Using Machine learning and Deep Learning Techniques

Amit Rajput[1], Suraksha Tiwari[2]
[1, 2]*Shriram College of Engineering & Management, Dist. Morena, Pin-476444, India*

Abstract: ***In order to entice data custodians to provide precise documentation so that data mining can continue with confidence, protecting the confidentiality of healthcare data is crucial. Association rule mining has been extensively used in the past to analyze healthcare data. The majority of applications ignore the drawbacks of specific diagnostic procedures in favor of positive association criteria. Negative association criteria may provide more useful information when bridging disparate diseases and medications than positive ones. In the case of doctors and social groups, this is particularly accurate. Data mining for medical purposes must be done with patient identities protected, especially when working with sensitive data. However, it might be attacked if this information becomes public. In order to perform data mining research, technology that modifies data (data sanitization) that reconstructs aggregate distributions has recently addressed the importance of healthcare data privacy. This study examines data sanitization in healthcare data mining using metaheuristics in order to safeguard patient privacy. Studies on SHM have looked at the uses of IoT &/or Machine Learning (ML) within the field, as well as the architecture, security, & privacy issues. However, no studies have looked into how AI and ubiquity computing technologies have affected SHM systems. The objective of this research is to identify and map the primary technical concepts within the SHM framework.***
Keywords: Healthcare data mining, machine learning, and privacy-preserving data mining.

I. INTRODUCTION

In an effort to enhance patient care and boost healthcare delivery efficiency, several healthcare institutions use electronic health records (EHRs)[1] on a large scale. In automating that data management process in challenging clinical settings, the EHR system speeds up clinician productivity[2][3]. These EHRs, when properly used, not only make many mundane medical duties easier, but also aid in the precise diagnosis of diseases. access to people's personal data EHRs make it easier to maintain medical records. Additionally, a home health tracking device is available to patients, enabling them to continuously monitor and evaluate their symptoms. For medical research to be of higher caliber, data from of the EMR system must be shared. These data are used by researchers to carry out a variety of data mining tasks[4], such as classification (predict the occurrence of diabetes), clustering (identify risks), and statistical tests (correlation between body mass index and diabetes), or query replying[5]. Healthcare researchers are anticipated to benefit from the integration of data and electronic medical records, which should also improve the actualized patient care[6].

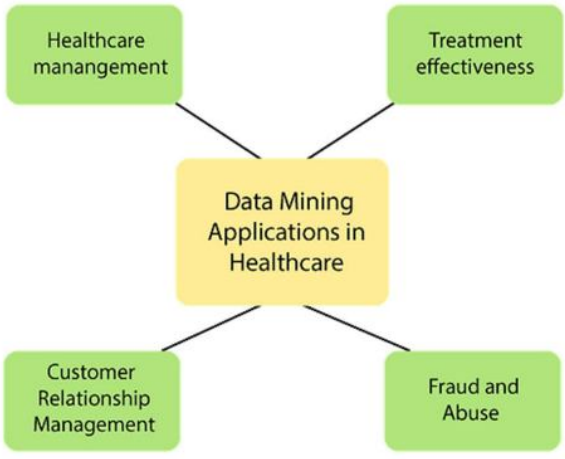


Fig.1 healthcare data mining applications.

Figure 1 displays the main applications of data mining in healthcare; see for additional details.[7] The literature has suggested using both encryption and anonymization-based techniques to achieve privacy. Researchers use anonymization frequently because it has lower transmission & computing costs than its rival cryptographic techniques[8]. The loss of information is a major issue with an anonymization-based approach. Information loss occurs when the difference among the original databases and the anonymized database is calculated. Information loss rises with a higher level of generalization and/or suppression technique. In general, there should be minimal information loss to increase the usefulness of the data[9].

Sensitive information can be more difficult to distinguish from non-sensitive information thanks to privacy-preserving measures that aim to prevent the leakage of sensitive information. But they don't rule out the possibility of finding inference laws[10][11]. Therefore, in recent years, experts have concentrated their attention on association norms that protect personal information. Throughout a wide range of industry areas, such as marketing, forecasting, diagnostics, or security, association rule mechanisms have been widely used in businesses and industrial corporations. Output privacy is a division of PPDM that includes sensitive association rule concealment. Restrictive regulations are ones that ought to be kept under wraps. Data sanitization is one of the PPDM methods used to conceal sensitive information[12].

II. RELATED WORK

Terziyan 2023 et al. Discuss a complex hybrid protection algorithm that requires the simultaneous use of two components: homeomorphic data space translation and synthetic data generation. The privacy for image data is given particular consideration. Special approaches to encryption and the creation of synthetic images are necessary due to the specifics of picture representation. To enable the latent feature vectors derived from the photos to be combined with privacy protection algorithms, We modified the hybrid algorithms consisting of homeomorphic transformation-as-encryption and synthetic picture generation in accordance with our recommendation to use trained (convolutional, variational) autoencoders with feature extractors. Showcase how a feature vector can be extracted, encrypted, and transformed into a secured representation using a feature extractor or encoder, a homeomorphic conversion into the latent space, and a convolutional variational autoencoder. [13].

Zapechnikov 2022 et al. In information security systems, practices, and protocols, algorithmic components receive the most attention. Systems that utilize both general-purpose modules for safe multi-party computations and specialized modules for protecting the privacy of certain machine learning techniques, like convolutional neural networks, from both passive and active attackers are taken into account. Examine actual PPML system prototype implementations. Conclusions regarding the aspects of the upcoming PPML systems are drawn in light of the analysis' findings[14].

Hamza 2022 et al. In applications based on wearable 5G devices, privacy and security are key considerations. The analysis of machine learning techniques that protect privacy is then offered. The implementation details of a study case of a secure prediction service which utilizes the Convolutional Neural Network (CNN) architecture and CKKS homomorphic encryption method are covered in the final section of this article. Particularly, we want to anticipate how security technologies will enhance the efficiency and usability of privacy-preserving artificial intelligence analytics in the 5G era and beyond, enabling the secure analysis of data from wearable devices[15].

Wang 2022 et al. In order to secure the cross-silo FL, it is suggested that the problem be solved using the Local Differential Privacy (LDP) approach using a three-plane structure. The fundamental conclusion to be drawn from this is how LDP can provide strong data privacy protection yet continuing to keep user data statistics intact and maintaining its high value. Our method is effective, as demonstrated by three real-world data sets used in experiments[16].

Field 2022 et al. research that shows. The infrastructure set up at each center was used to create a model that forecasts cardiovascular admission after a year of curative radiotherapy for non-small cell lung cancer. The model could be used to 802 of the 10,417 lung cancer patients who were identified. Twenty features were chosen for analysis from the medical record and associated registries. 8 characteristics were added after selection, and a logistic regression model generated out-of-sample data having an area under the receiver's operating characteristic (AUROC) curve = 0.70 & a C-index of 0.65. It was established that the infrastructure developed may be used to exchange routinely acquired oncology data between clinical centers and build models using federated learning. It provides a workable plan to enable further radiation oncology research studies utilizing real clinical data from patients[17].

Chen 2022 et al. An Architecture for Privacy-Preserving Federated Learning that is Practical and Effective (PEPFL). We first design a lifting global ElGamal cryptosystem in order to tackle the multi-key challenge for federated learning. In a subsequent step, we develop an efficient partially single instruction multiple data (PSIMD) parallelism approach that may encode a plaintext matrix into one plaintext for encryption, improving encryption efficiency and lowering communication costs in partially homomorphic

cryptosystems. Additionally, a novel convolutional neural network (CNN)-based federated learning framework with privacy preservation is built using momentum gradient descent and the established cryptosystem. (MGD). Finally, we evaluate PEPFL's usability and security. The experiment's results demonstrate the system's viability, effectiveness, security, and affordability in terms of communication and computation[18].

Wang 2022 et al. to reach thermodynamic equilibrium with the adjacent food components, the environment, and the environment. The movement of water in equilibrium (thermodynamics) & factors influencing the diffusion rate are two important parameters that impact the amount & rate of moisture migration. (dynamics of mass transfer). There are several ways to control water migration inside food systems, including adding an edible layer among them, altering the water action of food ingredients, altering the water's operational diffusivity, or altering the viscosity (molecular movement) of the trapped amorphous phases[19].

Abdel-Basset et al. data poisoning & inference are examples of privacy-related attacks. Federated learning (FL) has been seen as a promising method for providing distributed learning with secure intelligence in IoT applications. Even though there is considerable interest in creating FL that protects privacy, a great deal of studies only concentrate on FL that uses independently identically dispersed (i.i.d) data. The non-i. i.d. setting has only been briefly discussed in studies. It is commonly known that Generative Adversarial Network (GAN) attacks, where a hostile party could pose as a contributor taking an active role in the training process in order to steal the private information of other contributors, can be used against FL. The Privacy Protection-based Federation Deep Learning (PP-FDL) method shown in this research provides high rates of categorization utilizing non-i. d. data and data protection against privacy-related GAN assaults. The purpose of PP-FDL is to prohibit contributors from accessing one other's data while still enabling fog nodes to collaborate in order to train the FDL model[20]. A special private identity established for each class protects the class probability. Simple convolutional networks are trained on the MNIST & CIFAR-10 datasets and then put to the test to determine how well the PP-FDL architecture can classify images. The empirical results demonstrated the capability of PF-DFL to provide data security and the superior performance of the framework over the other three state-of-the-art models, with accuracy increases ranging from 3% to 8%[21].

Sav 2022 et al. To solve this issue, use PriCell, a federated learning-based method for complex models like convolutional neural networks. With the help of numerous healthcare organizations, PriCell's multiparty homomorphic encryption technology enables the cooperative development of encrypted neural networks. We protect the privacy of each institution's input data, any intermediate values, including the parameters of the trained models. We successfully and privately-protectedly duplicate the training of a documented state-of-the-art convolutional neural network (CNN) architecture. The accuracy of our solution is comparable to that of the centralized non-secure method. PriCell enables data utility for effective multi-center investigations involving complicated healthcare data while guaranteeing patient privacy[22].

Veeramakali 2022 et al. Choosing machine learning techniques should be based on solid results. We must apply each approach to the results in order to achieve this. The main problem appears during the training and validation of information. Eliminating errors could be challenging given the size of the dataset. In-depth presentations and comparisons are made of the providers, additional characteristics, different algorithms, data labeling methods, and assessment criteria. On the contrary hand, it's still early to detect unusual users on healthcare social networks. The result assessment layer explains how to assess and annotate the outcomes of the several algorithm selection layers. Finally, it anticipates further research in this field.

TABLE I. Literature Summary

Author/Year	Title	Method	Ref.
Lakshmanna/2022	Data Transmission Scheme in Clustered IIoT Environment Based on Deep Learning to Preserve Privacy	creates a revolutionary multi-agent system (MAS) that uses deep learning to protect privacy	[23]
Liu /2022	PPEFL: A Federated Learning Framework with an Edge for Privacy	federation learning's communication costs being cut	[24]
Qiang /2022	Intelligent Data Recognition and Machine Learning Based Privacy Protection	issue with privacy in machine learning.	[25]
Yu /2022	Using personal mobility data to anticipate transit modes using federated learning that protects privacy	a DNN Model	[26]
Venugopal /2022	Modeling Electronic Health Records with Privacy-Preserving Generative Adversarial Networks	KNN Model	[27]
Ma /2022	Internet of Automobiles in Satellite-Terrestrial Crowdsensing: A Blockchain-Based Privacy-Preserving Incentive Mechanism	Use blockchain to serve as a communication pathway between requesters and cars.	[28]

III. MACHINE LEARNING'S ROLE IN HEALTHCARE

We now perceive healthcare very differently as a result of the SHM. IoT sensors can gather information about a patient's surroundings, including their mobility, in real-time[29][30]. Finding previously undiscovered trends and details in the data is feasible utilizing machine learning (ML) / deep learning (DL) approaches as well as track the health of the patient to identify and alert to life-threatening illnesses[31]. ML, a branch of AI, uses mathematical and scientific methods to learn from the data and derive new insights, making healthcare apps smarter. Additionally, cognitive psychology is a synthesis of numerous scientific fields that employ AI, ML, and many other mathematical & scientific techniques to learn and obtain new insights[32]. It has a significant impact on how intelligent applications become. They covered how the potential for the health care system to be transformed by 5G, its accompanying technologies, AI, and ML in their essay[33]. Computing advancements known as cognitive technologies more closely mirror some aspects of how people think. As technology develops, we anticipate that the convergence of AI, ML, and SHM frameworks will become more pronounced. Data from "Electronic Health Records" (EHR) can help identify at-risk individuals and identify infection trends before symptoms appear[34]. These analytics may be made more accurate and offer healthcare providers with notifications that are quicker and more accurate by using ML and AI[35][36]. A new approach to customising medications to a person's genetic makeup may be made possible by ML algorithms and their capacity to synthesise extremely complicated information. For disease detection and patient emergency care, the massive data produced by medical equipment is a wonderful fit with ML capabilities. Using this approach, carers and medical professionals can identify patients who are at high risk and provide them with specialised treatment. AI has increased SHM's confidence and decreased the likelihood of human error. IoMT-based telemedicine, on the other hand, creates enormous volumes of data that must be transferred, processed, and stored. While scalable CC platforms can handle big data, ML algorithms must be expanded for faster analysis. But for more precision, availability, and real-time reactions, crucial healthcare infrastructure needs more sturdy architectures. Thus, there is a need for sophisticated cloud architecture that incorporates edge intelligence or fog computing (FC)[37].

IV. SECURITY & PRIVACY

Security can be summed up as controlling the legitimacy and establishing specific access guidelines for patient programs & information. With different computing systems and communication networks, the SHM framework utilizes IoMT. A key security problem that is no longer meticulously investigated is the growing usage of mobile & wearable technology in IoMT. Security in the IoMT is a major issue that is frequently handled with shoddy or default methods. Healthcare stakeholders are also less aware of computer security flaws and attacks[38][39]. In recent years, ransomware and other assaults have increasingly targeted medical data. Healthcare-related IoT privacy and security concerns, potential threats, attack vectors, and security setups have all been carefully examined. In order to deal with security risks, the well-known current security models are being examined. Finally, the essay outlined prospects, trends, and problems for the IoT in healthcare industry's future development. Message integrity and information secrecy are provided by "Information Security." Integrity in this context refers to preserving and guaranteeing the accuracy and completeness of data through its lifecycle. Confidentiality, on the other hand, is a privacy feature that imposes limited access to safeguard data from unauthorized access. The authors have addressed important concerns regarding security and privacy, crowdsourcing for the quick collecting of huge amounts of clinical data, open-source study hurdles, and potential IoMT considerations[40]. For the study of biosignal data, the authors suggested a framework that protects privacy and uses a clustering-based dispersed analysis method. A comprehensive and effective privacy and cyber security plan for contemporary health care networks, in our opinion, must address a number of factors. These include: 1. complete safety for software plus hardware; 2. Information security as well as confidentiality; 3. powerful encryption for data on networks; and 4. Patient privacy protection by regulators.

V. CONCLUSION

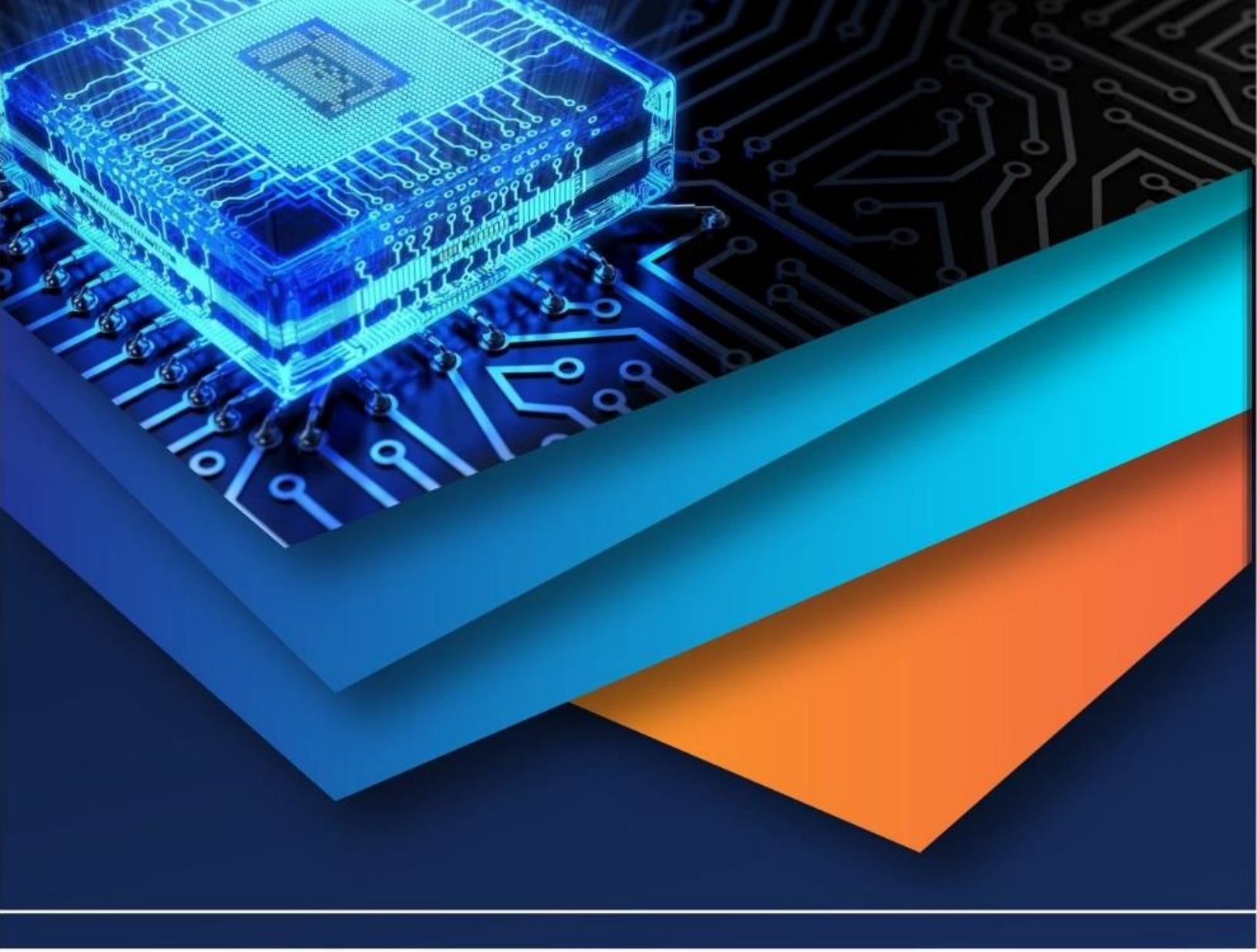
The confidentiality of healthcare information must be protected in order to persuade data custodians to offer reliable records so that data mining can proceed with confidence. Association rule mining has been extensively used in the past to analyze healthcare data. Most applications ignore the drawbacks of specific diagnostic techniques and instead concentrate on positive association rules. Positive association rules may not always yield the most valuable information when attempting to connect disparate illnesses and medications. In the case of doctors and social organizations, this is particularly accurate. Healthcare must use data mining with patient identity protection in mind, particularly when working with sensitive data. , it could be attacked openly, it could paraphrase this.

Recently, technology that alters data (data sanitization) also reconstructs aggregate distributions with the goal of undertaking data mining research has addressed the privacy of healthcare data. In order to protect patient privacy, this work investigates metaheuristic-based data sanitization in healthcare data mining. Studies on SHM have examined the framework, security, and individual concerns related to IoT &/or Machine Learning (ML) applications in the sector. However, no research has examined how AI & ubiquitous computing are progressing in SHM systems. The main technological concepts of the SHM framework are to be found and mapped out in this study.

REFERENCES

[1] T. Veeramakali, A. Shobanadevi, N. R. Nayak, S. Kumar, S. Singhal, and M. Subramanian, "Preserving the Privacy of Healthcare Data over Social Networks Using Machine Learning," Comput. Intell. Neurosci., vol. 2022, no. June 2012, 2022, doi: 10.1155/2022/4690936.
[2] J. D. Fernández, S. P. Menci, C. M. Lee, A. Rieger, and G. Fridgen, "Privacy-preserving federated learning for residential short-term load forecasting," Appl. Energy, vol. 326, no. April, p. 119915, 2022, doi: 10.1016/j.apenergy.2022.119915.
[3] X. Ma, Y. Zhou, L. Wang, and M. Miao, "Privacy-preserving Byzantine-robust federated learning," Comput. Stand. Interfaces, vol. 80, 2022, doi: 10.1016/j.csi.2021.103561.
[4] S. M. Darwish, R. M. Essa, M. A. Osman, and A. A. Ismail, "Privacy Preserving Data Mining Framework for Negative Association Rules: An Application to Healthcare Informatics," IEEE Access, vol. 10, no. June, pp. 76268–76280, 2022, doi: 10.1109/ACCESS.2022.3192447.
[5] C. Iwendi, S. A. Moqurrab, A. Anjum, S. Khan, S. Mohan, and G. Srivastava, "N-Sanitization: A semantic privacy-preserving framework for unstructured medical datasets," Comput. Commun., vol. 161, no. April, pp. 160–171, 2020, doi: 10.1016/j.comcom.2020.07.032.
[6] D. Mercier, A. Lucieri, M. Munir, A. Dengel, and S. Ahmed, "Evaluating Privacy-Preserving Machine Learning in Critical Infrastructures: A Case Study on Time-Series Classification," IEEE Trans. Ind. Informatics, vol. 18, no. 11, pp. 7834–7842, 2022, doi: 10.1109/TII.2021.3124476.
[7] L. Ren and D. Zhang, "A Privacy-Preserving Biometric Recognition System with Visual Cryptography," Adv. Multimed., vol. 2022, no. 1, 2022, doi: 10.1155/2022/1057114.
[8] K. Mivule, C. Turner, and S. Y. Ji, "Towards a differential privacy and utility preserving machine learning classifier," Procedia Comput. Sci., vol. 12, pp. 176–181, 2012, doi: 10.1016/j.procs.2012.09.050.
[9] S. Zapechnikov, "Contemporary trends in privacy-preserving data pattern recognition," Procedia Comput. Sci., vol. 190, no. 2019, pp. 838–844, 2021, doi: 10.1016/j.procs.2021.06.098.
[10] A. Girka, V. Terziyan, M. Gavriushenko, and A. Gontarenko, "Anonymization as homeomorphic data space transformation for privacy-preserving deep learning," Procedia Comput. Sci., vol. 180, pp. 867–876, 2021, doi: 10.1016/j.procs.2021.01.337.
[11] A. Ullah et al., "Fusion of Machine Learning and Privacy Preserving for Secure Facial Expression Recognition," Secur. Commun. Networks, vol. 2021, 2021, doi: 10.1155/2021/6673992
[12] Z. Zhou, Y. Tian, and C. Peng, "Privacy-Preserving Federated Learning Framework with General Aggregation and Multiparty Entity Matching," Wirel. Commun. Mob. Comput., vol. 2021, 2021, doi: 10.1155/2021/6692061.
[13] V. Terziyan, D. Malyk, M. Golovianko, and V. Branytskyi, "Encryption and Generation of Images for Privacy-Preserving Machine Learning in Smart Manufacturing," Procedia Comput. Sci., vol. 217, no. 2022, pp. 91–101, 2023, doi: 10.1016/j.procs.2022.12.205.
[14] S. Zapechnikov, "Secure multi-party computations for privacy-preserving machine learning," Procedia Comput. Sci., vol. 213, no. C, pp. 523–527, 2022, doi: 10.1016/j.procs.2022.11.100.
[15] R. Hamza and D. Minh-Son, "Research on privacy-preserving techniques in the era of the 5G applications," Virtual Real. Intell. Hardw., vol. 4, no. 3, pp. 210–222, 2022, doi: 10.1016/j.vrih.2022.01.007.
[16] C. Wang, X. Wu, G. Liu, T. Deng, K. Peng, and S. Wan, "Safeguarding cross-silo federated learning with local differential privacy," Digit. Commun. Networks, vol. 8, no. 4, pp. 446–454, 2022, doi: 10.1016/j.dcan.2021.11.006.
[17] M. Field et al., "Infrastructure platform for privacy-preserving distributed machine learning development of computer-assisted theragnostics in cancer," J. Biomed. Inform., vol. 134, no. April, p. 104181, 2022, doi: 10.1016/j.jbi.2022.104181.
[18] Y. Chen, B. Wang, H. Jiang, P. Duan, Y. Ping, and Z. Hong, "PEPFL: A framework for a practical and efficient privacy-preserving federated learning," Digit. Commun. Networks, 2022, doi: 10.1016/j.dcan.2022.05.019.
[19] N. Wang et al., "A blockchain based privacy-preserving federated learning scheme for Internet of Vehicles," Digit. Commun. Networks, 2022, doi: 10.1016/j.dcan.2022.05.020.
[20] G. Xu, H. Li, Y. Zhang, S. Xu, J. Ning, and R. H. Deng, "Privacy-Preserving Federated Deep Learning with Irregular Users," IEEE Trans. Dependable Secur. Comput., vol. 19, no. 2, pp. 1364–1381, 2022, doi: 10.1109/TDSC.2020.3005909.
[21] M. Abdel-Basset, H. Hawash, N. Moustafa, I. Razzak, and M. Abd Elfattah, "Privacy-preserved learning from non-iid data in fog-assisted IoT: A federated learning approach," Digit. Commun. Networks, 2022, doi: 10.1016/j.dcan.2022.12.013.
[22] S. Sav, J. P. Bossuat, J. R. Troncoso-Pastoriza, M. Claassen, and J. P. Hubaux, "Privacy-preserving federated neural network learning for disease-associated cell classification," Patterns, vol. 3, no. 5, p. 100487, 2022, doi: 10.1016/j.patter.2022.100487.
[23] K. Lakshmanna, R. Kavitha, B. T. Geetha, A. K. Nanda, A. Radhakrishnan, and R. Kohar, "Deep Learning-Based Privacy-Preserving Data Transmission Scheme for Clustered IIoT Environment," Comput. Intell. Neurosci., vol. 2022, 2022, doi: 10.1155/2022/8927830.
[24] Z. Liu, Z. Gao, J. Wang, Q. Liu, and J. Wei, "PPEFL: An Edge Federated Learning Architecture with Privacy-Preserving Mechanism," Wirel. Commun. Mob. Comput., vol. 2022, 2022, doi: 10.1155/2022/1657558.
[25] Q. Liu, "Privacy Protection Technology Based on Machine Learning and Intelligent Data Recognition," Secur. Commun. Networks, vol. 2022, 2022, doi: 10.1155/2022/1598826.
[26] F. Yu, Z. Xu, Z. Qin, and X. Chen, "Privacy-preserving federated learning for transportation mode prediction based on personal mobility data," High-Confidence Comput., vol. 2, no. 4, p. 100082, 2022, doi: 10.1016/j.hcc.2022.100082.

[27] R. Venugopal, N. Shafqat, I. Venugopal, B. M. J. Tillbury, H. D. Stafford, and A. Bourazeri, "Privacy preserving Generative Adversarial Networks to model Electronic Health Records," Neural Networks, vol. 153, pp. 339–348, 2022, doi: 10.1016/j.neunet.2022.06.022.
[28] Z. Ma, Y. Wang, J. Li, and Y. Liu, "A Blockchain Based Privacy-Preserving Incentive Mechanism for Internet of Vehicles in Satellite-Terrestrial Crowdsensing," Wirel. Commun. Mob. Comput., vol. 2022, 2022, doi: 10.1155/2022/4036491.
[29] M. A. P. Chamikara, P. Bertok, I. Khalil, D. Liu, and S. Camtepe, "Privacy preserving distributed machine learning with federated learning," Comput. Commun., vol. 171, no. April 2020, pp. 112–125, 2021, doi: 10.1016/j.comcom.2021.02.014.
[30] F. Zerka et al., "Privacy preserving distributed learning classifiers – Sequential learning with small sets of data," Comput. Biol. Med., vol. 136, no. July, p. 104716, 2021, doi: 10.1016/j.compbiomed.2021.104716.
[31] R. Aljably, Y. Tian, and M. Al-Rodhaan, "Preserving Privacy in Multimedia Social Networks Using Machine Learning Anomaly Detection," Secur. Commun. Networks, vol. 2020, 2020, doi: 10.1155/2020/5874935.
[32] Z. Song, Y. Ren, and G. He, "Privacy-Preserving KNN Classification Algorithm for Smart Grid," Secur. Commun. Networks, vol. 2022, 2022, doi: 10.1155/2022/7333175.
[33] T. Kim, Y. Oh, and H. Kim, "Efficient Privacy-Preserving Fingerprint-Based Authentication System Using Fully Homomorphic Encryption," Secur. Commun. Networks, vol. 2020, 2020, doi: 10.1155/2020/4195852.
[34] Y. Zou et al., "Improved Cloud-Assisted Privacy-Preserving Profile-Matching Scheme in Mobile Social Networks," Secur. Commun. Networks, vol. 2020, 2020, doi: 10.1155/2020/4938736.
[35] S. Zapechnikov, "Privacy-Preserving Machine Learning as a Tool for Secure Personalized Information Services," Procedia Comput. Sci., vol. 169, no. 2019, pp. 393–399, 2020, doi: 10.1016/j.procs.2020.02.235.
[36] Y. Chen, Z. Lu, H. Xiong, and W. Xu, "Privacy-Preserving Data Aggregation Protocol for Fog Computing-Assisted Vehicle-to-Infrastructure Scenario," Secur. Commun. Networks, vol. 2018, 2018, doi: 10.1155/2018/1378583.
[37] C. Xu, X. Shen, L. Zhu, and Y. Zhang, "A Collusion-Resistant and Privacy-Preserving Data Aggregation Protocol in Crowdsensing System," Mob. Inf. Syst., vol. 2017, 2017, doi: 10.1155/2017/3715253.
[38] Q. Huang, L. Wang, and Y. Yang, "Secure and Privacy-Preserving Data Sharing and Collaboration in Mobile Healthcare Social Networks of Smart Cities," Secur. Commun. Networks, vol. 2017, 2017, doi: 10.1155/2017/6426495.
[39] B. Kang, J. Wang, and D. Shao, "Certificateless Public Auditing with Privacy Preserving for Cloud-Assisted Wireless Body Area Networks," Mob. Inf. Syst., vol. 2017, 2017, doi: 10.1155/2017/2925465.
[40] Y. Sun, Q. Wen, Y. Zhang, and W. Li, "Privacy-preserving self-helped medical diagnosis scheme based on secure Two-party computation in wireless sensor networks," Comput. Math. Methods Med., vol. 2014, 2014, doi: 10.1155/2014/214841.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY