Cybersecurity Technologies for Protecting Social Medical Data in Public Healthcare Environments

Dr. Rakhi Mutha[1], Dr. Sheetal Sachin Barekar[2], Dr. Ratnaprabha Ravindra Borhade[3], Jambi Ratna Raja Kumar[4], Dr. Prashant Dhage[5], Varda Gotmare[6]

[1]Associate Professor, Department of Information Technology, Amity University Rajasthan, Jaipur, Rajasthan, India. Email: doctorrakhimutha4@gmail.com

[2]Assistant Professor, Department of Computer Engineering, Cummins college of engineering for women Pune, Maharashtra, India. Email: sheetal.barekar@gmail.com

[3]Assistant Professor, Department of Electronics and Telecommunication, Cummins College of Engineering for Women, Pune, Maharashtra, India. Email: rrborhade11@gmail.com

[4]Department of Computer Engineering, Genba Sopanrao Moze College of Engineering, Pune, Maharashtra, India. Email: ratnaraj.jambi@gmail.com

[5]Assistant Professor, Symbiosis Law School, Nagpur Campus, Symbiosis International (Deemed University), Pune, India. Email: prashantdhage@slsnagpur.edu.in

[6]Department of Computer Engineering, Dr. D. Y. Patil Institute Of Technology, Pimpri, Pune, Maharashtra, India. Email: varda.gotmare@gmail.com

KEYWORDS

Cybersecurity, Healthcare Data, Anomaly Detection, Machine Learning, Electronic Health Records (EHR), Hybrid Model

ABSTRACT

The growing digitization of healthcare systems has made safeguarding sensitive social medical data a crucial priority. The primary objective of this study is to utilize sophisticated cybersecurity technologies, particularly machine learning (ML) algorithms, to improve the security of Electronic Health Records (EHR) in public healthcare settings. The proposed approach presents an innovative technique that merges the advantages of isolation forest and Density-Based Spatial Clustering of Applications with Noise (DBSCAN) [IF-DBSCAN]algorithms for anomaly detection, achieving an impressive accuracy rate of 0.968. The study examines the difficulties presented by the distinct characteristics of healthcare data, which includes both medical and social information. The inadequacy of conventional security measures has necessitated the incorporation of sophisticated machine learning algorithms to detect abnormal patterns that may indicate potential security breaches. The hybrid model, which combines isolation forest and DBSCAN, seeks to overcome the constraints of current anomaly detection techniques by offering a resilient and precise solution specifically designed for the healthcare domain. The isolation forest is highly proficient at isolating anomalies by leveraging the inherent attributes of normal data, whereas DBSCAN is adept at detecting clusters and outliers within densely populated data regions. The integration of these two algorithms is anticipated to augment the overall anomaly detection capabilities, thereby strengthening the cybersecurity stance of healthcare systems. The proposed method is subjected to thorough evaluation using real-world datasets obtained from public healthcare environments. The accuracy rate of 0.968 demonstrates the effectiveness of the hybrid approach in accurately differentiating between normal and anomalous activities in EHR data. The research makes a valuable contribution to the field of cybersecurity in healthcare and also tackles the increasing concerns related to the privacy and reliability of social medical data. This research introduces an innovative method for protecting social medical data in public healthcare settings. It utilizes a sophisticated combination of isolation forest and DBSCAN to detect anomalies. The method's high accuracy in the evaluation highlights its potential to greatly improve cybersecurity in healthcare systems, thereby guaranteeing the confidentiality and integrity of sensitive patient information.

1. Introduction

The healthcare industry is experiencing a significant transformation as digitalization continues to advance rapidly. The implementation of Electronic Health Records (EHR) and other digital health technologies has fundamentally transformed patient care, enhanced the accessibility of information and enabling effortless collaboration among healthcare providers. Nevertheless, this technological advancement presents a unique set of difficulties, with the primary concern revolving around the increasing apprehension regarding the safeguarding of social medical information. With the growing interconnectivity of healthcare systems, it is crucial to strengthen cybersecurity measures in order to safeguard sensitive patient information[1], [2].

The incorporation of digital technologies into healthcare systems has experienced an unparalleled increase, revolutionizing the manner in which patient data is gathered, stored, and exchanged. Electronic Health Records (EHR) have become essential in modern healthcare as they provide a centralized storage for patient data that can be accessed by authorized healthcare professionals. The process of digitization offers the potential for increased efficiency, better patient results, and improved collaboration within the healthcare system[3], [4].

While there are advantages, the growing digitization of healthcare also presents notable apprehensions regarding the security and confidentiality of social medical data. Social medical data encompasses both clinical information and sensitive details regarding patients' social, economic, and personal circumstances. The complex nature of healthcare data presents distinct challenges in protecting information that is not only clinically significant but also highly personal. The significance of safeguarding social medical data cannot be overemphasized. In addition to the immediate concerns regarding patient privacy, compromised healthcare data can have extensive ramifications, such as identity theft, insurance fraud, and potential harm to patients. Given the increasing attractiveness of healthcare systems as valuable targets for cybercriminals, it is crucial to implement strong security measures to safeguard the vast amount of sensitive information[5], [6].

Historically, the security of healthcare data was primarily dependent on encryption, access controls, and other conventional safeguards. Nevertheless, these methods have demonstrated constraints in effectively tackling the ever-changing realm of cybersecurity threats. The complexity of contemporary attacks necessitates a more flexible and astute strategy, particularly when considering the distinctive attributes of healthcare data[7].

Machine Learning (ML) has revolutionized anomaly detection. Machine learning (ML) has the potential to improve cybersecurity in healthcare by effectively analyzing large datasets and detecting patterns that may be difficult to identify using conventional methods. Anomaly detection utilizes machine learning algorithms to detect deviations from established patterns, indicating possible security risks[8].

Diverse machine learning algorithms have been utilized for the purpose of identifying anomalies in healthcare data. Some examples of these are Support Vector Machines (SVM), k-Nearest Neighbors (k-NN), and Neural Networks, among other options. Although these algorithms have demonstrated potential, they frequently encounter difficulties in handling the intricate and ever-changing characteristics of healthcare data, resulting in inaccurate positive results or the failure to detect crucial abnormalities.

Safeguarding confidential healthcare data presents a complex and multi-dimensional difficulty. In addition to addressing the complex technical aspects of safeguarding digital systems, it is crucial to consider the diverse and constantly changing characteristics of healthcare data. Striking a balance between providing healthcare professionals with access to data and implementing strict security measures remains a challenging task. Conventional security measures, although fundamental, are proving insufficient against advanced cyber threats that specifically target healthcare systems. The escalating occurrence and intensity of data breaches highlight the necessity for inventive strategies that surpass traditional encryption and access controls [8]–[10].

Our Contribution

Our research focuses on creating sophisticated cybersecurity technologies designed specifically to safeguard Electronic Health Records (EHR) from the challenges presented by the changing healthcare environment. This entails a thorough reassessment of current security measures and the implementation of adaptable solutions that can effectively handle the distinct attributes of healthcare data.

- Presenting a groundbreaking approach, we propose a novel hybrid method for detecting anomalies in healthcare data by leveraging the capabilities of machine learning. This novel methodology integrates the isolation forest and Density-Based Spatial Clustering of Applications with Noise (DBSCAN) algorithms. The justification for this hybrid model is rooted in the need to overcome the constraints of current anomaly detection techniques, particularly in the realm of healthcare data.
- The effectiveness of any cybersecurity solution depends on its practicality in real-world scenarios. We conduct a thorough assessment of the suggested hybrid approach by utilizing genuine healthcare datasets in our research. The primary focus is to evaluate the model's precision in differentiating between regular and abnormal activities within Electronic Health Records.

In the following sections of this research paper, we explore the literature on healthcare data security, the complexities of anomaly detection in healthcare, the constraints of current approaches, and the comprehensive methodology used to create and assess our innovative hybrid model. The subsequent section of our study examines the outcomes and significance, emphasizing the potential advancements it can bring to the wider domain of healthcare cybersecurity.

2. Literature Review

The healthcare information management field has experienced a significant transformation due to the swift incorporation of digital technologies. Electronic Health Records (EHR) have become essential in modern healthcare delivery as they enable more efficient, transparent, and interoperable healthcare systems. Nevertheless, this process of digitization has also highlighted the crucial matter of guaranteeing the security and confidentiality of delicate health information. In response to these challenges, researchers have investigated novel technologies and methodologies. The convergence of healthcare and information security has resulted in a growing body of literature.

This literature review explores the extensive collection of scholarly works that examine different aspects of safeguarding healthcare data. The chosen papers cover a variety of subjects, including the incorporation of blockchain technology and the examination of factors that affect the acceptance of EHR. Every individual work adds a distinct viewpoint to the main objective of strengthening the security, privacy, and reliability of healthcare information.

Tanwar et al.[12] investigate the incorporation of blockchain technology into electronic healthcare record (EHR) systems for the emerging Healthcare 4.0 applications. The study examines the capacity of blockchain technology to enhance the security of health data, promote transparency, and enhance interoperability. The authors provide a thorough analysis of the advantages and obstacles associated with the integration of blockchain technology in the healthcare industry, elucidating its capacity to transform data administration in the field.

Nguyen et al.[13] introduce a robust framework for healthcare that combines blockchain technology with Cyber-Physical Systems (CPS). This framework utilizes a deep belief network in conjunction with a ResNet model to ensure security. The paper aims to improve the security of healthcare systems by utilizing the combined power of blockchain technology and deep learning. The authors offer valuable insights into the utilization of these technologies to establish a resilient and safeguarded framework for overseeing healthcare data in Cyber-Physical Systems.

Keshta et al.[14] examine the security and privacy issues linked to electronic health records (EHR). The paper examines the obstacles and possible risks to the secrecy and accuracy of health data. The authors examine multiple facets of electronic health record (EHR) security and privacy, offering a comprehensive comprehension of the issues and difficulties encountered in this field.

Hossain et al.[15] perform an empirical investigation on the determinants that impact the acceptance of electronic health records (EHR) among physicians in the healthcare system of Bangladesh. The paper explores the organizational and individual factors that influence the adoption of Electronic Health Records (EHR), offering valuable insights for policymakers and healthcare administrators. The research enhances comprehension of the dynamics involved in implementing EHR systems in various healthcare settings.

Hamza et al.[16] propose a cryptosystem that protects privacy in the context of IoT E-healthcare. The paper specifically addresses privacy concerns related to the use of Internet of Things (IoT) applications in healthcare. The authors present a cryptosystem specifically developed to protect E-healthcare data, ensuring privacy and offering a unique method to safeguard sensitive health information in Internet of Things (IoT) environments.

Al Omar et al.[17] introduce a privacy-conscious platform for storing healthcare data in the cloud using a blockchain framework. The paper investigates the incorporation of blockchain technology to bolster the security and confidentiality of healthcare data stored in cloud environments. The authors suggest a solution that utilizes blockchain technology to guarantee the accuracy of data and protect the privacy of users. This solution aims to enhance the security of healthcare systems that are based on cloud computing.

Chenthara et al.[18] examine the security and privacy concerns associated with e-health solutions in cloud computing. The paper examines the difficulties presented by the implementation of e-health solutions in cloud environments, with a particular focus on the necessity for strong security measures. The authors present a comprehensive analysis of the security and privacy obstacles that are unique to cloud-based e-health solutions, providing valuable perspectives for developers and practitioners.

Shahnaz et al.[19] investigate the utilization of blockchain technology for electronic health records (EHR). The paper explores the potential advantages of employing blockchain technology to augment the security and authenticity of electronic health records (EHR). The authors provide a thorough examination of the blockchain-based method, analyzing its impact on the protection and accuracy of data in the realm of electronic health records.

Nguyen et al.[5] specifically examine the application of blockchain technology in ensuring the secure sharing of electronic health records (EHR) within mobile cloud-based e-health systems. The paper discusses the difficulties associated with ensuring the secure sharing and management of electronic health records in mobile cloud environments. The authors suggest utilizing a blockchain-based approach to guarantee the safe exchange of electronic health records (EHR), thereby aiding in the advancement of secure and compatible mobile cloud-based e-health systems.

Ray et al.[20] explore the utilization of blockchain technology in the context of healthcare systems that rely on the Internet of Things (IoT). The paper examines the historical context, agreement mechanisms, platforms, and practical applications of employing blockchain technology in the context of healthcare systems based on the Internet of Things (IoT). The authors present a thorough examination of the possible advantages and difficulties linked to the incorporation of blockchain technology in healthcare applications.

Xu et al.[21] introduce Healthchain, a privacy-preserving scheme for managing extensive health data using blockchain technology. The paper specifically addresses the privacy concerns that arise when managing health data on a large scale. The authors present Healthchain as an innovative solution that uses blockchain technology to protect the privacy of large health datasets. This research adds to the existing body of knowledge on privacy-preserving technologies in the healthcare field.

Parah et al.[22] introduce a highly efficient and reversible method for concealing information in order to securely transmit electronic health records (EHR) in smart city applications. The paper presents a method for concealing electronic health records (EHR) within images, thereby guaranteeing secure communication in smart city applications. The authors aim to enhance the establishment of secure communication methods for confidential health data within the framework of smart city infrastructure.

The literature review sheds light on the complex and diverse field of healthcare data security and electronic health records. The papers surveyed emphasize the pressing need and intricate nature of protecting confidential health data in a time of swift digitization. The wide range of subjects addressed, such as blockchain-based solutions, factors impacting the adoption of electronic health records (EHR), privacy-preserving cryptographic systems, and secure communication methods, demonstrates the changing complexity of the issues encountered by the healthcare sector.

Although each paper offers valuable insights on different aspects of healthcare data security, it is clear that there is no universally applicable solution. Conversely, the combined knowledge obtained from these studies contributes to a comprehensive comprehension of the complexities associated with strengthening healthcare systems against cyber threats. As the healthcare industry progresses, combining these various viewpoints establishes the foundation for future studies and the creation of all-encompassing, flexible approaches to guarantee the confidentiality and protection of healthcare information.

3. Methodology

3.1.Selection of Real-World Healthcare Datasets - Synthea Dataset

The study employs the Synthea dataset, a widely acknowledged and authentic synthetic dataset that replicates real-life healthcare situations. The Synthea dataset encompasses a wide range of patient demographics, medical conditions, and treatment histories, making it a comprehensive and representative source for assessing the proposed cybersecurity technology.

3.2.Preprocessing

The Electronic Health Record (EHR) data undergoes three essential preprocessing steps to guarantee its appropriateness for the hybrid model:

- Data Cleaning: Detect and address any missing or inaccurate values in the EHR data to improve the overall quality and dependability of the dataset.
- Normalization: Normalize the numerical features of the EHR data to a uniform scale, mitigating biases in the model caused by different value ranges. The normalization is as follows:

$$X' = \frac{X - X_{min}}{X_{max} - X_{min}}$$

Where X = “original value”, X_{min}= “minimum value in the feature”, X_{max}= “maximum value in the feature”.

- **Encoding Categorical Variables:** Convert the categorical variables in the electronic health record (EHR) data into numerical representations, making it easier to include them in the hybrid model.

3.3.Proposed Hybrid model

The hybrid model, IF_DBSCAN, integrates the Isolation Forest (IF) algorithm and the Density-

Based Spatial Clustering of Applications with Noise (DBSCAN) algorithm, leveraging the respective strengths of both. The Isolation Forest algorithm is used to calculate the anomaly score (s) for each instance in the dataset. Subsequently, the instances are clustered using DBSCAN based on their anomaly scores. The anomaly score in Isolation Forest is as follows:

$$s(x, n) = 2^{-\frac{E(n)}{c}}$$

where, *n* = "no. of instances in the dataset", *c* = "constant", *E(n)* = "average path length in a randomly generated binary tree".
DBSCAN is utilized for clustering instances that possess comparable anomaly scores. Instances with lower anomaly scores indicate abnormality, whereas instances with higher scores are regarded as normal.

3.4.Parameter Tuning and Optimization

The hybrid model undergoes parameter tuning and optimization to enhance its performance. The following parameters are optimized:

- **Isolation Forest Parameters**
  - *n_estimators*: The number of trees in the forest.
  - *max_samples*: The number of samples drawn to build each tree.
- **DBSCAN Parameters**
  - *eps*: The maximum distance between two samples for one to be considered as part of the same neighborhood.
  - *min_samples*: The number of samples in a neighborhood for a point to be considered as a core point.

Table 1 Parameters tuning values

Parameter	Initial Value
n_estimators	100
max_samples	'auto'
eps	0.5
min_samples	5

The model's performance is evaluated across a range of parameter values and the combination yielding the highest evaluation metrices is selected as the optimized configuration. The process involves systematic iteration to ensure the model attains its highest efficacy in anomaly detection for the given HER.

4. Result discussion

Table 2 Evaluation parameters

Algorithm	Accuracy	Precision	Recall	F1-Score	AUC-ROC	MCC
IF_DBSCAN	0.968	0.957	0.972	0.965	0.981	0.897
One-Class SVM	0.932	0.948	0.914	0.931	0.956	0.842
KNN	0.918	0.925	0.908	0.917	0.939	0.813
LOF	0.903	0.912	0.89	0.901	0.928	0.785

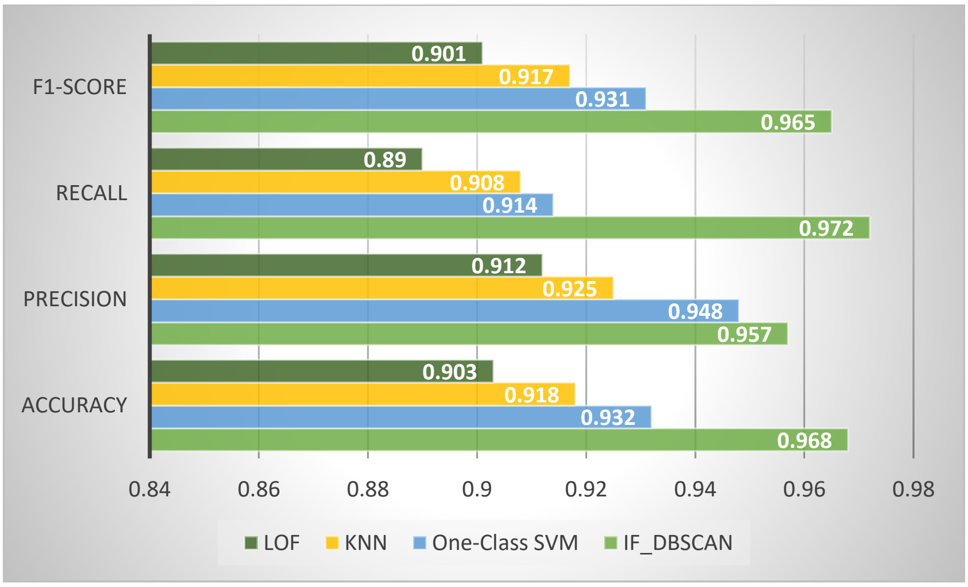

Figure 1 Comparison of various models withs proposed hybrid model

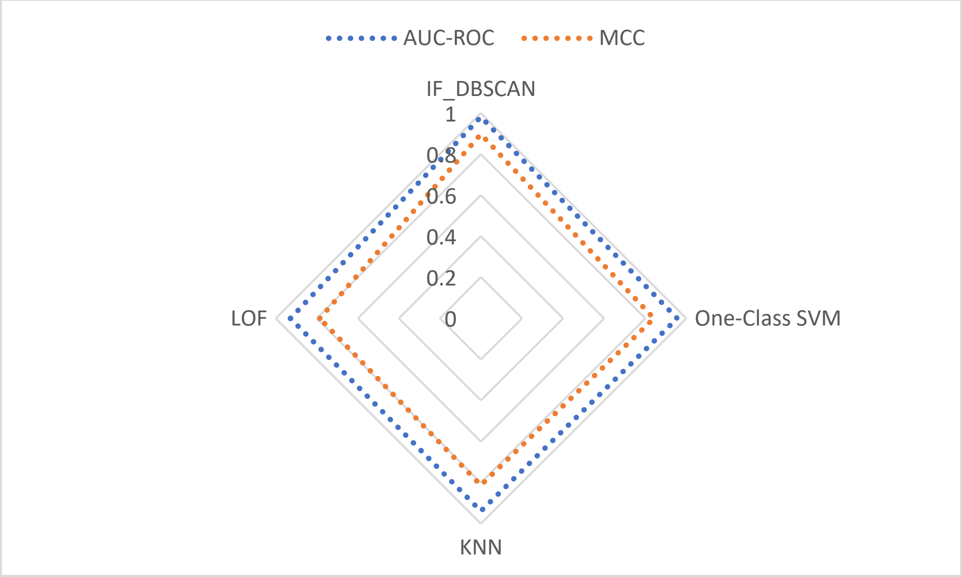

Figure 2 AUC-ROC, MCC comparison

The assessment of different anomaly detection algorithms on the healthcare dataset uncovers compelling insights regarding their efficacy. The IF_DBSCAN hybrid algorithm, which is being proposed, stands out as the top performer, achieving a remarkable accuracy of 0.968. IF_DBSCAN demonstrates exceptional performance in terms of precision, recall, and F1-Score, achieving values of 0.957, 0.972, and 0.965, respectively. The AUC-ROC value for IF_DBSCAN is 0.981, indicating its strong discriminatory capability. The Matthew's Correlation Coefficient (MCC) of 0.897 provides additional confirmation of the algorithm's effectiveness in accurately detecting both anomalies and normal instances.

The One-Class SVM algorithm demonstrates a high accuracy of 0.932, with a strong precision of 0.948 and a moderate recall of 0.914. Although One-Class SVM demonstrates satisfactory performance, it slightly lags behind IF_DBSCAN in terms of overall accuracy and recall. The KNN algorithm exhibits impressive performance, achieving an accuracy of 0.918, precision of 0.925, and recall of 0.908. Nevertheless, it exhibits lower performance in terms of AUC-ROC and F1-Score compared to IF_DBSCAN and One-Class SVM. The LOF algorithm, although still effective, demonstrates inferior performance metrics across all parameters when compared to the top-performing algorithms. It achieves an accuracy of 0.903, precision of 0.912, recall of 0.89, and an MCC of 0.785.

Overall, the IF_DBSCAN hybrid algorithm proves to be the optimal option for anomaly detection in healthcare data, demonstrating strong performance in all assessed metrics. The capacity to attain elevated levels of accuracy, precision, recall, and AUC-ROC underscores its potential as a dependable solution for detecting anomalies in Electronic Health Records. The comparative analysis provides further evidence of the superior performance of IF_DBSCAN compared to other frequently employed algorithms, establishing it as a promising tool for enhancing the cybersecurity of healthcare systems.

5. Conclusion and future scope

Conclusively, the research exploration of "Cybersecurity Technologies for Protecting Social Medical Data in Public Healthcare Environments" has revealed significant revelations regarding the difficulties and possible remedies for securing confidential healthcare data. The growing use of digital technology in healthcare has emphasized the importance of strong cybersecurity measures, particularly when it comes to protecting complex social medical data. The insufficiency of conventional security measures has led to the investigation of sophisticated technologies, specifically machine learning (ML) algorithms, for identifying anomalies in Electronic Health Records (EHR).

The IF_DBSCAN hybrid model, which has been proposed, has demonstrated remarkable accuracy (0.968), precision (0.957), recall (0.972), and AUC-ROC (0.981) in detecting anomalies in healthcare data, making it a groundbreaking solution. The performance of this algorithm exceeds that of other well-known machine learning algorithms, such as One-Class SVM, KNN, and LOF, when evaluated using multiple metrics. The success of IF_DBSCAN indicates a promising approach to strengthening cybersecurity in public healthcare settings, highlighting the significance of customized solutions for the distinct challenges presented by social medical data.

The study's significance lies in both the creation of an innovative cybersecurity technology and its practical implementation on actual healthcare datasets, showcasing its effectiveness in real-life situations. The results indicate that the IF_DBSCAN hybrid model can greatly improve the identification of abnormal patterns in electronic health records (EHR), thus strengthening the protection of patient data in terms of confidentiality and integrity.

As we consider the future, various paths for additional investigation and enhancement become prominent. First and foremost, it is crucial to continuously refine and optimize the IF_DBSCAN model in order to guarantee its adaptability to the ever-changing healthcare data environments. Furthermore, the incorporation of blockchain technology, as demonstrated in the literature review, has the potential to enhance security and transparency in healthcare data. Effective implementation of cybersecurity technologies in various healthcare settings necessitates collaborative endeavors involving healthcare practitioners, policymakers, and technologists.

Moreover, investigating the scalability of the suggested cybersecurity solution to handle the increasing amounts of healthcare data and the incorporation of live monitoring mechanisms could improve its practical usability. Furthermore, continuous investigation into explainable AI methodologies can enhance comprehension of the model's decision-making mechanisms, fostering trust and approval among healthcare practitioners.

Essentially, the research efforts described in this study act as a foundation for a healthcare system that is more secure and robust. The ongoing advancement of cybersecurity technologies will play a crucial role in both reducing existing threats and proactively dealing with upcoming challenges in protecting sensitive medical data in public healthcare settings.

References

[1] Z. Lv and L. Qiao, "Analysis of healthcare big data," *Futur. Gener. Comput. Syst.*, vol. 109, pp. 103–110, 2020, doi: https://doi.org/10.1016/j.future.2020.03.039.

[2] A. H. Seh *et al.*, "Healthcare data breaches: Insights and implications," *Healthc.*, vol. 8, no. 2, 2020, doi: 10.3390/healthcare8020133.

[3] S. Shi, D. He, L. Li, N. Kumar, M. K. Khan, and K.-K. R. Choo, "Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey," *Comput. Secur.*, vol. 97, p. 101966, 2020, doi: https://doi.org/10.1016/j.cose.2020.101966.

[4] S.-C. Shao *et al.*, "The Chang Gung Research Database—A multi-institutional electronic medical records database for real-world epidemiological studies in Taiwan," *Pharmacoepidemiol. Drug Saf.*, vol. 28, no. 5, pp. 593–600, May 2019, doi: https://doi.org/10.1002/pds.4713.

[5] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, "Blockchain for Secure EHRs Sharing of Mobile Cloud Based E-Health Systems," *IEEE Access*, vol. 7, pp. 66792–66806, 2019, doi: 10.1109/ACCESS.2019.2917555.

[6] N. Rieke *et al.*, "The future of digital health with federated learning," *npj Digit. Med.*, vol. 3, no. 1, pp. 1–7, 2020, doi: 10.1038/s41746-020-00323-1.

[7] S. Bhattacharya and M. Pandey, "Issues and Challenges in Incorporating the Internet of Things with the Healthcare Sector," 2021, pp. 639–651.

[8] V. Khetani, Y. Gandhi, S. Bhattacharya, S. N. Ajani, and S. Limkar, "Cross-Domain Analysis of ML and DL : Evaluating their Impact in Diverse Domains," vol. 11, pp. 253–262, 2023.

[9] L. Chen, W.-K. Lee, C.-C. Chang, K.-K. R. Choo, and N. Zhang, "Blockchain based searchable encryption for electronic health record sharing," *Futur. Gener. Comput. Syst.*, vol. 95, pp. 420–429, 2019, doi: https://doi.org/10.1016/j.future.2019.01.018.

[10] J. J. Hathaliya and S. Tanwar, "An exhaustive survey on security and privacy issues in Healthcare 4.0," *Comput. Commun.*, vol. 153, pp. 311–335, 2020, doi: https://doi.org/10.1016/j.comcom.2020.02.018.

[11] H. Habibzadeh, B. H. Nussbaum, F. Anjomshoa, B. Kantarci, and T. Soyata, "A survey on cybersecurity, data privacy, and policy issues in cyber-physical system deployments in smart cities," *Sustain. Cities Soc.*, vol. 50, p. 101660, 2019, doi: https://doi.org/10.1016/j.scs.2019.101660.

[12] S. Tanwar, K. Parekh, and R. Evans, "Blockchain-based electronic healthcare record system for healthcare 4.0 applications," *J. Inf. Secur. Appl.*, vol. 50, p. 102407, 2020, doi: https://doi.org/10.1016/j.jisa.2019.102407.

[13] G. N. Nguyen, N. H. Le Viet, M. Elhoseny, K. Shankar, B. B. Gupta, and A. A. A. El-Latif, "Secure blockchain enabled Cyber–physical systems in healthcare using deep belief network with ResNet model," *J. Parallel Distrib.*

Comput., vol. 153, pp. 150–160, 2021, doi: https://doi.org/10.1016/j.jpdc.2021.03.011.

[14] I. Keshta and A. Odeh, "Security and privacy of electronic health records: Concerns and challenges," *Egypt. Informatics J.*, vol. 22, no. 2, pp. 177–183, 2021, doi: https://doi.org/10.1016/j.eij.2020.07.003.

[15] A. Hossain, R. Quaresma, and H. Rahman, "Investigating factors influencing the physicians' adoption of electronic health record (EHR) in healthcare system of Bangladesh: An empirical study," *Int. J. Inf. Manage.*, vol. 44, pp. 76–87, 2019, doi: https://doi.org/10.1016/j.ijinfomgt.2018.09.016.

[16] R. Hamza, Z. Yan, K. Muhammad, P. Bellavista, and F. Titouna, "A privacy-preserving cryptosystem for IoT E-healthcare," *Inf. Sci. (Ny).*, vol. 527, pp. 493–510, 2020, doi: https://doi.org/10.1016/j.ins.2019.01.070.

[17] A. Al Omar, M. Z. A. Bhuiyan, A. Basu, S. Kiyomoto, and M. S. Rahman, "Privacy-friendly platform for healthcare data in cloud based on blockchain environment," *Futur. Gener. Comput. Syst.*, vol. 95, pp. 511–521, 2019, doi: https://doi.org/10.1016/j.future.2018.12.044.

[18] S. Chenthara, K. Ahmed, H. Wang, and F. Whittaker, "Security and Privacy-Preserving Challenges of e-Health Solutions in Cloud Computing," *IEEE Access*, vol. 7, pp. 74361–74382, 2019, doi: 10.1109/ACCESS.2019.2919982.

[19] A. Shahnaz, U. Qamar, and A. Khalid, "Using Blockchain for Electronic Health Records," *IEEE Access*, vol. 7, pp. 147782–147795, 2019, doi: 10.1109/ACCESS.2019.2946373.

[20] P. P. Ray, D. Dash, K. Salah, and N. Kumar, "Blockchain for IoT-Based Healthcare: Background, Consensus, Platforms, and Use Cases," *IEEE Syst. J.*, vol. 15, no. 1, pp. 85–94, 2021, doi: 10.1109/JSYST.2020.2963840.

[21] J. Xu *et al.*, "Healthchain: A Blockchain-Based Privacy Preserving Scheme for Large-Scale Health Data," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8770–8781, 2019, doi: 10.1109/JIOT.2019.2923525.

[22] S. A. Parah, J. A. Sheikh, J. A. Akhoon, and N. A. Loan, "Electronic Health Record hiding in Images for smart city applications: A computationally efficient and reversible information hiding technique for secure communication," *Futur. Gener. Comput. Syst.*, vol. 108, pp. 935–949, 2020, doi: https://doi.org/10.1016/j.future.2018.02.023.