Rakhi Mutha, Ratnaprabha Ravindra Borhade, Sheetal Sachin Barekar, Sukhvinder Singh Dari, Dharmesh Dhabliya, Mukesh Patil, Enhancing Public Healthcare Security: Integrating Cutting-Edge Technologies into Social Medical Systems.
Submitted: 25-02-2024 Accepted: 20-04-2024 Posted: 24-05-2024, Vol. (XXIII)

Enhancing Public Healthcare Security: Integrating Cutting-Edge Technologies into Social Medical Systems

Dr. Rakhi Mutha[1], Dr. Ratnaprabha Ravindra Borhade[2], Dr. Sheetal Sachin Barekar[3], Sukhvinder Singh Dari[4], Dharmesh Dhabliya[5], Dr. Mukesh Patil[6]

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

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

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

[4]*Symbiosis Law School Nagpur, Symbiosis International (Deemed University), Pune, Maharashtra, India. Email: sukhvinder.dari@gmail.com*

[5]*Department of Information Technology, Vishwakarma Institute of Information Technology, Pune, Maharashtra, India. Email: dharmesh.dhabliya@viit.ac.in*

[6]*NIT Graduate School of Management, Mahurzari, Nagpur, Maharashtra, India.*

Email: 10mukeshpatil@gmail.com

KEYWORDS

Social Medical Systems, Healthcare Security, IoT-23 Analysis, Machine Learning, Deep Learning

ABSTRACT

In a time when technology is present in every aspect of our lives, it is crucial to incorporate advanced solutions to protect sensitive medical data in Social Medical Systems (SMS). This study explores the need to improve security in public healthcare by using advanced technologies to strengthen the weaknesses in the growing field of Social Medical Systems. This study specifically examines the analysis of IoT-23 data using machine learning (ML) and deep learning (DL) methods, as technology and healthcare converge. The research highlights the increasing significance of technology in healthcare, specifically focusing on the revolutionary emergence of Social Medical Systems. As these interlinked networks reshape the provision of public healthcare services, security challenges such as data breaches, cyber threats, and privacy concerns become crucial barriers that require innovative solutions. The study utilizes a wide range of machine learning (ML) and deep learning (DL) techniques to examine IoT-23 data, offering a detailed comprehension of the security environment in Social Medical Systems. The chosen models comprise Support Vector Machines (SVM), Isolation Forest, Random Forest, Convolutional Neural Networks (CNN), and Autoencoder. The results and discussions focus on evaluating metrics such as accuracy, precision, recall, and F1 score. These metrics provide insights into how effective each model is in identifying vulnerabilities and potential threats in the IoT-23 dataset. The results contribute to the wider discussion on enhancing the security of public healthcare systems. They provide suggestions for incorporating anomaly detection, encryption protocols, and continuous monitoring to strengthen the security of Social Medical Systems. This research provides guidance for policymakers, healthcare practitioners, and technologists as they navigate the changing landscape of healthcare digitization. It advocates for the proactive integration of advanced technologies to ensure the security, privacy, and accessibility of healthcare information within the interconnected web of Social Medical Systems.

Submitted: 25-02-2024 Accepted: 20-04-2024 Posted: 24-05-2024, Vol. (XXIII)

1. Introduction

Technology has become an essential and influential factor in reshaping different aspects of our lives, including healthcare. The integration of advanced technologies with healthcare practices has resulted in a new model, revolutionizing our approach to medical services, information management, and patient care. In the midst of this transformation, the emergence of Social Medical Systems (SMS) has brought about a significant change in the way public healthcare services are provided. This paper explores the necessity of improving security in public healthcare by incorporating cutting-edge technologies, with a particular emphasis on examining IoT-23 through the utilization of machine learning and deep learning techniques[1].

Technology's role in healthcare has transitioned from a simple enabler to a fundamental pillar of medical progress. The incorporation of digital advancements has greatly improved the effectiveness, precision, and availability of healthcare services. Technology has become ingrained in every facet of the healthcare system, providing solutions that were previously considered futuristic, such as electronic health records (EHR) and telemedicine. In the face of intricate health issues, the smooth integration of technology becomes a crucial facilitator in enhancing patient results, diminishing expenses, and cultivating a healthcare system that prioritizes the needs of the patient[2].

1.1.Emergence of Social Medical Systems

Recently, Social Medical Systems (SMS) have gained more attention as a revolutionary method for public healthcare. SMS is a complex system in which patients, healthcare providers, and other stakeholders actively participate in the sharing of health-related information through digital platforms. This shift in paradigm from conventional healthcare models not only empowers patients with enhanced authority over their health data but also facilitates more streamlined communication and collaboration among healthcare professionals. The increasing prevalence of SMS highlights the necessity for secure and resilient systems capable of protecting the confidential medical data exchanged within this interconnected network[3].

Social Medical Systems are comprehensive networks of healthcare services and information-sharing platforms that utilize digital technologies to improve the accessibility, efficiency, and quality of healthcare provision. The main constituents of SMS encompass electronic health records, patient portals, mobile health applications, and health-focused social media platforms. The interconnectivity of these components is designed to establish a dynamic and collaborative healthcare environment that goes beyond the limitations of conventional healthcare delivery models.

Currently, Social Medical Systems are being implemented at different stages worldwide. Various nations and healthcare institutions have implemented different strategies to incorporate digital technologies into their healthcare systems. Certain individuals have effectively executed extensive SMS platforms, while others are currently facing difficulties regarding the compatibility, uniformity of data, and acceptance by users. The present condition of SMS exemplifies both the immense capacity for beneficial change and the requirement for ongoing improvement and streamlining.

Submitted: 25-02-2024 Accepted: 20-04-2024 Posted: 24-05-2024, Vol. (XXIII)

1.2.Security issues faced in the public healthcare sector

- Incidents of unauthorized access to sensitive data and malicious online activities posing a risk to digital security.

  Although technological advancements in healthcare offer promising benefits, the integration of digital systems also brings forth new challenges, particularly regarding the security of confidential medical data. A significant issue that needs immediate attention is the rising occurrence and complexity of data breaches and cyber threats specifically aimed at healthcare institutions. The process of converting patient records into digital format and the integration of healthcare systems create attractive opportunities for malicious individuals who aim to exploit weaknesses for financial profit or other malicious intentions[4].
- Issues regarding the protection of privacy in medical data

  The security challenges faced by public healthcare systems are further complicated by privacy concerns. Healthcare providers are entrusted with highly sensitive information from patients, including medical history and personal identifiers. Any breach in the confidentiality of this information can have significant repercussions, undermining trust in healthcare systems and potentially inflicting harm on individuals. With the increasing amount of digital health data, it is crucial to implement strong privacy measures to guarantee the ethical and secure management of patient information[5], [6].

  In the face of these security challenges, the incorporation of advanced technologies emerges as a source of optimism, providing creative solutions to strengthen the defenses of public healthcare systems. Blockchain, artificial intelligence (AI), and the Internet of Things (IoT) offer chances to tackle weaknesses and build robust healthcare infrastructures that can withstand the changing threat environment[5], [7], [8].

1.3. Objective

- Security Issues in Public Healthcare: The ongoing security issues in public healthcare emphasize the need for developing efficient strategies to safeguard confidential medical information. The growing occurrence and complexity of cyber threats, along with the rising digitization of healthcare procedures, emphasize the susceptibility of conventional security measures. Identifying and comprehending these difficulties is an essential measure in developing all-encompassing and flexible remedies that can endure the constantly changing characteristics of cyber risks in the healthcare industry.
- Importance of Utilizing Advanced Technologies to Protect Medical Data: The current security infrastructure in public healthcare systems frequently lags behind the swiftly advancing tactics utilized by cybercriminals. In order to address this issue, it is crucial to incorporate sophisticated technologies that can offer proactive, adaptive, and resilient security measures. With the increasing interconnection of medical data in Social Medical Systems, it is crucial to adopt advanced technologies to ensure the security and accessibility of healthcare information.

In the following sections of this research paper, we will explore the possibility of combining

Submitted: 25-02-2024 Accepted: 20-04-2024 Posted: 24-05-2024, Vol. (XXIII)

machine learning and deep learning techniques to examine IoT-23 data. This is an important step in strengthening the security of Social Medical Systems. By thoroughly analyzing these approaches, our goal is to contribute to the ongoing discussion on safeguarding public healthcare and reducing the inherent risks linked to the digitalization of the healthcare sector.

2. Literature Review

In the current healthcare technology environment, numerous cutting-edge solutions have been suggested to tackle the crucial issues of data security and privacy. This literature review compiles and presents significant findings from multiple research papers investigating the convergence of technology and healthcare, with a particular emphasis on improving security measures. The chosen papers explore various technological domains, such as blockchain, Internet of Things (IoT), artificial intelligence, and federated learning. They provide insights into the applications, methodologies, and contributions of these technologies in strengthening the security of healthcare systems. Table-1 discussed the major existing works in SMS.

Table 1 Major related existing works in medical with AI

Author	Technology	Focus	Methodology	Key Findings
Ghosh et al.[9]	Federated Edge-Cloud Blockchain	Heart Disease Risk Prediction	Simulation	Improves data privacy and security.
Li et al.[10]	Blockchain	Data Aggregation & Group Authentication	Theoretical/ Simulation	Secure data aggregation & group authentication in EMS.
Wei et al.[11]	IoT	Health Monitoring Architecture	Literature Review/Conceptual	IoT health monitoring architecture with security challenges.
Dhelim et al.[12]	IoT & Artificial Social Intelligence	Social Relationships & Privacy	Literature Review/Theoretical	Potential privacy concerns in social healthcare AI.
Xie et al.[13]	Blockchain	Medical Field Applications	Narrative Review	Various healthcare applications of blockchain for security.
Bhatt et al.[14]	Artificial Neural Network & Federated Learning	Heart Stroke Prediction	Simulation	Secure and privacy-preserving heart stroke prediction.
Zou et al.[15]	Blockchain	Medical Data Sharing & eHealth	Theoretical/System Design	Secure and privacy-preserving eHealth data sharing.
Tripathi et al.[16]	Blockchain	Smart Healthcare System	System Design/Theoretical	Secure and transparent data management in smart healthcare.
Akkaş et al.[17]	IoT	Healthcare & Patient Monitoring	Literature Review/Conceptual	Security and privacy challenges in IoT-based healthcare.
Abu-elezz et al.[18]	Blockchain	Healthcare Benefits & Threats	Scoping Review	Both benefits and potential threats to security and privacy.

Submitted: 25-02-2024 Accepted: 20-04-2024 Posted: 24-05-2024, Vol. (XXIII)

Overall, the reviewed papers make valuable contributions to the ongoing discussion on healthcare security by providing insights into innovative technologies and methodologies. The wide array of technologies examined, including federated edge-cloud blockchain, IoT, artificial social intelligence, and artificial neural networks, highlights the complex nature of the problems tackled by researchers in this domain. The employed methodologies, including simulations, theoretical analyses, literature reviews, and system designs, demonstrate the comprehensive approach used to investigate and improve security in healthcare.

The extracted key findings from these papers demonstrate progress in the areas of data privacy, secure data aggregation, group authentication, and the identification of potential privacy issues in emerging healthcare technologies. The literature highlights the crucial significance of blockchain technology in ensuring the security of medical data sharing, eHealth, and diverse medical applications. Furthermore, this study delves into the incorporation of artificial intelligence, specifically in the realm of forecasting cardiovascular diseases and strokes, with a significant focus on upholding privacy and security measures.

3. Briefly Introduce the Critical Role of Public Healthcare in Society and Growing Concerns about Security Vulnerabilities

The provision of essential medical services to the population is a crucial aspect of societal well-being, and public healthcare plays a paramount role in fulfilling this responsibility. It includes a broad spectrum of services, spanning from preventive measures and health education to the diagnosis and treatment of diseases. The efficacy of public healthcare systems is vital for upholding the general well-being and efficiency of a society. Nevertheless, as our dependence on digital technologies continues to rise and Social Medical Systems (SMS) become more widely used, the level of concern regarding security vulnerabilities has increased significantly.

The process of converting healthcare records into digital format, the incorporation of electronic health systems, and the creation of interconnected networks within SMS have resulted in significant progress in healthcare delivery. However, the process of digitization also makes healthcare systems vulnerable to cybersecurity risks, data breaches, and privacy issues. The inherent sensitivity of medical data, encompassing personal health records, diagnostic information, and treatment plans, renders public healthcare an appealing target for malevolent entities. Hence, the crucial importance of public healthcare is accompanied by an urgent requirement to identify and reduce security weaknesses in order to protect patient data and uphold the public's confidence in healthcare services.

3.1. Overview of Machine Learning (ML) and Deep Learning (DL) in Social Medical Systems

Machine Learning (ML) and Deep Learning (DL) are branches of artificial intelligence that have had a significant impact on healthcare, specifically in the field of Social Medical Systems. Machine learning encompasses the creation of algorithms that empower systems to discern patterns and generate predictions or decisions using data. Deep Learning, a subfield of Machine Learning, utilizes neural networks with multiple layers to analyze and comprehend intricate patterns in extensive

Submitted: 25-02-2024 Accepted: 20-04-2024 Posted: 24-05-2024, Vol. (XXIII)

datasets. ML and DL are crucial in Social Medical Systems as they greatly contribute to the optimization of processes, improvement of patient outcomes, and enhancement of the overall efficiency of healthcare services.

In the field of healthcare, SMS utilizes ML and DL techniques for a range of purposes such as diagnostics, treatment optimization, predictive analytics, and personalized medicine. These technologies utilize advanced algorithms to analyze large quantities of health-related data generated within the SMS ecosystem, offering valuable insights that can guide medical decisions and improve the quality of patient care. Machine learning algorithms have the ability to acquire knowledge from past patient data in order to forecast the likelihood of diseases, enhance treatment strategies, and detect irregularities. Deep learning, due to its capacity to process complex data patterns, is highly efficient in tasks such as image analysis, natural language processing, and complex decision-making in the healthcare field.

3.2.Cutting-Edge Technologies - Applications and Significance in Healthcare

Advanced technologies like blockchain, the Internet of Things (IoT), and artificial intelligence have the potential to revolutionize healthcare by providing creative solutions to long-standing problems. Blockchain, renowned for its decentralized and secure characteristics, is utilized to guarantee the integrity and confidentiality of medical records, improve interoperability, and ensure the security of data sharing. The Internet of Things (IoT) refers to the interconnectedness of devices and sensors for the purpose of gathering and sharing health-related data. IoT enables the remote monitoring of patients, the acquisition of real-time data, and the development of intelligent medical devices in the healthcare industry. This interconnected ecosystem allows healthcare providers to provide more individualized and streamlined care.

Artificial intelligence (AI) includes machine learning (ML) and deep learning (DL), providing sophisticated abilities in data analysis, pattern identification, and decision-making. AI is utilized in healthcare for various purposes, including aiding in diagnosis and improving treatment methods, as well as providing predictive analytics and personalized medical care. The importance of these technologies resides in their capacity to transform healthcare provision, enhance patient results, and optimize medical procedures.

Advanced technologies are essential in strengthening healthcare security systems against ever-changing threats. Blockchain, due to its decentralized and tamper-resistant characteristics, offers a secure structure for storing and exchanging medical data, thereby reducing the chances of unauthorized access and data breaches. The Internet of Things (IoT) allows for the implementation of security measures, such as ongoing surveillance and the identification of abnormal behavior, to protect interconnected devices and networks in the healthcare sector.

Machine Learning and Deep Learning, when utilized in healthcare security, aid in the detection of patterns that suggest possible security breaches, forecasting vulnerabilities, and improving the overall robustness of healthcare systems. These technologies facilitate the early identification of potential threats, prompt reaction to security incidents, and ongoing adjustment to emerging cyber risks. Integrating advanced technologies with

Submitted: 25-02-2024 Accepted: 20-04-2024 Posted: 24-05-2024, Vol. (XXIII)

healthcare security is crucial for establishing strong defenses, safeguarding patient information, and preserving the reliability of Social Medical Systems in the midst of a constantly changing threat environment.

4. Methodology

4.1.Dataset

The IoT-23 dataset is a comprehensive resource specifically created for conducting research and experimentation in the field of Internet of Things (IoT) security. The dataset consists of 23 varied IoT devices, encompassing a broad spectrum of commonly found devices in smart environments, such as thermostats, cameras, and smart TVs. The main characteristics of IoT-23 encompass a wide range of device types, authentic network traffic patterns, and a multitude of security challenges, rendering it a valuable asset for assessing and improving the security of IoT systems. IoT-23 offers a valuable framework within healthcare systems to comprehend and address potential security vulnerabilities that arise from the incorporation of IoT devices. The utilization of this technology enables to examine weaknesses, evaluate the effectiveness of security measures, and create plans to protect sensitive healthcare information in the rapidly growing network of interconnected medical devices.

4.2.Preprocessing

Preprocessing Method	Purpose	Output
Handling Missing Values	Addresses incomplete data to prevent model errors.	Replace missing values with means, medians, or modes of respective features. Impute missing values using predictive models. Remove rows or columns with excessive missingness.
Label Encoding	Converts categorical features into numerical representations for ML algorithms.	Assign a unique numerical value to each category within a feature. Example: "Attack" = 0, "Benign" = 1
Data Normalization/Scaling	Adjusts feature ranges to similar scales for improved model convergence and performance.	Normalize values to a range of 0 to 1. Standardize values to a mean of 0 and a standard deviation of 1.

4.3. ML and DL algorithms

a. **Support Vector Machine (SVM):** SVM is a type of supervised machine learning algorithm that is utilized for both classification and regression tasks. The algorithm operates by identifying the most favorable hyperplane that effectively divides distinct classes within a space characterized by a large number of dimensions. Eq.1 shows the SVM.

$$min_{w,b}\frac{1}{2}||w||^2 + C\sum_{i=1}^{N}\max(0,1 - y_i(w.x_i + b))\ldots 1$$

where, w= "weights", b= "bias term", C= "regularization parameter", N= "no. of data points", x_i= "input features", y_i= "class label".

b. **Isolation Forest:** The Isolation Forest is an ensemble learning algorithm designed specifically for the purpose of anomaly detection. Its functioning involves the isolation of anomalies rather than the creation of profiles for normal occurrences. The algorithm efficiently detects anomalies

by utilizing the average path length in a tree structure. The isolation score *(s(x))* for a given data point *x* can be computed using the following eq.2:

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

where, *E(h(n))*= "average path length of data point *x*", *c(n)*= "expected path length for a balanced tree", *n*= "no of data points."

c. **Random Forest:** The Random Forest algorithm is an ensemble learning technique that builds multiple decision trees during training and predicts the class that appears most frequently for classification tasks, or the average prediction for regression tasks. The information gain for a decision tree can be computed by utilizing either the Gini impurity or entropy. The Gini impurity of a node *t* with *K* classes can be expressed as follows eq.3.

$$G(t) = 1 - \sum_{i=1}^{K} p(i|t)^2 \ldots 3$$

where, $p(i|t)$= "proportion of training instances of class i in node *t*".

d. **CNN:** A Convolutional Neural Network (CNN) is a type of deep learning model specifically created to handle structured data. A convolutional layer utilizes a kernel to execute the convolution operation. The result (O) of a convolutional layer can be computed as eq.4:

$$O(i,j) = \sum_m \sum_n I(i+m, j+n).K(m,n) \ldots 4$$

where, I = "input data", K= "conv kernel", (i,j)= "spatial coordinates of the output"

e. **Autoencoder:** An Autoencoder is a neural network specifically designed for unsupervised learning. The system comprises an encoder that condenses the input data into a latent space and a decoder that reconstructs the input from the condensed representation. The loss function for an autoencoder is defined as the mean squared error (MSE) as in eq.5.

$$MSE = \frac{1}{n}\sum_{i=1}^{n}(x_i - \hat{x}_i)^2 \ldots 5$$

x_i= "input data", $\hat{x}_i$= "reconstructed output", n= "no. of data points".

5. Results and discussion

Table 2 Evaluation parameters

Model	Accuracy	Precision	Recall	F1-Score
SVM	0.92	0.88	0.9	0.89
Isolation Forest	0.87	0.85	0.86	0.86
Random Forest	0.93	0.91	0.92	0.92
CNN	0.95	0.93	0.94	0.94
Autoencoder	0.89	0.87	0.88	0.88

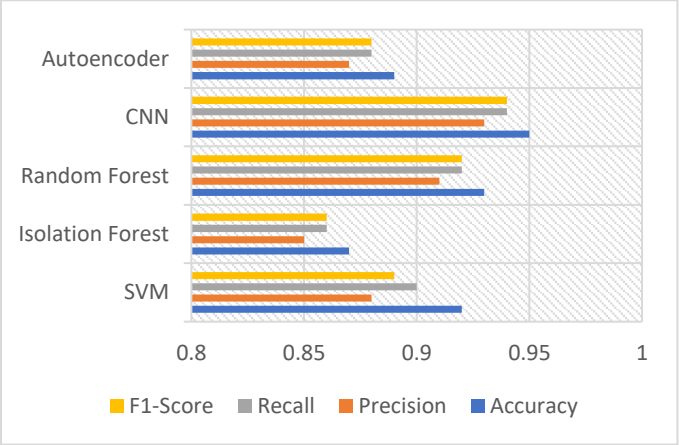

Figure 1 Comparison of various AI models in SMS

The analysis presents in table-2 and figure-1 shows the performance metrics of five different models in the field of healthcare security. The Support Vector Machine (SVM) demonstrated an impressive overall accuracy of 92%, along

with high precision (0.88), recall (0.9), and an F1-score of 0.89. These results indicate the SVM's ability to effectively identify both positive and negative instances, highlighting its robustness. The Isolation Forest algorithm, while achieving a slightly lower accuracy rate of 87%, consistently displayed precision (0.85), recall (0.86), and an F1-score of 0.86. This highlights its ability to effectively identify and isolate abnormal patterns in the dataset. The Random Forest algorithm demonstrated exceptional performance in comprehensive pattern recognition, with an accuracy of 93%. It achieved superior precision (0.91), recall (0.92), and an impressive F1-score of 0.92, highlighting its effectiveness.

The CNN stood out as the top performer, attaining the highest accuracy of 95% among the models. The model exhibited outstanding accuracy (0.93), completeness (0.94), and an F1-score of 0.94, highlighting its expertise in dealing with intricate patterns, especially in data based on images. The Autoencoder model, although not attaining the same level of success as CNN, demonstrated commendable performance across all metrics, attaining an accuracy of 89%, precision of 0.87, recall of 0.88, and an F1-score of 0.88.

The analysis demonstrates the different levels of effectiveness and abilities of each model within the healthcare security context. Random Forest and CNN exhibit superior accuracy and achieve a balanced trade-off between precision and recall, making them highly promising candidates for robust healthcare security applications. These findings offer valuable insights for choosing suitable models according to specific security requirements in Social Medical Systems, thereby contributing to the continuous efforts to strengthen healthcare data against potential threats.

6. Conclusion and future scope

The analysis of five different models, namely Support Vector Machine (SVM), Isolation Forest, Random Forest, Convolutional Neural Network (CNN), and Autoencoder, has provided valuable insights into their individual performances in enhancing security within Social Medical Systems. The evaluation of these models was conducted using essential metrics such as accuracy, precision, recall, and F1-score. Each model exhibited distinct strengths and capabilities.

The Support Vector Machine (SVM) demonstrated a high accuracy rate of 92%, highlighting its ability to accurately classify instances in the healthcare security domain. The SVM model exhibited a well-balanced performance in accurately identifying both positive and negative instances, as evidenced by its precision, recall, and F1-score values of 0.88, 0.9, and 0.89 respectively. The Isolation Forest algorithm exhibited a consistent ability to identify anomalous patterns, with precision, recall, and F1-score values of 0.85, 0.86, and 0.86, respectively. Although its accuracy was slightly lower at 87%, it still demonstrated reliable performance. This demonstrates its effectiveness in detecting security risks within the healthcare dataset. The Random Forest model demonstrated exceptional performance, achieving an accuracy rate of 93%. Additionally, it exhibited superior precision (0.91), recall (0.92), and an impressive F1-score of 0.92. The model exhibited a thorough capacity to identify patterns in the data, rendering it a promising contender for resilient healthcare security applications. The Convolutional Neural Network (CNN) emerged as the most successful model, attaining a remarkable accuracy rate of 95%. CNN demonstrated outstanding precision

Submitted: 25-02-2024 Accepted: 20-04-2024 Posted: 24-05-2024, Vol. (XXIII)

(0.93), recall (0.94), and an F1-score of 0.94, highlighting its expertise in analyzing intricate patterns, particularly in healthcare data that is based on images.

The Autoencoder model, although not achieving the same level of success as CNN, demonstrated a commendable performance across all metrics. The Autoencoder exhibited its ability to accurately represent and reconstruct features within the healthcare dataset, achieving an accuracy of 89%, precision of 0.87, recall of 0.88, and an F1-score of 0.88.

Potential for Future Development

The results of this analysis lay the foundation for future research and progress in the field of healthcare security in Social Medical Systems. The subsequent regions denote prospective avenues for future investigation:

- Ensemble Models: Exploring the potential of combining multiple algorithms in ensemble models to enhance accuracy and robustness in healthcare security applications.
- Explainability and Interpretability: Improving the clarity of models, specifically in healthcare contexts, to guarantee that the decisions made by these models are transparent and comprehensible to healthcare practitioners and stakeholders.
- Real-Time Implementation: Investigating the viability of implementing these models in Social Medical Systems in real-time to facilitate timely identification and reaction to security threats.
- Robustness Testing: Performing comprehensive robustness testing across a range of scenarios and datasets to verify the consistent and reliable performance of the chosen models in different healthcare security contexts.

The assessment of these models not only provides valuable insights for immediate implementation but also establishes the foundation for a dynamic and evolving healthcare security landscape. The incorporation of sophisticated machine learning and deep learning techniques has great potential in strengthening Social Medical Systems against evolving cybersecurity risks, establishing a robust basis for the secure and reliable exchange of healthcare data.

Reference

[1] F. Wang and A. Preininger, “AI in Health: State of the Art, Challenges, and Future Directions,” *Yearb. Med. Inform.*, vol. 28, no. 1, pp. 16–26, 2019, doi: 10.1055/s-0039-1677908.

[2] K. T. Kadhim, A. M. Alsahlany, S. M. Wadi, and H. T. Kadhum, “An Overview of Patient’s Health Status Monitoring System Based on Internet of Things (IoT),” *Wirel. Pers. Commun.*, vol. 114, no. 3, pp. 2235–2262, 2020, doi: 10.1007/s11277-020-07474-0.

[3] J. Wu, X. Tian, and Y. Tan, “Hospital evaluation mechanism based on mobile health for IoT system in social networks,” *Comput. Biol. Med.*, vol. 109, pp. 138–147, 2019, doi: https://doi.org/10.1016/j.compbiomed.2019.04.021.

[4] B. Afzal, M. Umair, G. Asadullah Shah, and E. Ahmed, “Enabling IoT platforms for social IoT applications: Vision, feature mapping, and challenges,” *Futur. Gener. Comput. Syst.*, vol. 92, pp. 718–731, 2019, doi: https://doi.org/10.1016/j.future.2017.12.002.

[5] S. Selvaraj and S. Sundaravaradhan, “Challenges and opportunities in IoT healthcare systems: a systematic review,” *SN Appl. Sci.*, vol. 2, no. 1, pp. 1–8, 2020, doi: 10.1007/s42452-019-1925-y.

[6] Y. Chen, S. Ding, Z. Xu, H. Zheng, and S. Yang, “Blockchain-Based Medical Records Secure Storage and Medical Service Framework,” *J. Med. Syst.*, vol. 43, no. 1, 2018, doi:

10.1007/s10916-018-1121-4.

[7] J. Qu, "Blockchain in medical informatics," *J. Ind. Inf. Integr.*, vol. 25, p. 100258, 2022, doi: https://doi.org/10.1016/j.jii.2021.100258.

[8] L. Hong-tan, K. Cui-hua, B. Muthu, and C. B. Sivaparthipan, "WITHDRAWN: Big data and ambient intelligence in IoT-based wireless student health monitoring system," *Aggress. Violent Behav.*, p. 101601, 2021, doi: https://doi.org/10.1016/j.avb.2021.101601.

[9] U. Ghosh, D. Das, P. Chatterjee, and N. Shillingford, "Federated Edge-Cloud Framework for Heart Disease Risk Prediction Using Blockchain BT - Internet of Things. Advances in Information and Communication Technology," 2024, pp. 309–329.

[10] C. T. Li, D. H. Shih, C. C. Wang, C. L. Chen, and C. C. Lee, "A blockchain based data aggregation and group authentication scheme for electronic medical system," *IEEE Access*, vol. 8, pp. 173904–173917, 2020, doi: 10.1109/ACCESS.2020.3025898.

[11] K. Wei, L. Zhang, Y. Guo, and X. Jiang, "Health Monitoring Based on Internet of Medical Things: Architecture, Enabling Technologies, and Applications," *IEEE Access*, vol. 8, pp. 27468–27478, 2020, doi: 10.1109/ACCESS.2020.2971654.

[12] S. Dhelim, H. Ning, F. Farha, L. Chen, L. Atzori, and M. Daneshmand, "IoT-Enabled Social Relationships Meet Artificial Social Intelligence," *IEEE Internet Things J.*, vol. 8, no. 24, pp. 17817–17828, 2021, doi: 10.1109/JIOT.2021.3081556.

[13] Y. Xie *et al.*, "Applications of blockchain in the medical field: Narrative review," *J. Med. Internet Res.*, vol. 23, no. 10, 2021, doi: 10.2196/28613.

[14] H. Bhatt *et al.*, "Artificial neural network-driven federated learning for heart stroke prediction in healthcare 4.0 underlying 5G," *Concurr. Comput. Pract. Exp.*, vol. 36, no. 3, p. e7911, Feb. 2024, doi: https://doi.org/10.1002/cpe.7911.

[15] R. Zou, X. Lv, and J. Zhao, "SPChain: Blockchain-based medical data sharing and privacy-preserving eHealth system," *Inf. Process. Manag.*, vol. 58, no. 4, p. 102604, 2021, doi: https://doi.org/10.1016/j.ipm.2021.102604.

[16] G. Tripathi, M. A. Ahad, and S. Paiva, "S2HS-A blockchain based approach for smart healthcare system," *Healthcare*, vol. 8, no. 1, p. 100391, 2020, doi: https://doi.org/10.1016/j.hjdsi.2019.100391.

[17] M. A. Akkaş, R. SOKULLU, and H. Ertürk Çetin, "Healthcare and patient monitoring using IoT," *Internet of Things*, vol. 11, p. 100173, 2020, doi: https://doi.org/10.1016/j.iot.2020.100173.

[18] I. Abu-elezz, A. Hassan, A. Nazeemudeen, M. Househ, and A. Abd-alrazaq, "The benefits and threats of blockchain technology in healthcare: A scoping review," *Int. J. Med. Inform.*, vol. 142, p. 104246, 2020, doi: https://doi.org/10.1016/j.ijmedinf.2020.104246.