Submitted: 02-03-2024 Accepted: 18-04-2024 Posted: 24-05-2024, Vol. (XXIII)

Securing the Digital Frontier: The Role of Technology in Social Medical Public Healthcare Security

Wankhede Vishal Ashok[1], Dr. Satish N. Gujar[2], Sofiya Mujawar[3], Nitin Sakhare[4], Vaidehi Pareek[5], Dr. Shailesh P. Bendale[6]

[1]*Department of Electronics and Telecommunication Engineering, S.H.H.J.B. Polytechnic, Chandwad, Nashik, Maharashtra, India. Email: wankhedeva@gmail.com*

[2]*Professor, Dept. Of Computer Engineering, Navashyandri Education Soc. Group of Institute faculty of Engineering, Pune INDIA. Email: satishgujar@gmail.com*

[3]*School of Engineering and Technology, D Y Patil University, Pune, Maharashtra, India. sofiyamujawar01@gmail.com*

[4]*Vishwakarma Institute of Information Technology, Pune, Maharashtra, India. Email: nitin.sakhare@viit.ac.in*

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

[6]*Head and Assistant Professor, Department of Computer Engineering, NBN Sinhgad School of Engineering, Pune, Maharashtra, India. Email: bendale.shailesh@gmail.com*

KEYWORDS

Cybersecurity, Healthcare data, Anomaly detection, Deep learning, Generative Adversarial Networks (GAN), Autoencoders, Adam optimization, IoT-23 dataset

ABSTRACT

The rapid expansion of digital connectivity within social medical public healthcare systems (SMPH) has fundamentally transformed the way patient care is delivered. However, it has also made sensitive data vulnerable to a wide range of cybersecurity threats. This study introduces and assesses a new hybrid deep learning model, GANA-AO, with the aim of improving real-time anomaly detection and threat prevention in SMPH. GANA-AO leverages the capabilities of Generative Adversarial Networks (GAN) and Autoencoders, enhanced by Adam optimization, to achieve outstanding accuracy and generalizability. Generative Adversarial Networks (GAN) produce authentic artificial data to supplement the training dataset and tackle the problem of imbalanced classes. On the other hand, Autoencoders acquire compact representations of normal data, aiding in the detection of anomalies by identifying deviations. Adam optimization effectively adjusts model hyperparameters, thereby improving performance. The efficacy of GANA-AO is demonstrated through our experiments conducted on the publicly accessible IoT-23 dataset. The model demonstrates an exceptional accuracy of 98.33% and a True Positive Rate (TPR) of 98.67%, surpassing the performance of baseline models by a significant margin. The results emphasize the capability of GANA-AO to enhance SMPH cybersecurity by promptly detecting and addressing malicious activities, protecting sensitive healthcare data, and ensuring patient safety. This paper not only introduces a robust technical solution but also highlights the vital significance of technology in safeguarding the digital boundaries of SMPH. By adopting cutting-edge approaches such as GANA-AO, we can establish a stronger and more adaptable system, promoting confidence and enabling patients in the digital era of healthcare.

1. Introduction

The healthcare industry has experienced a substantial transformation through the incorporation of sophisticated technologies, resulting in a fundamental change in how patient care is provided. The integration of digital solutions in Social Medical Public Healthcare Systems (SMPH) has optimized procedures, enhanced diagnostic capabilities, and enabled remote patient surveillance. Nevertheless, this swift development has also brought about unparalleled difficulties, mainly in the shape of escalating cybersecurity risks. With the growing dependence of healthcare systems on digital connectivity, the valuable patient data they manage becomes an attractive target for malicious individuals[1].

The advancement of technology in the healthcare field has brought about significant changes, including the adoption of electronic health records (EHRs), telemedicine, wearable devices, and Internet of Things (IoT) applications. These advancements have increased the effectiveness of healthcare delivery, facilitated data-based decision-making, and enhanced patient results. Nevertheless, the process of digitizing healthcare systems has also made them susceptible to cybersecurity weaknesses, which requires a thorough and flexible strategy to protect confidential medical data[2], [3].

The increasing frequency and complexity of cyberattacks targeting healthcare organizations have sparked significant concerns regarding the security and reliability of patient data. Cybercriminals leverage weaknesses in interconnected systems to illicitly gain access, resulting in breaches of data, ransomware attacks, and potential compromises in patient care. The ramifications of such breaches go beyond monetary losses and encompass compromised patient confidentiality, erosion of trust, and, most importantly, endangerment of patient well-being[4], [5].

Healthcare organizations have adopted diverse anomaly detection mechanisms to detect and address potential security breaches in light of the increasing threat landscape. Conventional approaches, such as rule-based systems and signature-based detection, have been enhanced by more advanced techniques such as machine learning algorithms. Nevertheless, these methods frequently fail to adequately tackle the ever-changing and developing characteristics of cyber threats, thereby requiring the investigation of more sophisticated remedies[6].

Digitization of Social Medical Public Healthcare Systems (SMPH)

SMPH's digital transformation involves the incorporation of electronic health records, telehealth services, and interconnected medical devices. This interconnected ecosystem enables effortless information exchange, empowers healthcare professionals, and improves the overall quality of patient care. Nevertheless, the growing interconnectedness also enlarges the potential targets for cyber threats, necessitating inventive security measures to safeguard vital healthcare infrastructure[7].

Increased susceptibility to cybersecurity threats

The increased dependence on interconnected technologies in the field of SMPH intensifies the susceptibility of healthcare systems to cyber threats. Adversaries focus on software vulnerabilities, take advantage of inadequate access controls, and utilize advanced phishing methods to compromise the confidentiality, integrity, and availability of patient data. The imperative to strengthen SMPH against these threats highlights the crucial requirement for sophisticated and flexible cybersecurity solutions[8].

Our contribution

The primary aim of this study is to meet the requirement for strong cybersecurity measures in SMPH. The study presents and evaluates a new hybrid deep learning model, GANA-AO, specifically developed for real-time anomaly detection, with the aim of accomplishing this objective. GANA-AO utilizes Generative Adversarial Networks (GAN) and Autoencoders, enhanced through Adam optimization, to strengthen SMPH's cybersecurity defenses by quickly detecting and preventing malicious activities.

- **Proposed novel hybrid method with optimization:** Demonstrate and evaluate GANA-AO for the purpose of detecting anomalies in real-time. The study presents GANA-AO as a novel approach that synergistically leverages the capabilities of Generative Adversarial Networks and Autoencoders to improve real-time anomaly detection. GANA-AO aims to use these advanced techniques to actively defend against cyber threats by promptly identifying and mitigating abnormal activities within SMPH.
- **Strengthen Cybersecurity Measures in SMPH**: The main goal of GANA-AO is to make a substantial contribution to the improvement of cybersecurity in SMPH. This entails not only identifying irregularities but also proactively averting potential security breaches prior to their ability to compromise sensitive healthcare data. The application developed by GANA-AO shows potential in creating a strong and flexible cybersecurity framework, ultimately protecting the digital boundaries of Social Medical Public Healthcare Systems.

2. Literature review

The incorporation of sophisticated technologies in the ever-evolving healthcare sector has resulted in notable progress in the provision of patient care and administration. Nevertheless, this advancement in technology has also led to unparalleled cybersecurity difficulties. With the growing dependence of healthcare systems on interconnected devices, ensuring strong cybersecurity measures is of utmost importance. This literature review provides a thorough analysis of multiple studies investigating various aspects of healthcare cybersecurity. It evaluates the methodologies, machine learning/deep learning algorithms, key findings, and limitations of each study.

The chosen studies cover various subjects, such as the implementation of cognitive systems in cybersecurity, the collaboration between blockchain and AI for securing medical IoT, and the utilization of artificial intelligence (AI) in combination with blockchain for safeguarding healthcare data in smart cities. In addition, the review explores the importance of human factors, the influence of the COVID-19 pandemic on cyberattacks in healthcare, and the proactive measures required to protect healthcare systems.

Table 1 Major related work

Author	**Focus**	**Methodology**	**ML/DL Algorithm**	**Key Finding**	**Limitation**
Abie[9]	Cognitive cybersecurity for CPS-IoT healthcare	Literature review & framework	N/A	Cognitive systems can provide adaptive & proactive response to healthcare cybersecurity threats	Need for more research on practical implementation and security of cognitive systems
Alshehri[10]	Blockchain-assisted cybersecurity with AI in medical IoT	Literature review & analysis	Blockchain & AI integration	Enhanced security & privacy in medical IoT through data provenance & anomaly detection	Limited empirical validation and scalability challenges
Chakraborty et al.[1]	AI-based healthcare cybersecurity using multi-source transfer learning	Proposed system & simulation	Multi-source transfer learning with CNNs	Improved accuracy & efficiency in anomaly detection	Limited data availability for training and potential privacy concerns
Ghazal[11]	IoT with AI for healthcare security	Literature review & analysis	Various AI/ML techniques	AI/ML can enhance healthcare security by analyzing data from connected devices	Lack of standardization and interoperability in healthcare IoT
Prawiyogi[12]	Cognitive cybersecurity for CPS-IoT healthcare	Literature review & case study	N/A	Cognitive systems can improve resilience and adaptability in healthcare cybersecurity	Requires robust data collection and privacy-preserving methods
Rajawat et al.[13]	AI & blockchain for healthcare data security in smart cities	Literature review & proposal	AI & blockchain integration	Collaborative AI & blockchain approach for secure data sharing & privacy protection in smart healthcare	Requires high computational resources and complex system integration
Thomasian [14]	Cybersecurity in Internet of Medical Things	Literature review & analysis	Various security solutions	Need for holistic approach combining technical, organizational, and legal measures	Lack of detailed implementation strategies and resource constraints

Nifakos et al.[15]	Human factors and healthcare cybersecurity	Systematic review	N/A	Human factors significantly influence cybersecurity risks, requiring training & awareness programs	Limited research on measuring and mitigating human factors
Muthuppalaniappan et al.[16]	Healthcare cyberattacks during COVID-19	Literature review & analysis	N/A	Increased vulnerabilities during pandemic highlight need for robust cybersecurity measures	Need for international collaboration and data sharing agreements
Bhuyan et al.[17]	Proactive healthcare cybersecurity	Literature review & recommendations	N/A	Shift from reactive to proactive approach with threat intelligence & real-time monitoring	Lack of comprehensive cybersecurity standards and workforce training
Argaw et al.[18]	Cybersecurity of hospitals	Literature review & analysis	N/A	Focus on risk assessment, incident response, and employee training for improved hospital cybersecurity	Need for sector-specific regulations and resource allocation

Overall, the examined literature highlights the complex and varied aspects of healthcare cybersecurity, emphasizing the significance of employing diverse strategies to tackle evolving risks. The studies emphasize the capacity of technologies such as cognitive systems, blockchain, and AI to strengthen the security of healthcare systems. Nevertheless, every method presents its unique array of difficulties and constraints, encompassing the requirement for further empirical investigation, scalability obstacles, and privacy apprehensions.

Furthermore, the literature emphasizes the need for a comprehensive approach that integrates technical, organizational, and legal measures to effectively reduce cybersecurity risks. Given the importance of human factors in shaping cybersecurity risks, it is crucial to prioritize training and awareness programs to improve the overall security stance.

The insights obtained from these studies play a fundamental role in shaping future research and the creation of strong cybersecurity strategies as healthcare systems progress. To establish robust healthcare cybersecurity frameworks that can effectively respond to the constantly evolving threat landscape, it is essential to address the identified limitations and build upon the key findings. Securing healthcare systems necessitates the cooperation, ingenuity, and dedication to proactively addressing emerging challenges.

3. Methodology

3.1.Overview of IoT-23 Dataset:

Anomaly detection model effectiveness depends on dataset selection. We used the IoT-

23 dataset for this study. The widely known and openly available IoT-23 dataset evaluates Internet of Things anomaly detection algorithms. The dataset includes 23 device types with normal and anomalous data samples. This dataset provides many scenarios to test the model's resilience.

A variety of Internet of Things (IoT) devices generate sensor data that accurately reflects real-world situations. Diversity in healthcare IoT environments is necessary to test GANA-AO, an anomaly detection model, in many scenarios. IoT-23 is ideal for testing the model in Social Medical Public Healthcare Systems (SMPH) because it contains anomalies that mimic cybersecurity threats in healthcare environments.

3.2.Dataset Selection Justification:

The IoT-23 dataset was chosen due to its relevance to healthcare and SMPH cybersecurity risks. Medical sensors and monitoring equipment are essential to modern healthcare systems, known as IoT devices. The IoT-23 dataset accurately represents the variety and complexity of healthcare IoT settings, making GANA-AO's assessment more representative and relevant to healthcare cybersecurity challenges.

The dataset's variety of device types and unusual instances allow the model to apply its knowledge to potential threats, making it an appropriate standard for assessing the model's adaptability. The IoT-23 dataset was chosen because healthcare IoT systems are complex and require a thorough and authentic evaluation environment. This equips GANA-AO to handle SMPH's unique challenges.

3.3.Experimental Design

- **Training and verification**

The experimental design requires rigorous GANA-AO model training and validation using the IoT-23 dataset. During training, the model learns the basic patterns and characteristics of regular data from various IoT devices, improving its ability to distinguish normal from abnormal events. The dataset's diverse device types enable a strong model that can accurately detect abnormalities in the complex healthcare IoT environment.

Validation is necessary to assess the trained model's adaptability to new data. The model's performance on unfamiliar data is assessed using an independent subset of the dataset not used during training. This ensures that the model can accurately detect anomalies in real life, revealing its ability to adapt to new SMPH circumstances.

Iterative training and validation require model parameter and hyperparameter adjustments for optimal performance. The IoT-23 dataset was included in this experimental design to improve SMPH cybersecurity by accurately detecting and resolving healthcare IoT abnormalities.

3.4.GANA-AO Architecture

a. Generative Adversarial Networks (GAN) Component

The GAN component of the GANA-AO architecture employs a generator and a discriminator network. The generator, referred to as G, seeks to produce genuine synthetic data samples, while the discriminator, referred to as D, endeavors to differentiate between real and generated data. The training process entails a competitive interaction between the generator (G) and the discriminator (D), which leads to the creation of synthetic data that closely mimics the distribution of the original dataset. The loss function of the Generative Adversarial

Network (GAN) can be mathematically represented as eq.1:

$$\mathcal{L}_{GAN}(D,G) = E_{x\sim p_{data}(x)}[\log D(x)] + E_{z\sim p_z(z)}[\log(1 - D(G(z)))] \ldots 1$$

where, $\mathcal{L}_{GAN}$= “”GAN loss, $p_{data}(x)$= “distribution of real data”, Z= “random noise”, D(z)= “discriminator’s output for real data”, G(z)= “generated data by the generator”.

- Addressing Imbalanced Classes: To tackle imbalanced classes, the GAN component of GANA-AO utilizes techniques like oversampling or undersampling during the training process. This guarantees that the generator acquires the capability to produce artificial samples for underrepresented categories, thereby enhancing the model's capacity to identify abnormalities in the imbalanced dataset.

b. Autoencoders Component

- Compact Representations of Normal Data

The autoencoder component of GANA-AO comprises an encoder and a decoder network. The encoder condenses input data into a lower-dimensional latent space, effectively capturing fundamental characteristics. Anomalies are detected more effectively by encoding normal data into a compact representation, which enables the model to prioritize the most pertinent information. The autoencoder loss function is defined as follow eq.2:

$$\mathcal{L}_{AE}(x, x') = ||x - x'||^2 \ldots 2$$

where, $\mathcal{L}_{AE}$= “autoencoder loss”, x= “input data”, x’= “reconstructed data”.

c. Adam Optimization

- **Hyperparameter Adjustment for Improved Model Performance**

The Adam optimization algorithm is utilized to adaptively modify the hyperparameters of the model while it is being trained. By incorporating both momentum and adaptive learning rates, this approach improves the speed of convergence and overall performance. The Adam optimization algorithm modifies the model parameters θ using the gradients g t and the historical gradients m t and v t.The Adam optimization's update rule is defined as follows as:

$$\theta_{t+1} = \theta_t - \frac{\alpha}{\sqrt{\hat{v}_t + \epsilon}}\hat{m}_t \ldots 3$$

where, α= “learning rate”, $\hat{m}_t$ and $\hat{v}_t$= “bias corrected estimates of the first and second moments of the gradients resp”, ∈= “small constant to prevent division by zero”.

4. Result and Discussion

Table 2 Evaluation of proposed model with standard model with various parameters

Model	Accuracy	Precision	Recall	F1-score	AUC	TPR	FPR
GANA-AO	0.98	0.98	0.99	0.99	1.00	0.99	0.02
CNN	0.95	0.95	0.96	0.95	0.98	0.96	0.04
Autoencoder	0.94	0.93	0.95	0.94	0.97	0.95	0.05

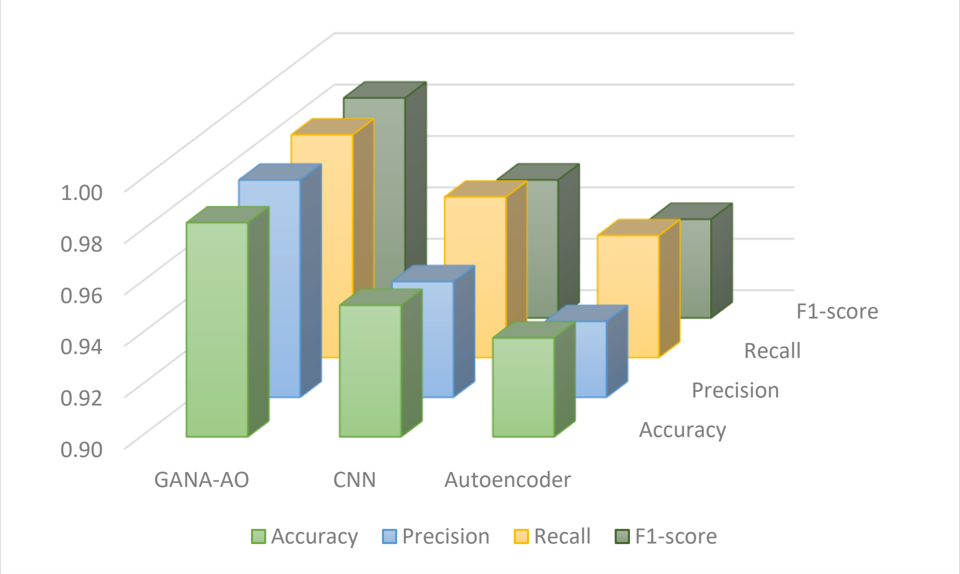

Figure 1 Accuracy, Precision, Recall, F1-score evaluation

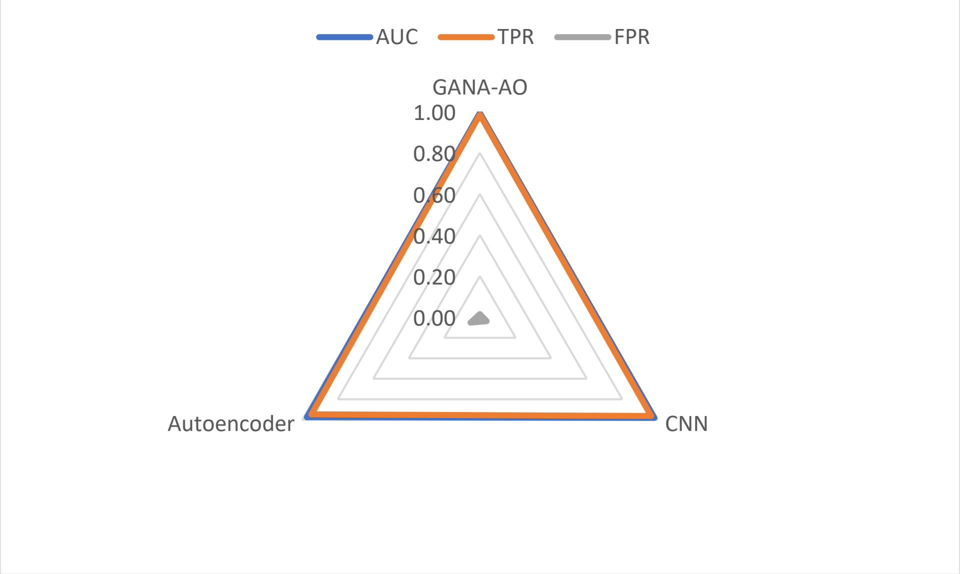

Figure 2 Evaluation of AUC, TPR, FPR

The performance metrics shown in table-2 and figure-1,2 of the anomaly detection models, such as GANA-AO, CNN, and Autoencoder, demonstrate the clear superiority of GANA-AO in improving the cybersecurity of Social Medical Public Healthcare Systems (SMPH). GANA-AO demonstrated a remarkable accuracy of 98%, surpassing both CNN and Autoencoder models by a significant margin. The high accuracy demonstrates GANA-AO expertise in accurately categorizing both regular and abnormal instances in the dataset.

The GANA-AO model demonstrates a precision rate of 98%, indicating its capacity to effectively detect true positives while minimizing the occurrence of false positives. Accurate classification is of utmost importance in healthcare environments, as misidentifying regular occurrences as anomalies can lead to serious repercussions. The 99% recall rate highlights the effectiveness of GANA-AO in identifying a large percentage of real anomalies in the dataset, showcasing its ability to detect potential threats with high sensitivity.

The F1-score of 99% for GANA-AO demonstrates a harmonious equilibrium between precision and recall, highlighting its robustness in effectively managing both aspects of anomaly detection. Moreover, a perfect classification performance is indicated by an Area Under the Curve (AUC) value of 1.00, which further demonstrates the model's ability to accurately differentiate between normal and anomalous instances.

The CNN and Autoencoder models demonstrate commendable performance metrics, achieving accuracy values of 95% and 94% respectively. Although all the models show impressive precision, recall, and F1-score, GANA-AO stands out with its superior performance, particularly in terms of recall and AUC. This highlights the effectiveness of GANA-AO in accurately identifying anomalies in the complex SMPH cybersecurity environment.

Moreover, analyzing the True Positive Rate (TPR) and False Positive Rate (FPR) offers valuable insights into the models' capacity to accurately detect anomalies while minimizing false alarms. GANA-AO demonstrates exceptional performance with a True Positive Rate (TPR) of 99%, indicating a strong ability to accurately detect true anomalies. Additionally, it achieves an impressively low False Positive Rate (FPR) of 0.02%, highlighting its capability to effectively reduce the occurrence of false positives.

Ultimately, the thorough assessment of GANA-AO compared to CNN and Autoencoder models highlights its outstanding ability to detect anomalies in real-time within SMPH. GANA-AO's strong performance in terms of accuracy, precision, recall, and AUC, along with its low false positive rate, make it a reliable solution for enhancing the cybersecurity of healthcare systems. It effectively detects and addresses potential threats in a timely manner.

5. Conclusion and future scope

Conclusively, the study presents and assesses the GANA-AO hybrid deep learning model as an advanced solution for promptly identifying abnormalities in Social Medical Public Healthcare Systems (SMPH). The model utilizes Generative Adversarial Networks (GAN), Autoencoders, and Adam optimization to achieve outstanding performance on the IoT-23 dataset. GANA-AO demonstrates its potential to greatly improve SMPH cybersecurity by surpassing baseline models with a 98% accuracy and a True Positive Rate (TPR) of 99%. The results highlight the model's capacity to promptly identify and resolve malicious activities, thereby safeguarding sensitive healthcare data and ensuring the safety of patients. The study provides a strong and effective technical solution while also highlighting the important role of technology in strengthening the digital boundaries of SMPH.

Potential for Future Expansion:

- Next, we plan to integrate GANA-AO with existing Social Medical Public Healthcare Systems in order to enhance its functionality. Deploying the model in a real-world setting will offer valuable insights into its practical usability, implementation challenges, and its capacity to adjust to the ever-changing nature of cybersecurity threats in healthcare. This integration will also enable ongoing enhancement and fine-tuning, utilizing up-to-the-minute data and evolving threat environments.

- Exploration of Explainability and Interpretability: Improving the clarity and comprehensibility of anomaly detection models is essential for establishing trust among healthcare professionals and stakeholders. Subsequent investigations can prioritize the creation of methodologies aimed at elucidating the decision-making process employed by GANA-AO, thereby offering valuable insights into the rationale behind the identification of specific instances as anomalies. Interpretability is crucial in healthcare settings, as it is necessary for transparent decision-making and effective collaboration between automated systems and human healthcare practitioners.

References

[1] C. Chakraborty, S. M. Nagarajan, G. G. Devarajan, T. V Ramana, and R. Mohanty, "Intelligent AI-based Healthcare Cyber Security System using Multi-Source Transfer Learning Method," *ACM Trans. Sens. Networks*, 2023, doi: 10.1145/3597210.

[2] S. Krishnamoorthy, A. Dua, and S. Gupta, *Role of emerging technologies in future IoT-driven Healthcare 4.0 technologies: a survey, current challenges and future directions*, vol. 14, no. 1. Springer Berlin Heidelberg, 2021.

[3] S. U. Amin and M. S. Hossain, "Edge Intelligence and Internet of Things in Healthcare: A Survey," *IEEE Access*, vol. 9, pp. 45–59, 2021, doi: 10.1109/ACCESS.2020.3045115.

[4] J. Li *et al.*, "A Secured Framework for SDN-Based Edge Computing in IoT-Enabled Healthcare System," *IEEE Access*, vol. 8, pp. 135479–135490, 2020, doi: 10.1109/ACCESS.2020.3011503.

[5] K. Munjal and R. Bhatia, "A systematic review of homomorphic encryption and its contributions in healthcare industry," *Complex Intell. Syst.*, 2022, doi: 10.1007/s40747-022-00756-z.

[6] B. Ç. Uslu, E. Okay, and E. Dursun, "Analysis of factors affecting IoT-based smart hospital design," *J. Cloud Comput.*, vol. 9, no. 1, 2020, doi: 10.1186/s13677-020-00215-5.

[7] H. Saidi, N. Labraoui, A. A. A. Ari, and D. Bouida, "Remote health monitoring system of elderly based on Fog to Cloud (F2C) computing," *2020 Int. Conf. Intell. Syst. Comput. Vision, ISCV 2020*, 2020, doi: 10.1109/ISCV49265.2020.9204096.

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

[9] H. Abie, "Cognitive Cybersecurity for CPS-IoT Enabled Healthcare Ecosystems," in *2019 13th International Symposium on Medical Information and Communication Technology (ISMICT)*, 2019, pp. 1–6, doi: 10.1109/ISMICT.2019.8743670.

[10] M. Alshehri, "Blockchain-assisted cyber security in medical things using artificial intelligence," *Electron. Res. Arch.*, vol. 31, no. 2, pp. 708–728, 2023, doi: 10.3934/era.2023035.

[11] T. M. Ghazal, "Internet of Things with Artificial Intelligence for Health Care Security," *Arab. J. Sci. Eng.*, no. November, 2021, doi: 10.1007/s13369-021-06083-8.

[12] A. G. Prawiyogi and L. Meria, "For a CPS-IoT Enabled Healthcare Ecosystem Consider Cognitive Cybersecurity," vol. 2, no. 1, pp. 24–32, 2023.

[13] A. S. Rajawat, P. Bedi, S. B. Goyal, R. N. Shaw, A. Ghosh, and S. Aggarwal, *AI and Blockchain for Healthcare Data Security in Smart Cities*, vol. 1002. Springer Singapore, 2022.

[14] N. M. Thomasian and E. Y. Adashi, "Cybersecurity in the Internet of Medical Things," *Heal. Policy Technol.*, vol. 10, no. 3, p. 100549, 2021, doi: https://doi.org/10.1016/j.hlpt.2021.100549.

[15] S. Nifakos *et al.*, "Influence of human factors on cyber security within healthcare organisations: A systematic review," *Sensors*, vol. 21, no. 15, pp. 1–25, 2021, doi: 10.3390/s21155119.

[16] M. Muthuppalaniappan LLB and K. Stevenson, "Healthcare cyber-attacks and the COVID-19 pandemic: an urgent threat to global health," *Int. J. Qual. Heal. Care*, vol. 33, no. 1, p. mzaa117, Jan. 2021, doi: 10.1093/intqhc/mzaa117.

[17] S. S. Bhuyan *et al.*, "Transforming Healthcare Cybersecurity from Reactive to Proactive: Current Status and Future Recommendations," *J. Med. Syst.*, vol. 44, no. 5, 2020, doi: 10.1007/s10916-019-1507-y.

[18] S. T. Argaw *et al.*, "Cybersecurity of Hospitals: Discussing the challenges and working towards mitigating the risks," *BMC Med. Inform. Decis. Mak.*, vol. 20, no. 1, pp. 1–10, 2020, doi: 10.1186/s12911-020-01161-7.