International Journal of Wireless and Ad Hoc Communication

♦ ISSN: 2692-4048 Vol: 08, No .02, 2024 ♦ PP. 21–24

Article DOI: https://doi.org/10.54216/IJWAC.080204

FULL LENGTH ARTICLE

Comprehensive Detection of Security Threats in Wireless Ad Hoc Networks: Bridging Healthcare 4.0

Shereen Zaki[1] **Heba R. Abdelhady**[1] **Ahmed A. Metwaly**[1] **Mahmoud M. Ismail**[1,*]

[1] Information Systems Department, Faculty of Computers and Informatics, Zagazig University, Zagazig, Sharqiyah, 44519, Egypt

Emails: SZSoliman@fci.zu.edu.eg · HRAbdelhady@fci.zu.edu.eg · a.metwaly23@fci.zu.edu.eg · mmsabe@zu.edu.eg

Received: September 17, 2023 Revised: December 18, 2023 Accepted: March 25, 2024 ⋆ Corresponding author

ABSTRACT

Healthcare 4.0, which is the integration of digital technologies in healthcare, promises to bring about revolutionary advancements but also introduces significant cybersecurity challenges. This research seeks to address the growing concerns by investigating security threats in Healthcare 4.0 systems. The study uses a multifaceted methodology that includes a comprehensive literature review and empirical analysis using advanced algorithms such as Random Forest. Using visualization techniques, data distribution analysis, and intrusion detection experiments, the research identifies common vulnerabilities and patterns in Healthcare 4.0 environments. The findings highlight the need for proactive measures and strong policies to protect patient data integrity, safeguard medical infrastructure, and ensure continuous provision of health care services. This study calls for a holistic approach to cyber security with an emphasis on collaborative efforts toward strengthening Healthcare 4.0 systems against emerging threats.

Keywords: Cybersecurity ▪ Health informatics ▪ Threat detection ▪ Data privacy ▪ Risk assessment ▪ Security protocols ▪ Internet of Things ▪ Network security ▪ Artificial intelligence (AI) ▪ Threat mitigation ▪ Data breaches ▪ Blockchain

1. INTRODUCTION

Healthcare 4.0, which is the integration of digital technologies in healthcare, has transformed the industry and promises improved patient care, efficient operations, and data-driven decision-making [1]. Healthcare 4.0 leverages interconnected devices, artificial intelligence (AI), the Internet of Things (IoT), and big data analytics to enhance healthcare delivery [2]. However, this technological advancement has brought forth a myriad of cybersecurity challenges, posing substantial threats to patient data security, medical infrastructure, and overall healthcare systems [3]. The healthcare sector has experienced an alarming increase in cyber threats and security breaches in recent years. Malicious actors exploit vulnerabilities in interconnected systems intending to access sensitive patient information, disrupting healthcare operations, and compromising the integrity of medical devices [4]. These threats not only violate patient privacy but also hinder the provision of essential healthcare services, thus emphasizing the need to strengthen healthcare systems against evolving cybersecurity risks [5].

A comprehensive and proactive approach is required to address security threats in Healthcare 4.0. Conventional security measures are not enough to protect against sophisticated cyber-attacks. A holistic strategy involves technological solutions, strong policies, strict protocols, regular risk assessments, and a culture of cybersecurity awareness among healthcare practitioners and stakeholders. This approach aims at strengthening defenses across the entire healthcare ecosystem from patient data repositories to interconnected medical devices [4, 6, 7].

This paper explores the multifaceted landscape of security threats in Healthcare 4.0 with a focus on the need for a holistic approach to threat detection and mitigation. By analyzing

prevalent cybersecurity challenges, exploring current detection strategies, and proposing comprehensive frameworks, this research seeks to provide insights that strengthen healthcare systems against emerging threats. Furthermore, it seeks to emphasize the importance of proactive measures in protecting patient data integrity, preserving medical infrastructure, and ensuring uninterrupted delivery of quality healthcare services in the era of Healthcare 4.0.

2. RELATED WORKS

This section aims to synthesize and analyze the body of existing literature, encompassing diverse perspectives on cybersecurity in Healthcare 4.0. The literature related to Healthcare 4.0 and its associated security challenges has seen substantial exploration and investigation by various scholars. Kumar et al. [6] introduced a comprehensive study focusing on the design, simulation, and implementation of Smart Healthcare within the framework of Healthcare 4.0 processes. Aceto et al. [7] delved into the convergence of Industry 4.0 and healthcare, highlighting the significance of the Internet of Things (IoT), Big Data, and Cloud Computing in the context of Healthcare 4.0. Moustafa et al. [8] proposed a novel threat intelligence scheme specifically tailored for safeguarding Industry 4.0 systems. Al-Jaroodi et al. [9] contributed to the discourse by emphasizing the holistic management of transformation in Healthcare 4.0. Kumari et al. [10] explored the potential and challenges of Fog Computing within the Healthcare 4.0 environment.

Pang et al. [11] introduced the convergence of automation technology, biomedical engineering, and health informatics as a crucial element in the realization of Healthcare 4.0. Blockchain technology's role in embracing Healthcare 4.0 was underscored by Abbate et al. [12], shedding light on its potential applications within this domain. Chataut et al. [13] conducted a comprehensive review of IoT applications and future prospects across various sectors, including healthcare, agriculture, smart homes, smart cities, and Industry 4.0. Ahmed et al. [14] offered insights into the progression from artificial intelligence to explainable artificial intelligence within Industry 4.0, exploring its dimensions and applications.

Pace et al. [15] proposed an edge-based architecture to support efficient applications for Healthcare Industry 4.0. Yaacoub et al. [16] investigated the limitations, issues, and recommendations for securing Internet of Medical Things systems. Collectively, these studies emphasize that cybersecurity in Healthcare 4.0 requires a combination of emerging technologies, risk-aware architectures, and operational governance mechanisms.

3. METHODOLOGY

This section outlines the structured approach adopted to investigate and analyze the landscape of security threats, detection methodologies, and mitigation strategies specific to the Healthcare 4.0 domain. Random Forest is a powerful ensemble learning technique that works by building multiple decision trees and combining their predictions to improve accuracy and robustness in classification tasks. This method takes advantage of the strength of individual decision trees while reducing their tendency to overfit or be biased.

Random Forest combines different trees created from random subsets of features and data points, which results in better generalization and performance, making it a popular method for predictive modeling and classification tasks (see Figure 1). In cybersecurity, Random Forest has been shown to be effective in detecting anomalies as well as identifying intrusion attempts in complex systems. It can handle different types of data, high-dimensional data, and assess feature importance naturally, making it suitable for intrusion detection tasks.

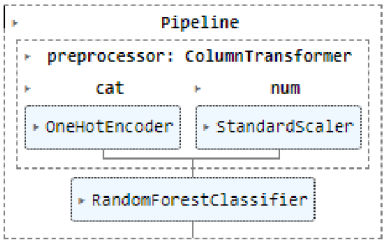

Figure 1. Architecture of proposed system.

By using its ensemble learning strategy and ability to handle unbalanced datasets, Random Forest is useful in identifying suspicious activities and potential security breaches. In this study, we apply the Random Forest algorithm to the domain of Healthcare 4.0 security for intrusion detection. By leveraging its robustness and adaptability, we utilize Random Forest to analyze and classify patterns indicative of potential security threats within interconnected healthcare systems.

The algorithm's ability to discern abnormal activities amidst the complexity of healthcare data enables the detection of anomalous behavior, potentially flagging suspicious incidents that may compromise the integrity and confidentiality of patient information, medical devices, and overall system functionality in the context of Healthcare 4.0.

4. RESULTS AND DISCUSSION

This section presents and analyzes the results obtained from the rigorous examination of existing vulnerabilities, detection methodologies, and mitigation strategies within Healthcare 4.0 environments. Table 1 presents a visual representation of the statistical analysis conducted on the dataset. Utilizing various graphical tools such as histograms, box plots, and scatter plots, we visually depict the distribution, central tendencies, and relationships within the dataset. These visualizations offer a succinct and comprehensive overview, facilitating a clearer understanding of the dataset's characteristics and providing valuable insights into the trends and patterns present in the data.

Table 1. Statistical Analysis Visualizations of Dataset Characteristics

	Source Port	Destination Port	Packet Length	Anomaly Scores
count	40000	40000	40000	40000
mean	32970.36	33150.87	781.4527	50.11347
std	18560.43	18574.67	416.0442	28.8536
min	1027	1024	64	0
25%	16850.75	17094.75	420	25.15
50%	32856	33004.5	782	50.345
75%	48928.25	49287	1143	75.03
max	65530	65535	1500	100

In Figure 2, we present a visual representation of the data distribution, employing histograms and density plots to illustrate the frequency and distribution patterns of the dataset. This visualization offers a clear depiction of the spread and concentration of data points across various ranges or categories, providing valuable insights into the distributional characteristics and helping identify potential outliers or clusters within the dataset.

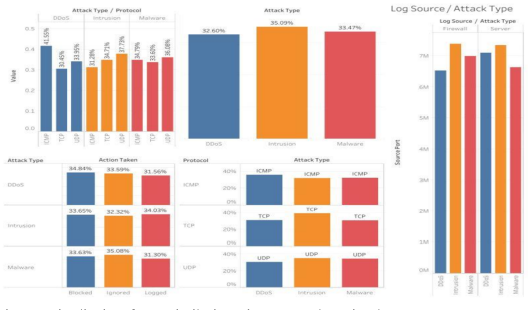

Figure 2. Visualization of Data Distribution: Histograms and Density Plots.

Figure 3 showcases heat maps representing different attack patterns within the dataset. Each heat map visually delineates the occurrence and intensity of specific attacks across various parameters or time intervals. These visual representations offer a comprehensive overview of attack frequencies and their correlations, enabling a nuanced understanding of attack patterns, their temporal distribution, and potential associations among different attack types within the analyzed dataset.

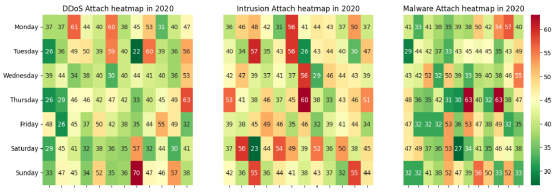

Figure 3. Heat Maps Illustrating Attack Patterns and Frequencies.

In Figure 4, we present visual representations depicting the performance of distinct classifiers in detecting security threats within the dataset. These visualizations include ROC curves, precision-recall curves, or confusion matrices, showcasing the comparative efficacy of different classification models. These visuals offer a comprehensive insight into the classifiers' detection capabilities, illustrating their sensitivity, specificity, accuracy, and potential trade-offs. Such visual representations aid in assessing and comparing the performance of various classifiers, assisting in informed decision-making regarding the selection of optimal models for threat detection within the studied Healthcare 4.0 environment.

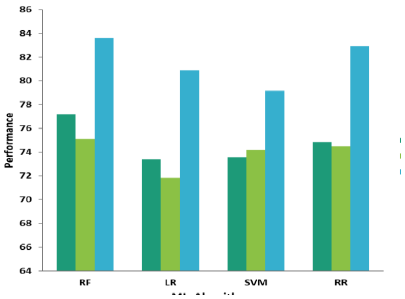

Figure 4. Classifier Performance Visualizations: ROC Curves, Precision-Recall Curves, and Confusion Matrices.

5. CONCLUSION

This research endeavors to address the pressing concerns surrounding security threats in Healthcare 4.0 by illuminating the multifaceted nature of cybersecurity challenges and proposing a comprehensive framework for threat detection and mitigation. Through an extensive review of existing literature and empirical analysis utilizing advanced algorithms such as Random Forest, this study highlights the urgency of fortifying healthcare systems against evolving threats.

The findings underscore the critical need for proactive measures, robust policies, and advanced technologies to safeguard patient data integrity, protect medical infrastructure, and ensure the uninterrupted delivery of quality healthcare services amidst the transformative landscape of Healthcare 4.0. By emphasizing the significance of a holistic approach to cybersecurity, this study aims to contribute valuable insights and strategic recommendations essential for the resilience and security of Healthcare 4.0 systems.

REFERENCES

[1] J. J. Hathaliya and S. Tanwar, "An exhaustive survey on security and privacy issues in healthcare 4.0," *Computer Communications*, vol. 153, pp. 311–335, 2020.

[2] G. Manogaran, C. Thota, D. Lopez, and R. Sundarasekar, "Big data security intelligence for healthcare industry 4.0," in *Cybersecurity for Industry 4.0: Analysis for Design and Manufacturing*, 2017, pp. 103–126.

[3] G. L. Tortorella, F. S. Fogliatto, A. M. C. Vergara, R. Vassolo, and R. Sawhney, "Healthcare 4.0: Trends, challenges and research directions," *Production Planning & Control*, vol. 31, no. 15, pp. 1245–1260, 2020.

[4] S. K. Jagatheesaperumal, P. Mishra, N. Moustafa, and R. Chauhan, "A holistic survey on the use of emerging technologies to provision secure healthcare solutions," *Computers and Electrical Engineering*, vol. 99, p. 107691, 2022.

[5] S. Silvestri, S. Islam, D. Amelin, G. Weiler, S. Papastergiou, and M. Ciampi, "Cyber threat assessment and management for securing healthcare ecosystems using natural language processing," *International Journal of Information Security*, pp. 1–20, 2023.

[6] A. Kumar, R. Krishnamurthi, A. Nayyar, K. Sharma, V. Grover, and E. Hossain, "A novel smart healthcare

design, simulation, and implementation using healthcare 4.0 processes," *IEEE Access*, vol. 8, pp. 118 433–118 471, 2020.

[7] G. Aceto, V. Persico, and A. Pescapé, "Industry 4.0 and health: Internet of things, big data, and cloud computing for healthcare 4.0," *Journal of Industrial Information Integration*, vol. 18, p. 100129, 2020.

[8] N. Moustafa, E. Adi, B. Turnbull, and J. Hu, "A new threat intelligence scheme for safeguarding industry 4.0 systems," *IEEE Access*, vol. 6, pp. 32 910–32 924, 2018.

[9] J. Al-Jaroodi, N. Mohamed, N. Kesserwan, and I. Jawhar, "Healthcare 4.0–managing a holistic transformation," in *2022 IEEE International Systems Conference (SysCon)*, 2022, pp. 1–8.

[10] A. Kumari, S. Tanwar, S. Tyagi, and N. Kumar, "Fog computing for healthcare 4.0 environment: Opportunities and challenges," *Computers & Electrical Engineering*, vol. 72, pp. 1–13, 2018.

[11] Z. Pang, G. Yang, R. Khedri, and Y.-T. Zhang, "Introduction to the special section: Convergence of automation technology, biomedical engineering, and health informatics toward the healthcare 4.0," *IEEE Reviews in Biomedical Engineering*, vol. 11, pp. 249–259, 2018.

[12] S. Abbate, P. Centobelli, R. Cerchione, E. Oropallo, and E. Riccio, "Blockchain technology for embracing healthcare 4.0," *IEEE Transactions on Engineering Management*, 2022.

[13] R. Chataut, A. Phoummalayvane, and R. Akl, "Unleashing the power of iot: A comprehensive review of iot applications and future prospects in healthcare, agriculture, smart homes, smart cities, and industry 4.0," *Sensors*, vol. 23, no. 16, p. 7194, 2023.

[14] I. Ahmed, G. Jeon, and F. Piccialli, "From artificial intelligence to explainable artificial intelligence in industry 4.0: A survey on what, how, and where," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 8, pp. 5031–5042, 2022.

[15] P. Pace, G. Aloi, R. Gravina, G. Caliciuri, G. Fortino, and A. Liotta, "An edge-based architecture to support efficient applications for healthcare industry 4.0," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 1, pp. 481–489, 2018.

[16] J.-P. A. Yaacoub, M. Noura, H. N. Noura, O. Salman, E. Yaacoub, R. Couturier, and A. Chehab, "Securing internet of medical things systems: Limitations, issues and recommendations," *Future Generation Computer Systems*, vol. 105, pp. 581–606, 2020.

[17] M. Ismail and F. A. Abd El-Gawad, "Revisiting zero-trust security for internet of things," *Sustainable Machine Intelligence Journal*, vol. 3, 2023.

[18] M. Puri and S. Gochhait, "Data security in healthcare: Enhancing the safety of data with cybersecurity," in *2023 8th International Conference on Communication and Electronics Systems (ICCES)*, 2023, pp. 1779–1783.

[19] R. Gupta, S. Tanwar, S. Tyagi, and N. Kumar, "Tactile-internet-based telesurgery system for healthcare 4.0: An architecture, research challenges, and future directions," *IEEE Network*, vol. 33, no. 6, pp. 22–29, 2019.

[20] M. Javaid, A. Haleem, R. Vaishya, S. Bahl, R. Suman, and A. Vaish, "Industry 4.0 technologies and their applications in fighting covid-19 pandemic," *Diabetes & Metabolic Syndrome: Clinical Research & Reviews*, vol. 14, no. 4, pp. 419–422, 2020.