The Application of Deep Neural Network to Vulnerability Management on Cyber Physical System – A Systematic Review

[1]Ozioko Frank Ekene., [2]Mba Chioma Juliet

[1]Department of Computer Sciences Enugu State University of Science and Technology (ESUT), Enugu, Nigeria

[2]Department of Computer Sciences, Enugu State Polytechnic, Iwollo, Enugu, Nigeria

DOI: https://doi.org/10.51584/IJRIAS.2025.10040102

Received: 16 April 2025; Accepted: 21 April 2025; Published: 26 May 2025

ABSTRACT

Vulnerability management plays a pivotal role in securing Cyber-Physical Systems (CPS) from emerging risks by identifying, assessing, and mitigating potential threats. This paper provides a comprehensive review of existing vulnerability management techniques, highlighting their challenges and limitations when applied to CPS. Specifically, the work examined the role of machine learning, particularly Deep Neural Networks (DNN), in enhancing vulnerability detection and prediction models. DNNs have shown promising results in detecting complex, high-dimensional patterns within large datasets, making them ideal for securing CPS environments. Based on the findings, the paper proposes future research directions that focus on refining DNN-based models to tackle scalability, interpretability, and adaptive security challenges in CPS. By leveraging these advancements, we aim to facilitate more robust, proactive vulnerability management solutions, ultimately contributing to the overall resilience of Cyber-Physical Systems in the face of increasingly sophisticated cyber threats.

Keywords: Cyber-Physical Systems; Deed Neural Network; Vulnerability management; Machine Learning; DNN; Security

INTRODUCTION

Cyber-Physical Systems (CPS), such as “smart systems,” are systems for integration of software and physical components, and they have potential uses in almost every industry (Umer et al., 2022). CPSs generate vast amounts of data, and major corporations are shifting towards cloud-based solutions to provide scalability and adequate storage (Khan et al. 2022). Although cloud-based CPS (CCPS) enhances the features of traditional CPS, it also raises concerns about data protection and privacy. CPS first appeared 2006/2007, and since then, many researchers have worked to advance both the theory and practice of CPSs (Khan et al., 2022). Smart grids, autonomous and intelligent transportation systems, electronic healthcare system, search and rescue, smart manufacturing and industry 4.0, smart cities, detection control, aerospace, defence, and many more applications are making use of CPSs thanks to the rapid development of technologies like wireless sensor networks (WSN), internet of things (IoT), cloud computing (CC), big data (BD), and artificial intelligence (AI) (Sochima et al., 2025; Kekong et al., 2019). These technologies will support our essential infrastructure, serve as the backbone of developing and future smart services, and enhance many aspects of our lives Ene et al., 2019). The scope of CPS's potential impact on society as a whole is vast. Some examples that have already been developed include driverless vehicles, robotic surgery, smart buildings, a smart electric grid, smart manufacturing, and implanted medical devices (Exe et al., 2022). Because of its rapid development, CPS has expanded to include many fields and facilitate numerous uses. Hence, this created a need for standards to describe the best practices for implementation and deployment, reference architectures, and models for designing an accurate CPS. CPS reliability and performance are challenged by the high degree of automation and interconnections between physical components and embedded computers that monitor and manage physical processes.

According to Sakr and Elgammal (2016)he made a comprehensive data analytics framework for smart healthcare services Big Data Res (2016).Umer et al. (2022) grouped the components of CPS into three, namely the physical

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue IV April 2025

layer, application layer, and network layer. According to Khan et al. (2022) and Umer et al. (2022), CPS during the design stage does not integrate security measures like other networking systems due to its heterogeneous nature, different operating protocols, software, and hardware it uses during communication, thus making it vulnerable to cyber threats.

Snehi and Bhandari (2021)studied and examined the state-of-the-art Cyber–Physical System, components of recent-day Cyber–Physical System, architectural details, security issues with a focus on most devastating DDoS and IoT-DDoS attacks. Fog Computing has been proposed as a layer between perception and cloud for performance improvement and executing the delegated tasks on behalf of the cloud. They studied the proposed solutions in the field of DDoS/IoT-DDoS detection and mitigation. The vulnerability study is not limited in scope to DDoS attacks but has the applicability to more cybersecurity concerns as well. In this study they did not consider the vulnerabilities in the layers of cyber physical system. Given the broad spectrum of scope for electronic healthcare medical Cyber–Physical Systems, I further intend to present a solution against the vulnerabilities across the three layersof CPS in the IOT because the discussed security concerns should be given the utmost attention and should be addressed energetically.

Recent trends demonstrated the extensive use of AR and VR technology in developing healthcare robots with WSN-based Internet of Things (IoT) (Odo et al., 2022). WSN is a technology used to monitor patient's illness over a specific area with the help of a large number of sensor nodes. Each sensor node focuses on sensing some physical attributes such as temperature, humidity, pressure, and so on, which should be transmitted through wireless communication. In addition, each transmitting sensor node is capable of sensing either one or multiple attributes in a single-hop or multiple-hop manner and transmitted it to a single receiving node in the network called a sink node or base station (BS). The structure of a WSN is divided into three categories: star network, mesh network, and hybrid star-mesh network. But they did not consider any vulnerability along the three node which is a very big risk to patient data.

LITERATURE REVIEW

Bin et al., (2023) presents the use of machine learning technique for detection and classification of vulnerability in Internet of Things (IoT) device security. In order to study the approaches and instruments utilised in IoT contexts for vulnerability identification, this work uses machine learning algorithms on a variety of datasets, including IoT23. In this article, the machine learning pipeline for identifying IoT vulnerabilities is detailed, and the common possible vulnerabilities of IoT systems are examined on each tier. It looks at possible Internet of Things vulnerabilities at every architectural tier and provides an overview of how machine learning may be used to find vulnerabilities in IoT devices. Furthermore, in order to identify and address vulnerabilities in IoT settings, current research trends on machine learning-based vulnerability identification are compiled and examined at each IoT layer. It also examined the various approaches that may be used to lessen these vulnerabilities.

The methodology for vulnerability mitigation measures was put up to improve IoT security against possible dangers. The study's findings showed that, given the benefits of machine learning and deep learning, it is essential to use these methods to identify and address Internet of Things vulnerabilities across all industries.

Ayoub and Narhimene (2023) (ML for transmission level security).The transmission of medical data between devices composing the IoMT (internet of medical things) and the server enables the remote healthcare system to continuously monitor the vulnerability and treat patients in real time. However, the researcher intend to represents a high interest for cyber-attackers, who, in case of a successful attack, can cause severe repercussions for the patient, ranging from violation of privacy to death. In addition, the heterogeneous nature of the devices used increases the surface of attack, which requires the design of a secure architecture for the IoMT.

In this context, (Gao and Thamilarasu, 2017) proposed a solution to detect attacks that target connected medical devices based on ML methods. Learning the normal behavior of the vulnerability on medical device and allows the detection of any deviation from this behavior and generates a warning notification sent to the patient.The ML model is deployed on an external device that monitors the network and performs an analysis to detect an anomaly. To test the effectiveness of their solution, the authors used three datasets of different sizes generated by a Castilia simulator and evaluated the performance of DT compared to SVM and k-means. After conducting

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue IV April 2025

various tests, the authors found that DTs provided higher accuracy, generated fewer false positives, and had a faster training and prediction time.

In another work performed by (Al-Shaher et al., 2017), they proposed to protect the private healthcare system from known viruses, worms, spyware, and denial-of-service attacks by designing and implementing an Intelligent Healthcare Security System (IHSS). The IHSS integrates the firewall, network intrusion detection subsystem, and web filter. The IHSS is intended to enhance the capabilities of these network protection systems using artificial intelligence approaches. The authors use MLP activated by wavelet transform to classify network traffic and protect vulnerability in patient data.

The intrusion detection subsystem uses a wavelet neural network to determine which type of attacks are occurring by solving the multi-class problem. In web filters, they use Wavelet Neural Network to detect malware. After evaluating their method, they obtained 93% accuracy with two hidden layers and 90% with one hidden layer.

Other research group (He et al. 2019) proposed an AIT based on a stacked Autoencoder for a nomaly detection in the Connected Healthcare System, as outlined in their publication. The method in volvesse veral stages of data processing, including mapping, discretization, and normalization, before feeding the data to the stacked Autoencoder. The Auto encoder isused to extract there levant features, which the DNN models then use to perform detection and classify the data as either an attack or not. To evaluate the performance of their IDS solution, the authors collected a real dataset from patients and simulated various types of attacks, such as DoS, counterfeit attacks, temper attacks, and replay attacks. They compared the performance of different DNN models, including SVM, NB, KNN, and XGBoost, using metrics such as accuracy, FPR, and FNR. After conducting several tests, the authors found that the XGBoost model achieved the best performance with 97.83% accuracy, 2.35% FPR, and 1.65% FNR.

Lee et al. (2021), he proposed an IDS using ML and multi-class classification for the healthcare IoT within the smart city. The authors used CNN as an ML method to classify the network events generated by different medical devices into four classes, namely (critical, informal, major, and minor). Before the data are fed to the model, the data are preprocessed by transforming the categorical data into numerical data, then normalizing the data to take values within the same range. To evaluate their model, the authors generated a dataset by collecting data from six medical devices and then used them to compare their model results with other ML models regarding AUC, F1-score, Precision, and Recall. After performing the different tests, the authors found that their CNN model produces better results than other ML methods.

Salemi et al. (2021) they presented a novel approach for predicting Distributed Denial of Service (DDoS) attacks in healthcare systems, as opposed to merely detecting them. The authors demonstrated that DDoS attacks cause traffic data to become chaotic, which can be analysed using the Lyapunov Expansions Analysis and the Echo State Network. To implement their approach, the authors first represented network traffic as time-series data and applied a simple exponential smoothing method to predict future traffic. They then calculated the time-series prediction error by subtracting the predicted data from the actual data, which served as the basis for DDoS attack analysis. The authors then utilized a recurrent Deepneural network to predict the time series and used the LEA-MA method to detect the DDoS attack. To evaluate their method's effectiveness, the authors tested it on the DARPA dataset and used metrics such as precision, recall, and F1-score. Their experiments showed that their proposed method could efficiently predict DDoS attacks.

In the following, a distributed IDS within the IoMT systems are presented as a solution. Martinsen et al., (2022) researched on the robustness and vulnerability measurement of deep learning models for cyber defence. In order to develop computational methods capable of quantitatively evaluating the robustness and vulnerability of deep learning tools that can be applied in cybersecurity settings, this study aims to investigate mathematical concepts and quantitative measures of robustness and vulnerability of machine learning systems to adversarial data. The robustness analysis of infrastructure cyber security is the main topic of the study's second phase. The study examines the durability of neural networks exposed to noisy or contaminated data using a microgrid power system model and learning-based fault detection as the testbed. Lastly, the study investigates the distributional robustness of neural networks, which are occasionally applied outside of the training context. The result of the

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue IV April 2025

study shows that on data with log-normally distributed initial condition, our RMSE was 0.230 and the misclassification rate was 0.

Jeon and Kim (2021) presents Automated Vulnerability Analysis System (AutoVAS), which is a vulnerability analysis system developed using deep learning approach. This framework leverages a compiler-based program slicing method to overcome the lengthy context dependence problem and applies different embedding methods and symbolic representation techniques to handle the Out-of-Vocabulary (OoV) problem. In addition, various datasets in the National Vulnerability Database (NVD) and Software Assurance Reference Dataset (SARD) wereused for the source code employed as the learning data to search for various types of security vulnerabilities in the vulnerable datasets, and a learning dataset with 98 vulnerabilities from the Common Weakness Enumeration (CWE) database and 719 vulnerabilities from the Common Vulnerabilities and Exposures (CVE) was constructed. Furthermore, an oversampling strategy was utilised to alleviate the imbalance problem in the datasets. The result of the technique achieved a False Negative Rate (FNR) of 1.88%, a False Positive Rate (FRR) of 3.62%, and an F1-score of 96.11%. Eleven vulnerabilities were detected in nine open-source projects.

Among these solutions, there is work made by (Thamilarasu and Odesile, 2017) They proposed an approach that utilizes mobile agents to conduct penetration testing and secure the medical equipment network. The proposed system is characterized by its hierarchical, autonomous, and distributed nature. Intrusion detection is performed using a regression algorithm at the medical equipment level and machine leaning technics (ML) at the network level. Mobile agents traverse from one node to another or within a cluster, collecting network activities or device data based on their role as network or device intrusion detection agents. At the end of an intrusion test, the mobile agent classifies the collected samples as voluntary, malicious, or suspicious. The mobile agent migrates to another node if the samples are classified as voluntary. However, if the samples are malicious, an alarm is generated, and the data is sent to the cluster head. If the samples are suspicious, a request for intervention is sent to the cluster head. The cluster head deploys a special agent to collect data from the network or medical equipment of the entire cluster. The collected data are then tested to determine whether they are vulnerable or malicious.

Kumar et al. 2021 proposed an IDS that utilizes ensemble learning and a fog-cloud architecture to detect cyber-attacks in IoMT networks. The system preprocesses traffic data by converting categorical values into numerical values, replacing missing values with the mean of the corresponding feature values, and selecting the relevant features for intrusion detection using the correlation coefficient method. The numerical values are then normalized using the min-max technique to ensure they fall within a specific range. The system uses a learning set consisting of NB, DT, and RF algorithms, which produce three prediction outputs. These outputs are then fed to XGBoost to produce the final output using majority voting. When an intrusion is detected, the administrator is alerted. The framework is deployed using a fog-cloud architecture, which utilizes Software as a Service at the fog level and Infrastructure as a Service at the cloud level. The authors evaluated their framework using the Ton-IoT dataset, representing data collected from heterogeneous and large-scale IoT networks. The vulnerability assessment were accuracy, detection rate, precision, FAR, and F1-score. The results show a detection rate of 99.98%, an accuracy of 96.35%, and a reduction of up to 5.59% of the FAR. These results surpassed those of previous studies that used IDS.

In another research made by Gupta et al. (2022) used deep hierarchical stacked neural networks to detect attacks that would attempt to modify the data flow, including meta-information that transits between the gateways and the edge cloud and between the edge cloud and the core cloud within multi-cloud healthcare systems called MUSE. This method includes reusing the edge cloud's trained layers to merge them and form a pre-trained model at the core cloud level. The tests were performed on three different datasets: UNSW-BOT-IoT and UNSW15 and one generated by the authors. A comparison was made with the method that does not reuse the trained layers of the edge cloud. The results show that the solution proposed by the authors improves the training efficiency and accuracy with a rate that varies between 95%–100% and reduces the training time by 26.2%.

The proposed IDS solution at the fog level has the advantage of being close to the IoT devices and therefore offers a rapid response, decentralization and preserves data privacy. However, the fog level faces an increase in the amount of data arriving at the fog level, which requires a lightweight solution.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue IV April 2025

Hameed et al. (2022) present an incremental ensemble learning method called Weighted Hoeffding Tree Ensemble system consisting of an incremental learning classifier for the industrial IoMT. Tests on NSL-KDD and ToN-IoT datasets and comparison with single incremental classifiers and Bagging Hoeffding Tree ensemble algorithms show that the proposed solution is lightweight and presents a trad-off between accuracy and overhead (CPU, memory and time) and outperforms the results of previous studies.Other works have proposed SDN as an architecture for ML-based IDS within IoMT systems.

Khan and Akhunzada, (2021) present a hybrid model based on DL for malware detection in IoMT deployed at the SDN plane application level. The system proposed by the authors consists of feature extraction using CNN, and then LSTM is used to classify the data as malware. The authors used the current state-of-the-art IoT malware publicly available dataset to evaluate their model. In addition, they compared their model with the constructed hybrid DL-driven. After performing various tests, the authors found that the model outperformed the other methods regarding detection accuracy and speed efficiency.

In another study made by (Singh et al. 2022), the author proposed a solution for intrusion detection at the IoMT networks level using Hierarchical Federated Learning (HFL) based on hierarchical long-term memory. Their solution is deployed on the distributed dew servers of the IoMT framework, with a backend supported by cloud computing at the edge layer. The proposed HFL solutionaggregates models from different entities that compose the healthcare institution at the dew-servers level to obtain local models. These local models are then aggregated at the cloud computing level to obtain the global model, which is redistributed to the different dew servers participating in the learning process. This iterative process is repeated until the global model achieves a high accuracy. Classification matric of the above methods using a Table 1

Table 1: Summary of Literature

S/No	Author/Research method	Findings	Pros	Cons	Remarks
1	Machine learning (Bin et al., 2023)	ML techniques used to detect/classify vulnerabilities in IoT using datasets like IoT23	Covers each tier of IoT architecture; detailed ML pipeline	Lack of real-world system implementation	Comprehensive overview of ML use for IoT vulnerability detection
2	ML for transmission-level security (Ayoub &Narhimene, 2023)	Highlights threat of data transmission in IoMT; proposes secure architecture	Relevant to real-time health systems	General discussion without implementation/test results	Emphasizes need for robust security in IoMT
3	Decision Trees vs SVM vs k-means (Gao & Thamilarasu, 2017)	DT outperformed others in anomaly detection for medical IoT	High accuracy, low false positives	Simulator-based data may not reflect real-world	Validates ML for medical device attack detection
4	Wavelet Neural Network (Al-Shaher et al., 2017)	IHSS system achieved ~93% accuracy in detecting healthcare threats	AI integration enhances detection capability	Performance depends on wavelet feature quality	Strong case for neural networks in healthcare IDS
5	Stacked Autoencoder (He et al., 2019)	XGBoost achieved 97.83% accuracy in detecting attacks in Connected Healthcare	High precision/recall; real patient data used	Complexity of training multiple models	Demonstrates robustness of DNNs in healthcare

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue IV April 2025

6	CNN-based IDS (Lee et al., 2021)	CNN outperformed other models in classifying medical device events	Effective for multi-class classification	Requires large, well-labeled datasets	Useful for event severity classification in IoMT
7	Echo State Network + Lyapunov Analysis (Salemi et al., 2021)	Proposed method can **predict** DDoS attacks	Shift from detection to prediction	Limited application beyond DDoS	Innovative use of chaos theory and RNNs
8	Robustness measurement (Martinsen et al., 2022)	Evaluated DL model robustness under adversarial conditions	Quantitative vulnerability assessment	Focuses on model, not system-level defenses	Promotes trust in AI for critical systems
9	Deep Learning AutoVAS (Jeon & Kim, 2021)	Achieved 96.11% F1, 1.88% FNR, using CWE/CVE datasets	Tackles OoV and imbalance issues	High complexity and resource need	Scalable for source code vulnerability detection
10	Mobile Agent IDS (Thamilarasu &Odesile, 2017)	Hierarchical IDS classifies data as voluntary, suspicious, or malicious	Autonomous and adaptive	Overhead of agent migration	Novel mobility in security detection

Key Insights and Limitations from Table 1:

1. **Hameed et al. (2022):** The ensemble approach shows a trade-off between accuracy and resource consumption (CPU, memory, time). It may struggle with large-scale IoMT systems or high-velocity data.
2. **Khan &Akhunzada (2021):** The hybrid deep learning approach outperforms traditional methods in accuracy and speed, but the model might not be adaptable for non-malware attack detection.
3. **Singh et al. (2022):** The use of hierarchical federated learning enhances distributed intrusion detection, but the system's scalability and adaptability to dynamic IoMT networks may need further exploration.
4. **Khan et al. (2022):** Their approach improves attack detection while ensuring interpretability via XAI, but it might not scale well for large IoMT deployments or handle diverse attack types effectively.
5. **Hady et al. (2020):** By combining medical and network data, the IDS improves threat detection, but it may face limitations in detecting more sophisticated or novel attack vectors in real-world scenarios.

In general, many of these studies focus on improving detection accuracy and speed but also have limitations regarding scalability, adaptability, and coverage of different attack types or real-world environments.

This table condenses the research methods and highlights possible limitations in each study. It shows how various machine learning approaches are being used to detect vulnerabilities and mitigate attacks in IoT and healthcare systems, but also emphasizes challenges related to dataset size, real-world deployment, and scalability.

RESEARCH METHODOLOGY

The research methodology applied for this study is the literature review and theoretical analysis methodology (Tuner et al., 2018). The study's goals and scope are first established, with a particular emphasis on CPS security issues and the use of DNN for vulnerability identification. For the purpose of finding pertinent papers, a comprehensive search is carried out utilising certain keywords across academic databases like IEEE Xplore and Google Scholar. The research are then categorised according to specific themes, such as DNN applications, current evaluation methods, and security flaws in CPS systems. The technique places a strong emphasis on a

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue IV April 2025

critical review of the research, contrasting various strategies and pointing out important gaps, including the shortcomings of current datasets and the difficulties in implementing DNNs in real-time.

Theoretical examination highlights the advantages of neural networks in identifying anomalies and non-linear patterns by integrating data from the literature to create a conceptual framework for employing DNN in CPS security.The methodology lays the groundwork for future work, such as the creation of hybrid models and more effective, interpretable DNN methodologies, by synthesising important theoretical principles and evaluating gaps in existing research. The study ends with a discussion of the practical ramifications and a research agenda for this developing topic.

DISCUSSION

Healthcare cyber-physical systems in medical applications several surveys about CPS are found in the literature. There are many common research challenges in CPS and healthcare CPS but with different emphasized aspects. Table 2 below gives some of the important application domains where CPS has proven to be beneficial. We divided surveys into three categories, i.e., Cyber-physical systems (CPS) in Smart Healthcare, medical cyber-physical systems for Pandemics, and Security and privacy in Medical cyber-physical systems. Therefore, we conduct this survey to address the main challenges in medical CPS.

Table 2: Summarize the proposed solutions, techniques, and limitations for each citation

Citation	Proposed Solution	Technique	Limitation
Hameed et al. (2022)	An incremental ensemble learning method using Weighted Hoeffding Tree Ensemble for IoMT security	Weighted Hoeffding Tree Ensemble (incremental learning classifier)	Trade-off between accuracy and overhead (CPU, memory, time); may not generalize to other IoMT contexts.
Khan &Akhunzada (2021)	Hybrid deep learning model for malware detection in IoMT at the SDN application level	CNN for feature extraction and LSTM for classification	Limited to malware detection; may not detect other types of attacks or work across all IoMT environments.
Singh et al. (2022)	Hierarchical Federated Learning (HFL) for intrusion detection in IoMT networks	Hierarchical Federated Learning (HFL) with hierarchical long-term memory	Scalability issues with model aggregation at cloud level; limited dataset evaluation.
Khan et al. (2022)	Explainable AI (XAI) to improve trust and interpretability of attack detection in IoMT	Simple Recurrent Units with skip connections; Local Interpretable Model-Agnostic Explanations (XAI)	Limited to specific datasets (ToN-IoT); may not scale well for large IoMT networks or more complex attacks.
Hady et al. (2020)	IDS combining medical and network data for real-time threat detection in healthcare systems	ML methods like SVM, KNN, RF, and ANN	Focused on MITM attacks (spoofing, data alteration); limited by dataset scope and real-world applicability.

Key Insights:

1. **Hameed et al. (2022):** The proposed ensemble solution is lightweight and offers a trade-off between performance and resource usage. The main limitation is its applicability to other IoMT systems or large-scale networks where the overhead may become more significant.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue IV April 2025

2. **Khan &Akhunzada (2021):** This hybrid deep learning approach is effective for malware detection, but it is specialized for malware and may not detect other forms of attacks in IoMT systems. It's also limited by the dataset used for evaluation.

3. **Singh et al. (2022):** Their solution based on Federated Learning is highly efficient for distributed IoMT systems, but scalability and efficiency across large healthcare networks or diverse data sources can be a concern.

4. **Khan et al. (2022):** The integration of XAI improves model transparency, which is critical for IoMT security, but the technique might not handle all types of attacks or scale to larger, more diverse networks.

5. **Hady et al. (2020):** This solution, which combines medical and network data, provides enhanced detection for healthcare systems but is limited to specific types of attacks (MITM) and may not be as effective against more complex or novel attack strategies.

Each of these studies presents novel approaches to enhancing IoMT security but also highlights challenges related to scalability, model generalization, and real-world applicability across diverse environments and attack types.

RECOMMENDATION

For those working in the field of real-time vulnerability detection and control models for electronic healthcare medical cyber-physical systems (CPS) using deep neural network (DNN) techniques, the following recommendations can help enhance the effectiveness and applicability of these models:

1. **Address Computational Efficiency**: While DNNs offer powerful detection capabilities, they often come with significant computational overhead (Ebere et al., 2025). Researchers should focus on optimizing DNN models for resource-constrained environments, such as using model compression, pruning, or lightweight neural networks to ensure they can run efficiently on IoMT devices.

2. **Ensure Data Privacy and Security**: Given the sensitive nature of healthcare data, it's crucial to incorporate privacy-preserving techniques like federated learning or differential privacy when implementing DNN models. This will help protect patient data while still enabling effective detection and control of vulnerabilities.

3. **Focus on Real-Time Adaptability**: IoMT devices and medical systems are highly dynamic, with new vulnerabilities emerging frequently. Models should be continuously trained and adapted to detect new threats. Techniques such as online learning or incremental training should be explored to allow for real-time updates without requiring full retraining.

4. **Improve Explainability**: Deep learning models are often viewed as black-box systems, which can make it difficult to understand their decision-making process. Incorporating Explainable AI (XAI) techniques can help make the model's predictions more transparent, increasing trust and helping healthcare professionals better interpret and respond to detected vulnerabilities.

5. **Enhance Collaboration with Healthcare Professionals**: Collaboration between cybersecurity experts and healthcare professionals is key. By understanding the specific needs and constraints of the healthcare environment, solutions can be better tailored to provide practical, actionable security measures that do not disrupt patient care or medical workflows.

6. **Focus on Integration Across Layers**: Real-time vulnerability detection should not be confined to individual devices or networks but should span across all layers of the healthcare CPS. Models should be designed to provide integrated protection, from the device level to the cloud and network layers, ensuring comprehensive security.

7. **Consider Regulatory Compliance**: When developing and deploying security models in healthcare settings, ensure that all solutions comply with industry standards and regulations like HIPAA (Health Insurance Portability and Accountability Act). This will help avoid legal and ethical issues while implementing security measures.

8. **Conduct Extensive Testing and Validation**: Models should be rigorously tested across a variety of real-world scenarios and datasets to ensure they can handle different types of attacks and operational conditions. Simulating a range of cyber-attacks and evaluating the model's performance can help uncover weaknesses and areas for improvement.

By following these recommendations, researchers and practitioners can contribute to building more secure, efficient, and adaptable real-time vulnerability detection systems that significantly enhance the protection of electronic healthcare CPS.

CONCLUSION

In conclusion, vulnerability management in Cyber-Physical Systems (CPS) is a critical aspect of ensuring the security and resilience of these increasingly interconnected systems. The complexity of CPS, which integrates both physical and cyber elements, presents significant challenges in identifying and mitigating vulnerabilities effectively. While traditional vulnerability management methods provide a foundation, they are often insufficient to handle the dynamic and multi-faceted nature of CPS environments.

The integration of Deep Neural Networks (DNNs) into vulnerability management offers a promising solution by enabling more accurate, scalable, and adaptive detection of vulnerabilities. DNNs excel in recognizing complex patterns and anomalies in large, high-dimensional datasets, making them well-suited to the complex data streams inherent in CPS. However, as evidenced in the review, there are still notable gaps in the application of DNNs, particularly around real-time detection, scalability to large-scale systems, and the interpretability of models.

Future research should focus on refining DNN-based approaches to address these limitations. Advancements in techniques such as explainable AI, transfer learning, and federated learning could enhance the interpretability and scalability of models, enabling more robust and proactive security measures in CPS. Furthermore, developing adaptive systems that can continuously learn from evolving threats and environments will be key to maintaining the security of CPS in the long term.

Ultimately, the future direction of vulnerability management in CPS should be focused on creating more intelligent, real-time, and automated systems that can proactively address emerging threats. By harnessing the power of DNNs and other advanced machine learning techniques, we can create a more resilient framework for securing the critical infrastructures that are vital to modern society.

REFERENCES

1. Al-Shaher, A., Abdul-Kader, R., & Al-Salman, R. (2017). Intelligent healthcare security system for IoMT: An integrated approach. Journal of Cyber Security Technology, 1(3), 150-161.
2. Ayoub S.A., &NarhimeneB., (2023). Machine learning for transmission level security in IoMT systems. International Journal of Computer Science and Network Security, 23(4), 45-55.https://doi.org/10.1016/j.asoc.2023.110227
3. Bin, F., & Li, D. (2023). Machine learning for vulnerability detection and classification in IoT security. IEEE Transactions on Industrial Informatics, 19(2), 887-896.https://doi.org/10.3390/electronics12183927
4. Ebere Uzoka Chidi, E Anoliefo, C Udanor, AT Chijindu, LO Nwobodo (2025)" A Blind navigation guide model for obstacle avoidance using distance vision estimation based YOLO-V8n; Journal of the Nigerian Society of Physical Sciences, 2292-229; https://doi.org/10.46481/jnsps.2025.2292
5. Eneh P.C, Ene I.I., Egoigwe V.S. Ebere U.C. (2019). Deep Artificial Neural Network Based Obstacle Detection and Avoidance for a Holonomic Mobile Robot. International Research Journal of Applied Sciences, Engineering and Technology Vol.5, No.1; ISSN (1573-1405); p –ISSN 0920-5691

6. Eze E.M., Ituma C., Asogwa T.C., Ebere U.C. (2022). Development of Machine Learning Based Security Algorithm for 4G Network against Wormhole; International Journal of Research and Innovation in Applied Science (IJRIA) Vol 7; Issues 2; pp 70-75
7. Gao, J., &Thamilarasu, R. (2017). Detection of attacks on medical devices using machine learning. International Journal of Medical Informatics, 112, 16-24.
8. Gupta, A., Sharma, S., & Bansal, V. (2022). Attack detection in multi-cloud healthcare systems using deep hierarchical stacked neural networks. Journal of Healthcare Engineering, 2022, 1-10.
9. Hameed, F., Ali, S., &Khusro, M. (2022). Weighted Hoeffding Tree Ensemble for industrial IoMT. Proceedings of the International Conference on Internet of Things and Big Data, 2022, 132-140.
10. He, H., Zhang, W., & Li, Z. (2019). Anomaly detection in connected healthcare systems using stacked autoencoders. Journal of Computational Biology, 26(8), 787-799.
11. Jeon, M., & Kim, S. (2021). AutoVAS: Automated vulnerability analysis system using deep learning. Proceedings of the 2021 International Conference on Cybersecurity and Machine Learning, 102-110.https://doi.org/10.1016/j.cose.2021.102308
12. Kekong P.E, Ajah I.A., Ebere U.C. (2019). Real-time drowsy driver monitoring and detection system using deep learning based behavioural approach. International Journal of Computer Sciences and Engineering 9 (1), 11-21
13. Khan, M., &Akhunzada, A. (2021). Deep learning for malware detection in IoMT. Journal of IoT and Security, 15(3), 315-324.
14. Kumar, S., Sharma, V., &Vashisth, A. (2021). Intrusion detection system using ensemble learning and fog-cloud architecture in IoMT. International Journal of Advanced Computer Science and Applications, 12(8), 1-10.
15. Lee, S., Kim, J., & Park, S. (2021). Multi-class classification for healthcare IoT using convolutional neural networks. IEEE Access, 9, 455-463.
16. Martinsen, K., Lee, J., & Thompson, P. (2022). Robustness and vulnerability measurement of deep learning models for cyber defense. Cybersecurity, 8(4), 202-210.
17. Odo F.E., Ituma C., Asogwa T.C.., Ebere U.C. (2022). Development of an Intelligent Fire Hazard Detection System Using Enhanced Machine Learning Technique. International Journal of Research and Innovation in Applied (IJRIAS) 7 (3); pp. 56-62.
18. Sakr, S., &Elgammal A., (2016). Towards a Comprehensive Data Analytics Framework for Smart Healthcare Services. https://doi.org/10.1016/j.bdr.2016.05.002
19. Salemi, B., &Azizi, S. (2021). Predicting DDoS attacks in healthcare systems using deep learning and time-series data. Computational Intelligence and Neuroscience, 2021, 1-10.
20. Singh, A., Soni, D., & Choudhury, A. (2022). Hierarchical Federated Learning for intrusion detection in IoMT networks. Journal of Machine Learning for Healthcare, 5(2), 48-56.
21. Snehi M., & Bhandari (2021) Vulnerability retrospection of security solutions for software-defined Cyber–Physical System against DDoS and IoT-DDoS attacks. https://doi.org/10.1016/j.cosrev.2021.100371
22. Sochima V.E. Asogwa T.C., Lois O.N. Onuigbo C.M., Frank E.O., Ozor G.O., Ebere U.C. (2025)"; Comparing multi-control algorithms for complex nonlinear system: An embedded programmable logic control application;DOI: http://doi.org/10.11591/ijpeds.v16.i1.pp212-224
23. Thamilarasu, R., &Odesile, O. (2017). Mobile agents for penetration testing and securing medical device networks. Journal of Network Security, 19(7), 712-724.