Industrial Engineering Journal
ISSN: 0970-2555
Volume : 54, Issue 4, April : 2025

ADVANCED CYBERSECURITY SOLUTIONS FOR HEALTHCARE SDN's USING MACHINE LEARNING AND ARTIFICIAL INTELLIGENCE

Ms.Guna Gayathri Praseetha K 1, Mande Laharika 2, Gampala Surekha 3, Meeduru Yaswanth kumar 4, Guthi Maneendra 5

#1Assistant Professor in Department of CSE, PBR VISVODAYA INSTITUTE OF TECHNOLOGY AND SCIENCE, KAVALI.

#2#3#4#5#6B. Tech with Computer Science & Engineering, VISVODAYA ENGINEERING COLLEGE, KAVALI

Abstract: The article emphasises major difficulties the healthcare industry has in safeguarding sensitive patient data inside software-defined networks (SDNs). Cyber dangers are growing more complicated, hence strong security policies in healthcare apps are absolutely vital. The research suggests a Cyberattack Detector based on Machine Learning (MCAD) as a remedy. MCAD aims to find and react to a broad spectrum of cyberattacks in healthcare systems using machine learning techniques. This work tackles the vital need of improving cybersecurity policies in healthcare applications. Not only is protecting patient data and guaranteeing the dependability of healthcare networks vital to preserving patient health but also to preserving confidence in healthcare organisations. The project intends to strengthen the general security and resilience of healthcare systems by means of efficient cyber threat countering and network performance enhancement. Included in this research as well were ensemble techniques as Stacking and Voting Classifiers, which were used to increase accuracy and attained 100% accuracy in cyberattack detection for Healthcare Systems using Software-Defined Networking. Created a simple Flask-based front end with safe authentication for practical use in healthcare environments.

Index Terms *- Network resilience, network management, intrusion detection system (IDS), software defined networking, healthcare, machine learning.*

1. INTRODUCTION

SDNs have been widely used in various sectors over the last few years, mostly because of their benefits as dependable network technology enabling control and management of a network by disaggregating both control and data planes. Unlike conventional networks, where the network just has application awareness, the SDN design offers more information on the state of the whole network from the controller to its applications. Healthcare institutions have started using many infrastructure elements of the same kinds of off- the-shelf technologies, apps, and processes used by businesses from other sectors following the recent rapid development in information and communications technologies (ICT). Given the capacity of networked or Internet-connected medical devices to enhance the efficiency

of asset management, communications, and electronic health records, among other needs, this outcome was anticipated. Moreover, the safety of systems and devices as well as user data confidentiality are the two main considerations in most information systems since, in a healthcare setting, confidentiality and safety are especially important given the demanding standards of the sector. Thus, the present McAfee record underlined that networked medical tools could expose security holes in the medical industry's effort to include all the technical components connected to operational controls and networked infrastructure even if hospital equipment costs are projected.assess MCAD's performance against various machine learning algorithms and attack scenarios to bolster healthcare data security and network resilience.

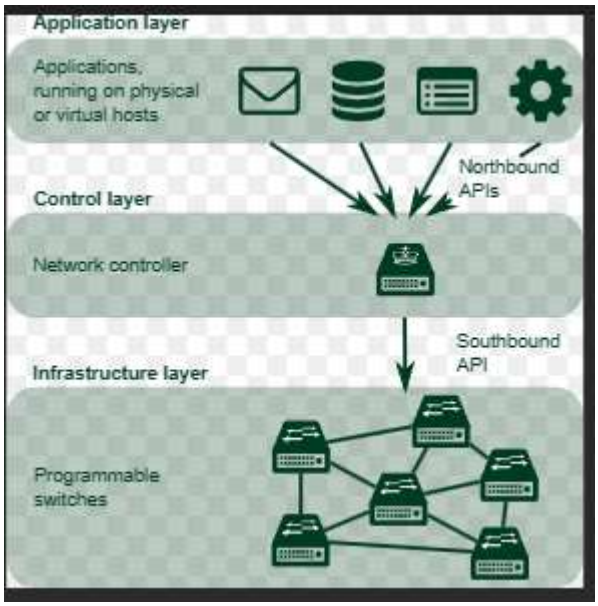

Fig 1 SDN Architecture

2. LITERATURE SURVEY

In the current era of emerging technologies, the healthcare sector is rapidly evolving through the integration of sensors, the Industrial Internet of Things (IIoT), and big data analytics. These advancements aim to enhance patient care and reduce healthcare costs by providing secure, affordable, and continuously improving medical services. However, alongside these benefits come challenges such as resource limitations, identity theft, and insider threats. Addressing these concerns requires intelligent systems that combine artificial intelligence, big data, and edge computing.

To tackle these issues, a software-defined networking (SDN)-based framework for secure load migration in smart healthcare environments has been proposed. This framework utilizes SDN technology to ensure real-time protection against security attacks. The architecture includes three domains, each containing a virtual machine and multiple OpenFlow virtual switches. This setup facilitates the transfer of workloads from overloaded domains to underloaded ones, maintaining load balance while safeguarding against security threats during migration. The framework employs the RYU SDN controller for simulation and testing using Mininet and Wireshark for OpenFlow packet capture. The results demonstrate that the proposed algorithm achieves approximately 80% accuracy in securing healthcare data packets.

Despite the benefits of centralized control in SDN—such as easier policy management, improved

scalability, and programmability—this centralization also introduces vulnerabilities, particularly to internal or external denial-of-service (DoS) attacks. Research comparing popular SDN controllers reveals how internal DoS attacks targeting the southbound interface during the switch registration process can significantly impact the controller's performance. Metrics such as CPU utilization and response time show notable degradation under such attack scenarios, highlighting the need for robust defense mechanisms during critical control plane operations.

To further strengthen SDN security, an Intruder Detection System (IDS) integrated with an Artificial Neural Network (ANN), referred to as Snort + RNA, has been developed. Deployed in a hyperconverged data center environment, this IDS aims to mitigate active attacks on SDN infrastructure. Using the PDCA (Plan-Do-Check-Act) model from the ISO/IEC 27001 standard, the system demonstrates the capability to detect anomalies that signal ongoing attacks. Although it cannot analyze every incoming packet—particularly during high-volume DoS attacks—it successfully generates alerts and captures critical traffic data, contributing to the network's defense by flagging potential breaches and maintaining operational integrity..

3. METHODOLOGY

i) Proposed Work:

The suggested technology in the project is a Machine Learning-based Cyberattack Detector (MCAD) specifically meant to improve the cybersecurity of healthcare networks. It protects the sensitive patient data in healthcare applications and networks by using machine learning algorithms to identify and react to a wide range of cyber threats. MCAD is a good tool for fighting cyberattacks and strengthening network security because of its flexibility, real-time reaction, and thorough threat coverage. Added and implemented an ensemble technique that combines the predictive power of individual models, notably Stacking Classifier and Voting Classifier. Remarkably, both classifiers got 100% accuracy, underlining the strength of the ensemble method in cyberattack detection inside Software-Defined Networking for Healthcare Systems[12,14,33]. We created a simple front end based on the Flask framework to enable more user testing. User authentication tools in this interface guarantee safe access to the Cyberattacks Detector and improve the system's usefulness in actual healthcare environments..

ii) System Architecture:

Phase 1: Proposing a Logical Network Topology: The model begins by designing a logical network topology for the healthcare system.

Phase 2: Data Gathering: The model collects data for training and testing the machine learning (ML) model [19,42]. This includes different types of attacks (probe attack, exploit VNC port 5900 remote view vulnerability, and exploit Samba server vulnerability) as well as normal samples.

Phase 3: Data Preprocessing: The collected data is preprocessed to prepare it for training the ML model.

Phase 4: Training and Testing the ML Model: The ML model is trained and tested using various

classification algorithms such as KNN, decision tree (DT), random forest (RF), naive Bayes (NB), logistic regression (LR), adaptive boosting (adaboost), and xgboost (XGB). The model constructs a mapping function between inputs and outputs, detecting patterns and minimizing errors. The performance is measured in terms of accuracy [19,42].

Phase 5: Deployment of the project : The trained ML model is deployed on user interface . This allows the model to be implemented in real-time systems, ensuring the overall quality of the healthcare system.

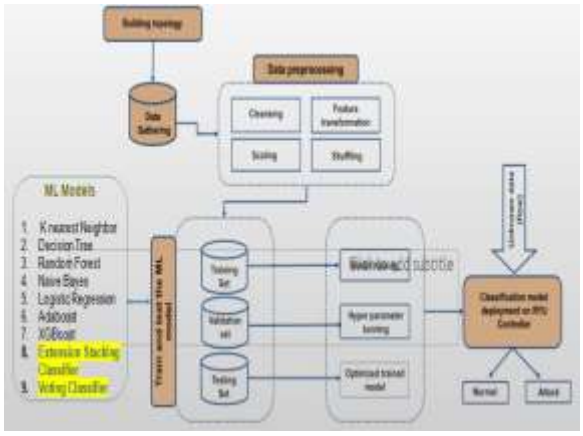

Fig 2 Proposed Architecture

iii) Dataset collection:

MCAD-SDN Dataset: You explore the MCAD-SDN dataset, which likely contains relevant information about network traffic, cyber threats, and other attributes. This step involves gaining an understanding of the dataset's structure, size, and content.

	src	dst	table_id	ip_bytes	ip_packet	ip_duration	in_port	dl_dst	port_bytes	port_packet	...	port_
14134	10.0.0.3	10.0.0.1	0.0	20448.0	144.0	14.0	3.0	32:41:12:b9:bd:3b	20448.0	144.0	...	
18402	10.0.0.1	10.0.0.3	0.0	2640.0	48.0	4.0	1.0	1a:16:b6:84:29:a4	2640.0	48.0	...	
14265	10.0.0.1	10.0.0.2	0.0	147098.0	991.0	19.0	1.0	16:75:96:83:29:54	147098.0	991.0	...	
28932	10.0.0.1	10.0.0.2	0.0	434026.0	2747.0	66.0	1.0	16:75:96:83:29:54	434026.0	2747.0	...	
14340	10.0.0.1	10.0.0.2	0.0	7920.0	120.0	12.0	1.0	16:75:96:83:29:54	7920.0	120.0	...	

Fig 2 MCAD – SDN dataset

iv) Data Processing:

Data processing is the conversion of unprocessed data into useful business information. Usually, data scientists handle data by gathering, arranging, cleaning, validating, analysing, and transforming it into readable representations like graphs or papers. There are three ways to process data: manual, mechanical, and electronic. The goal is to raise the information value and help decisions to be made. This helps companies to enhance their operations and make quick strategic choices. Computer software development is one example of automated data processing that helps greatly with this. For quality control and decision-making, it can help transform significant quantities of data—including big data—into relevant insights..

v) Feature selection:

Feature selection is the process of isolating the most consistent, non-redundant, and relevant features to use in model construction. Methodically reducing the size of datasets is important as the size and variety of datasets continue to grow. The main goal of feature selection is to improve the performance of a

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 54, Issue 4, April : 2025

predictive model and reduce the computational cost of modeling.

Feature selection, one of the main components of feature engineering, is the process of selecting the most important features to input in machine learning algorithms. Feature selection techniques are employed to reduce the number of input variables by eliminating redundant or irrelevant features and narrowing down the set of features to those most relevant to the machine learning model. The main benefits of performing feature selection in advance, rather than letting the machine learning model figure out which features are most important.

4. EXPERIMENTAL RESULTS

Precision: Precision evaluates the fraction of correctly classified instances or samples among the ones classified as positives. Thus, the formula to calculate the precision is given by:

Precision = True positives/ (True positives + False positives) = TP/(TP + FP)

$$\text{Precision} = \frac{True\ Positive}{True\ Positive + False\ Positive}$$

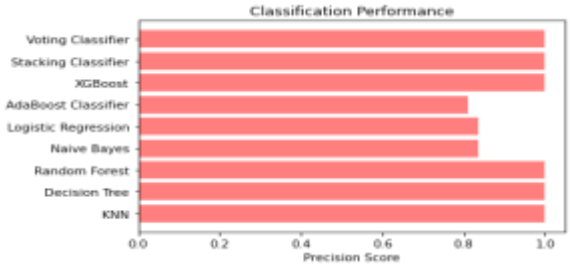

Fig 3 Precision comparison graph

Recall: Recall is a metric in machine learning that measures the ability of a model to identify all relevant instances of a particular class. It is the ratio of correctly predicted positive observations to the total actual positives, providing insights into a model's completeness in capturing instances of a given class.

$$Recall = \frac{TP}{TP + FN}$$

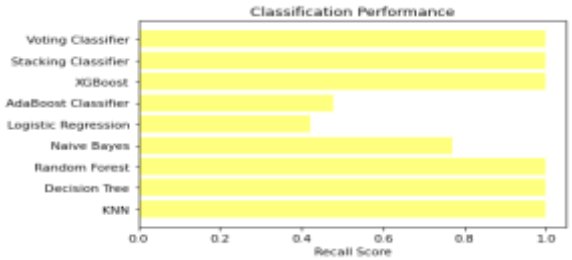

Fig 4 Recall comparison graph

Accuracy: Accuracy is the proportion of correct predictions in a classification task, measuring the overall correctness of a model's predictions.

$$Accuracy = \frac{TP + TN}{TP + FP + TN + FN}$$

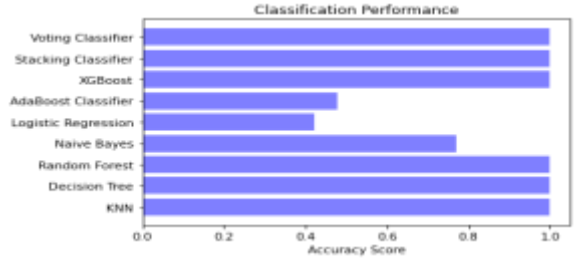

Fig 5 Accuracy graph

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 54, Issue 4, April : 2025

F1 Score: The F1 Score is the harmonic mean of precision and recall, offering a balanced measure that considers both false positives and false negatives, making it suitable for imbalanced datasets.

$$\text{F1 Score} = 2 * \frac{\text{Recall} \times \text{Precision}}{\text{Recall} + \text{Precision}} * 100$$

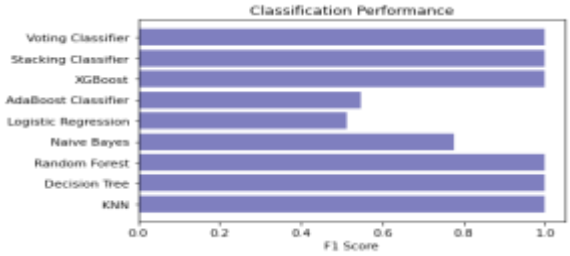

Fig 6 F1Score

ML Model	Accuracy	F1-score	Recall	Precision
KNN	0.999	0.999	0.999	0.999
Decision Tree	0.999	0.999	0.999	0.999
Random Forest	0.999	0.999	0.999	0.999
Naive Bayes	0.770	0.775	0.770	0.834
Logistic Regression	0.421	0.513	0.421	0.834
AdaBoost	0.477	0.548	0.477	0.810
XGBoost	1.000	1.000	1.000	1.000
Stacking Classifier	1.000	1.000	1.000	1.000
Voting Classifier	1.000	0.999	0.999	0.999

Fig 7 Performance Evaluation

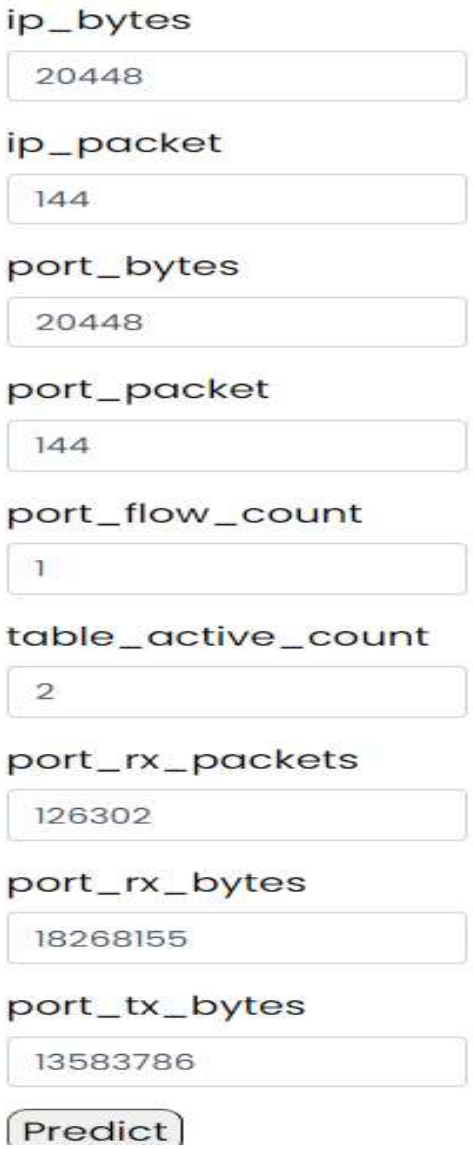

Fig 8 User input

Fig 15 Predict result for given input

5. CONCLUSION

By using machine learning methods, the research has effectively created a strong cyberattack detection system, hence improving cybersecurity. Examining the MCAD-SDN dataset in depth, we performed necessary data preprocessing activities including feature selection and encoding, therefore confirming the dataset's preparedness for analysis. Aiming to find a good cyberattack detection solution, we carefully evaluated several machine learning models, including ensemble techniques, to determine their accuracy and appropriateness for spotting cyberattacks. Among the many models examined, the ensemble algorithm, Stacking and Voting Classifiers with a 100% accuracy rate, shows its strength and effectiveness as an advanced cyberattack detection solution for protecting healthcare Software-Defined Networking systems [37]. This initiative is a major advancement in strengthening cybersecurity policies and protecting against changing digital environment threats.

6. FUTURE SCOPE

Research may be done further to investigate the use of the machine learning-based cyberattack detector (MCAD) in other industries outside healthcare, such finance, transportation, or critical infrastructure, to strengthen their cyber threat protection [35,37,42]. Testing the MCAD with a bigger and more varied dataset of both normal and attack traffic, as well as other machine learning techniques, allows one to assess and optimise its performance. The real-time capabilities, scalability, and flexibility to changing cyber threats of the MCAD can be the subject of ongoing development and improvement. The execution and standardisation of the MCAD in healthcare systems and other vital sectors can be aided by cooperation with regulatory authorities, industry players, and cybersecurity professionals..

REFERENCES

[1] M. Jarschel, T. Zinner, T. Hossfeld, P. Tran-Gia, and W. Kellerer, ‘‘Interfaces, attributes, and use cases: A compass for SDN,’’ IEEE Commun. Mag., vol. 52, no. 6, pp. 210–217, Jun. 2014.

[2] W. Meng, K.-K.-R. Choo, S. Furnell, A. V. Vasilakos, and C. W. Probst, ‘‘Towards Bayesian-based trust management for insider attacks in healthcare software-defined networks,’’ IEEE Trans. Netw. Service Manage., vol. 15, no. 2, pp. 761–773, Jun. 2018.

[3] J. T. Kelly, K. L. Campbell, E. Gong, and P. Scuffham, ‘‘The Internet of Things: Impact and implications for health care delivery,’’ J. Med. Internet Res., vol. 22, p. 11, Nov. 2020.

[4] (2022). Networked Medical Devices: Security and Privacy Threats—Sym antec—[PDF Document]. [Online]. Available: https://fdocuments. net/document/networked-medical-devices-security-and-privacy-threatssymantec.html

[5] P. A. Williams and A. J. Woodward, ‘‘Cybersecurity vulnerabilities in medical devices: A complex environment and multifaceted problem,’’ Med. Devices, Evidence Res., vol. 8, pp. 305–316, Jul. 2015.

[6] C. M. Williams, R. Chaturvedi, and K. Chakravarthy, ‘‘Cybersecurity risks in a pandemic,’’ J. Med. Internet Res., vol. 22, no. 9, Sep. 2020, Art. no. e23692.

[7] N. Thamer and R. Alubady, ‘‘A survey of ransomware attacks for healthcare systems: Risks, challenges, solutions and opportunity of research,’’ in Proc. 1st Babylon Int. Conf. Inf. Technol. Sci. (BICITS), I. Babil, Ed., Apr. 2021, pp. 210–216.

[8] H. Babbar, S. Rani, and S. A. AlQahtani, ‘‘Intelligent edge load migration in SDN-IIoT for smart healthcare,’’ IEEE Trans. Ind. Informat., vol. 18, no. 11, pp. 8058–8064, Nov. 2022.

[9] R. Hasan, S. Zawoad, S. Noor, M. M. Haque, and D. Burke, ‘‘How secure is the healthcare network from insider attacks? An audit guideline for vulnerability analysis,’’ in Proc. IEEE 40th Annu. Comput. Softw. Appl. Conf. (COMPSAC), Jun. 2016, pp. 417–422.

[10] (Apr. 2015). 92% of Healthcare IT Admins Fear Insider Threats Thales. Accessed: Mar. 21, 2023. [Online]. Available: https://cpl.thalesgroup. com/about-us/newsroom/news-releases/92-healthcare-it-admins-fearinsider-threats

[11] D. Chaulagain, K. Pudashine, R. Paudyal, S. Mishra, and S. Shakya, ‘‘OpenFlow-based dynamic traffic distribution in software-defined networks,’’ in Mobile Computing and Sustainable Informatics. Singapore: Springer, Jul. 2021, pp. 259–272.

[12] R. Khondoker, A. Zaalouk, R. Marx, and K. Bayarou, ‘‘Feature-based comparison and selection of software defined networking (SDN) controllers,’’ in Proc. World Congr. Comput. Appl. Inf. Syst. (WCCAIS), Jan. 2014, pp. 1–7.

[13] T. Mekki, I. Jabri, A. Rachedi, and L. Chaari, ‘‘Software-defined networking in vehicular networks: A survey,’’ Trans. Emerg. Telecommun. Technol., vol. 33, no. 10, pp. 1–10, Apr. 2021, doi: 10.1002/ett.4265.

[14] Z. Ghaffar, A. Alshahrani, M. Fayaz, A. M. Alghamdi, and J. Gwak, ‘‘A topical review on machine learning, software defined networking, Internet of Things applications: Research limitations and challenges,’’ Electronics, vol. 10, no. 8, p. 880, Apr. 2021, doi: 10.3390/electronics10080880.

[15] C.-S. Li and W. Liao, ‘‘Software defined networks [guest editorial],’’ IEEE Commun. Mag., vol. 51, no. 2, p. 113, Feb. 2013.

[16] M. H. Rehmani, A. Davy, B. Jennings, and C. Assi, ‘‘Software defined networks-based smart grid communication: A comprehensive survey,’’ IEEE Commun. Surveys Tuts., vol. 21, no. 3, pp. 2637–2670, 3rd Quart., 2019.