OPEN ACCESS JOURNALS
Indiana Journal of Multidisciplinary Research
Abbriviate Tittle- Ind J Multi Res
ISSN *(Online)*- 2583-3820
Journal Homepage Link- https://indianapublications.com/Journals/IJMR
DOI: https://doi.org/10.5281/zenodo.12679904

INDIANA PUBLICATIONS
PRODUCTIVE AND QUALITY RESEARCH

Research Article

Volume-04|Issue-03|2024

MCAD: A Machine Learning Based Cyberattacks Detector in Software-Defined Networking (SDN)

Varun P[1], G Dharani[2], Raja Yogeshwaran[3], Varshith Veerabomma*[4], Dr. Shruthi P[5]

[1,2,3.4,5] Information Science & Engineering, RV Institute of Technology & Management, Visvesvaraya Technological University, India

Article History
Received: 20.05.2024
Accepted: 05.06.2024
Published: 30.06.2024

Citation
Varun, P., Dharani, G., Yogeshwaran, R., Veerabomma, V., & Shruthi, P. (2024). MCAD: A Machine Learning Based Cyberattacks Detector in Software-Defined Networking (SDN). *Indiana Journal of Multidisciplinary Research*, *4*(3), 212-217.

Abstract: The safeguarding of sensitive patient data within healthcare systems is a top priority in the face of escalating cyber threats. This research introduces MCAD, a cutting-edge solution designed to protect healthcare data within Software-Defined Networks (SDNs). SDNs, while flexible, are susceptible to intrusions that can disrupt network performance and endanger patient safety. MCAD addresses this vulnerability by leveraging machine learning techniques to analyze network traffic and detect both known and emerging cyber-attacks. By modifying an L3 learning switch application, it establishes a baseline of normal network behavior and proactively identifies deviations that may indicate malicious activity. Through rigorous evaluation using various machine learning algorithms and simulated attack scenarios, MCAD demonstrates its effectiveness in proactively mitigating cyber threats. Results highlight its robust F1-score in accurately differentiating between normal and malicious traffic patterns. This research strengthens the security of healthcare systems, ensuring the protection of critical patient data against constantly evolvingcyber threats.

Keywords: Machine learning, network management, intrusion detection system (IDS), software defined networking.

Copyright © 2024 The Author(s): This is an open-access article distributed under the terms of the Creative Commons Attribution 4.0 International License (**CC BY-NC 4.0**).

INTRODUCTION

Software-Defined Networks (SDNs) have revolutionized network management, offering flexibility, centralized control, and enhanced visibility. Their adoption in healthcare systems streamlines asset management and communication, leading to potential cost savings and improved patient care.

However, the integration of networked medical devices introduces significant security vulnerabilities. This is especially concerning in light of the escalating frequency of cyberattacks during the COVID-19 pandemic. These attacks pose a grave risk to the integrity and availability of critical healthcare systems.

To combat these evolving threats, and propose MCAD, a cutting-edge, low- complexity solution tailored for safeguarding healthcare SDNs.

MCAD employs machine learning techniques to proactively identify and mitigate a wide range of cyberattacks. By analyzing network traffic patterns, it learns to distinguish between normal behavior and malicious activity.

Research explores the development, methodology, and rigorous experimental evaluation of MCAD, demonstrating its effectiveness in protecting healthcare networks against both known and emerging threats.

PROBLEM STATEMENT

Developing an innovative cyber security solution tailored for healthcare networks, specifically focusing on real-time heart monitoring systems, to proactively mitigate threats, protect patient data confidentiality, and ensure seamless remote patient care.

EXISTING SYSTEM

Recent developments in IoT-enabled heart monitoring devices harness the benefits of cloud computing for streamlined data collection, visualization, storage, and remote analysis. This integration often involves fog computing and Software-Defined Networking (SDN) principles to optimize performance. Thorough evaluations on medical data and sensor readings demonstrate the potential of these systems to revolutionize patient care while reducing healthcare costs.

However, the cloud-centric approach in many existing IoT-enabled heart monitoring systems can lead to latency, interoperability issues, and increased cybersecurity risks. There's a need to shift some of the intelligence and decision-making closer to the data source. This is where MCAD can excel.

By embedding machine learning algorithms directly within the SDN, MCAD can proactively detect anomalies indicative of cyberattacks, even without constant reliance on a remote cloud connection. This

***Corresponding Author:** Varshith Veerabomma

approach aims to minimize latency, strengthen security, and preserve the privacy of sensitive healthcare data.

Further research is crucial to address the shortcomings identified in related works [1,2]. Integrating robust security mechanisms into IoT devices themselves is essential to counter identity theft, insider attacks, and threats stemming from the use of Big Data and AI in healthcare. Similarly, while intrusion detection systems (IDS) offer promise, their adaptation within the complex and dynamic IoT landscape requires specialized solutions to address the ever-evolving nature of cyberattacks.

PROPOSED SYSTEM

To implement MCAD, Cybersecurity solution specifically designed for healthcare SDNs, Therefore outlining a comprehensive five-phase strategy. Initially, established the logical network topology by configuring network adapters and Open vSwitch (OVS) bridges.This careful configuration ensures seamless communication between machines, creating the foundation for comprehensive network monitoring and analysis.

Data preprocessing is the next crucial phase. This involves meticulous data cleansing, feature transformation, data scaling, and data shuffling. These steps prepare the dataset for optimal use by the machine learning algorithms, ensuring accuracy and efficiency during the learning process.

The heart of MCAD lies in its adaptive learning and model selection phase. The solution employs a diverse suite of machine learning algorithms, including K-Nearest Neighbors (KNN), Decision Tree (DT), Random Forest (RF), Naïve Bayes (NB), Logistic Regression (LR), Adaptive Boosting (AdaBoost), and XGBoost (XGB).

Each algorithm offers unique strengths, allowing MCAD to robustly detect complex cyberattack patterns. Once a suitable model is selected, it's seamlessly deployed on the Ryu controller. This integration empowers MCAD to analyze network traffic in real-time, classifying it as normal or malicious, and taking appropriate mitigative actions to enhance Key Performance Indicators (KPIs).

Finally, MCAD prioritizes continuous monitoring and evaluation. Stringent testing and validation throughout its lifecycle ensure the system remains effective against evolving threats. Its most powerful feature lies in its ability to continuously learn from new data and attack patterns, maintaining its effectiveness in a dynamic cyber threat landscape.

LITERATURE REVIEW

The integration of emerging technologies in healthcare has led to the rise of smart healthcare solutions, leveraging sensors, Industrial Internet of Things (IIoT), and big data analytics to improve patient care while reducing costs. However, challenges such as resource constraints and security threats necessitate robust solutions.Proposed solution involves software-defined networking (SDN)-based security compliance structures for smart healthcare load migration systems. By employing SDN-IIoT technology, researchers aim to enhance real-time protection against security attacks.

A proposed framework involves multiple domains, each equipped with virtual machines and OpenFlow virtual switches, facilitating the migration of healthcare data to balance loadsand mitigate security risks.Furthermore, studies focus on the effects of internal denial-of-service (DOS) attacks on SDN controllers during switch registration. While SDNsoffer benefits like centralized control and improved security, they are susceptible to DOS attacks.Analyzing the impact of such attacks on CPU utilization and controller response time helps in understanding vulnerabilities and devising countermeasures.

Additionally, there are efforts to integrate intrusion detection systems (IDS) into SDNs using artificial neural networks (ANN) to mitigate active computer attacks on SDNs. By detecting anomalies and analyzing network traffic, these systems enhance the security of SDNs, albeit with some limitations.Furthermore, a survey explores the integration of IDS in IoT networks to ensure secure communication among devices. With cyberattacks becoming more complex, integrating IDS becomes crucial for safeguarding IoT-based devices.

Finally, the deployment of intrusion detection systems in wireless environments, such as Wireless Sensor Networks (WSN), Mobile Ad Hoc Networks (MANET), and IoT, presents unique challenges. Addressing these challenges involves adopting traditional wired intrusion detection methods and developing specific techniques tailored to wireless networks.

Overall, these studies highlight the importance of leveraging advanced technologies like SDN, AI, and IDS to enhance the security and efficiency of healthcare and IoT networks while addressing evolving challenges.

1. Focuses on analyzing Denial-of-Service (DoS) attacks in T-S fuzzy networked control systems by transforming performance error estimation into ellipsoid constraints. The approach involves constructing improved Lyapunov-Krasovskii functions with fuzzy membership functions, introducing a second-order weight method, and establishing an integral elastic event trigger mechanism. However, this method might introduce computational complexity and may not be universally applicable to all network security scenarios.

***Corresponding Author:** Varshith Veerabomma

2. Involves creating datasets from SDN using Mininet and Ryu controller, including normal traffic and various attack types. Feature extraction tools are applied, and supervised binary classification machine learning algorithms like decision trees are trained for real-time attack classification. However, the effectiveness may depend on dataset accuracy and completeness, and implementing machine learning algorithms may require significant computational resources and expertise.
3. Focuses on probe attack detection in SDN using the Grey-wolf optimizer (GWO) for feature selection and Light Gradient Boosting Machine (LightGBM) classifier. The InSDN dataset is used for training and testing, serving as a benchmarking dataset in SDN for intrusion detection. However, implementing machine learning algorithms like LightGBM may require significant computational resources, limiting accessibility in resource-constrained environments.
4. Explores using SDN combined with IIoT for securing smart healthcare load migration systems. SDN technology, along with the RYU SDN controller, is employed for real-time security protection and performance evaluation. However, the effectiveness of the system may be limited in larger-scale healthcare networks, and implementing SDN and IIoT technologies may require substantial resources and infrastructure.
5. Compares two SDN controllers and assesses the impact of internal denial-of-service attacks during switch registration. The study focuses on internal denial-of-service attacks, potentially overlooking other vulnerabilities. Findings may not be universally applicable to all SDN controllers or network configurations.
6. Implements an Intruder Detection System (IDS) integrated into an Artificial Neural Network (ANN) to mitigate active computer attacks on SDN. The study follows the PDCA model from ISO/IEC 27001. However, the system's inability to analyze all packets may leave some vulnerabilities unaddressed, and the study may not account for variations in network configurations or attack types.
7. Conducts a systematic literature review to investigate IoT and IDS integration. It examines threat models, challenges, proposed models, and implementations. However, the study lacks empirical data or real-world implementation insights and may not cover all possible IoT network scenarios and challenges.
8. Conducts a comprehensive survey to investigate complexities and challenges of deploying IDS for wireless IoT devices. The study primarily relies on literature review and analysis, potentially lacking real-world implementation insights and coverage of all wireless IoT network scenarios and challenges.
9. Employs a quantitative threat model to assess cyberattacks on a specific protocol using ML and SDN technologies for intrusion detection and automated mitigation. However, the study may not cover broader healthcare IoT security challenges and relies on analysis and simulation for evaluation.
10. Uses an ML model to calculate dynamic threshold limits for DDoS attack detection in real-time. The effectiveness heavily relies on the accuracy of the ML model, which may require continuous tuning. Implementing a dynamic threshold system based on ML may introduce complexity and resource overhead, potentially impacting SDN performance.

METHODOLOGY

Approach draws inspiration from advancements in IoT-enabled heart monitoring systems, harnessing cloud computing for efficient data management and remote analysis. Recognizing the limitations of cloud-centric solutions, And propose Adaptive -shield machine learning defence for healthcare SDN's a solution designed specifically to strengthen the security of healthcare systems.

MCAD prioritizes the protection of sensitive patient data and healthcare infrastructure. It uses machine learning algorithms to detect a wide range of cyberattacks, offering robust defense against various threats.

Also focus on real-time threat detection by adapting a layer three learning switch application. This approach minimizes potential damage and disruption – critical for patient safety. Additionally, the machine learning approach promotes resource optimization, making it ideal for healthcare environments where resources may be limited.

Methodology involves these phases:

1. Data Exploration: Dataset loading and initial analysis.
2. Preprocessing: Data preparation including cleansing, feature transformation, normalization, and shuffling.
3. Train/Test Split: Dataset division for model training and evaluation.
4. Model Generation: Training diverse machine learning algorithms (KNN, DT, RF, NB, LR, AdaBoost, XGBoost) and potentially ensemble techniques for optimal results.
5. User Signup/Login: Authentication system for access control.
6. User Input: Interface for gathering data required for predictions.
7. Prediction: The trained model predicts whether the incoming traffic represents a cyberattack.

Benefits

- Security Focus: MCAD directly addresses the security vulnerabilities often found in cloud- centric systems, enhancing the protection of sensitive data.
- Comprehensive Threat Detection: The use of

***Corresponding Author:** Varshith Veerabomma

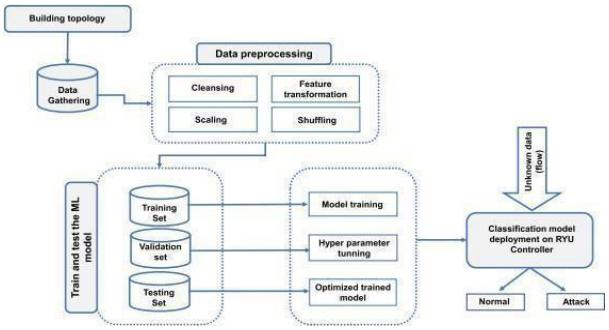
machine learning allows for the detection of a wide array of threats, providing broad protection.

- Real-Time Efficiency: The focus on real-time threat detection supports rapid response, minimizing potential harm in healthcare settings.
- Resource Optimization: The system's design prioritizes minimal resource usage, making it suitable for environments with potential limitations.

Drawbacks

- Dataset Dependence: The accuracy of MCAD, like other machine learning systems,relies on the quality and representativeness of the training dataset.
- Computational Overhead: While optimized, the system may have some computational resource requirements compared to simpler network monitoring tools.
- Evolving Attacks: Continuous adaptation is necessary to keep pace with the changing landscape of cyberattacks.
- Potential for False Positives: There is a possibility, albeit minimized through careful algorithm selection, of flagging benign traffic as malicious.

SYSTEM ARCHITECTURE



ALGORITHMS

KNN: The okay-nearest associates algorithm (KNN or okay-NN) is a non-parametric supervised mastering classifier that is predicated on proximity to classify or are expecting the grouping of character statistics points.

DT: Decision tree is a non-parametric supervised mastering algorithm used for categoryand regression responsibilities. It follows a hierarchical tree shape comprising root, branch,inner, and leaf nodes.

RF: Random wooded area is a extensively-used machine studying set of rules that combines outputs from a couple of selection bushes to produce a single result. Known for its ease of use and versatility, it handles each classification and regression troubles effectively.

NB: Naïve Bayes classifier is a supervised getting to know algorithm normally used for category tasks like textual content class. It belongs to the family of generative getting to know algorithms, aiming to model the distribution of inputs for a given magnificence.

LR: Logistic regression is a supervised gaining knowledge of set of rules typically hired for type responsibilities, predicting the chance of an example belonging to a particular elegance. It's a statistical algorithm analyzing the connection between independent and established binary variables, assisting decision-making.

AdaBoost: AdaBoost, or Adaptive Boosting, is an Ensemble Method in Machine Learning. It commonly employs choice timber with handiest one level (Decision Stumps) as estimators to reinforce overall performance.

XGBoost: XGBoost is an optimized allotted gradient boosting library designed for green and scalable training of gadget gaining knowledge of fashions. It employs ensemble learning, combining predictions from more than one susceptible fashions to beautify prediction accuracy.

Stacking Classifier (RF MLP with LightGBM): Stacking classifier is an ensemblemethod wherein outputs from a couple of classifiers function inputs to a meta-classifier for very last class. This approach effectively tackles multi-category troubles.

Voting Classifier (RF DT): Voting classifier is a gadget getting to know estimator that trains numerous base fashions or estimators and aggregates their findings for prediction. It combines selection outputs from each base estimator to make very last predictions.

RESULTS

The project aims to enhance the security of healthcare systems implemented within software-defined networks (SDNs)utilizing a layer 3 (L3) learning switch application to collect and analyze normal and abnormal network traffic, deployed on the Ryu controller. Rigorous testing involving multiple machine learning algorithms and cyberattack scenarios was conducted to provide a comprehensive performance evaluation.

The results suggest that Adaptive -shield machine learning defence for healthcare SDN's demonstrates robust performance, achieving a high F1-score for both normal and attack training, indicating reliability. This enhances data security and network resilience.

In summary, the project effectively tackles the critical task of safeguarding sensitive patient data within SDNs, offering valuable insights into the efficacy of machine learning-based approaches for cybersecurity in healthcare settings.

CONCLUSION

The development of MCAD represents a promising advancement in securing healthcare systems that integrate Software-Defined Networking (SDN) and IoT-enabled devices. While traditional IoT-enabled heart

***Corresponding Author:** Varshith Veerabomma

monitoring systems offer advantages in data collection, remote care, and efficiency, they often lack the robust cybersecurity mechanisms necessary to protect sensitive patient data. MCAD directly addresses this vulnerability by harnessing the power of machine learning to proactively detect and neutralize diverse cyberattacks.

Methodology underscores a meticulous approach. Adapting a layer three learning switch application enables rapid network traffic analysis, facilitating real-time threat detection essential for rapid response in critical healthcare settings. Thorough data preprocessing, combined with a rigorous exploration of various machine learning algorithms, ensures that MCAD achieves optimal performance in identifying potential attacks.

Despite these challenges, MCAD exhibits considerable potential in safeguarding the integrity of healthcare networks. Future research could focus on advanced ensemble learning strategies to further refine its accuracy.

Expanding and refining the training dataset, while meticulously minimizing the potential for false positives, will also enhance the system's reliability. Additionally, investigating ways to minimize computational overhead will make MCAD even more accessible in resource- sensitive.

REFERENCES

1. Cai, X., Zhang, D., Li, Z., Wang, F., & Liu, Y. (2023). Performance error estimation and elastic integral event triggering mechanism design for T–S fuzzy networked control system under DoS attacks. *IEEE Transactions on Control Systems Technology*.
2. Abubakar, A., & Pranggono, B. (2017, September). Machine learning based intrusion detection system for software defined networks. In *2017 Seventh International Conference on Emerging Security Technologies (EST)* (pp. 138-143). IEEE.
3. Almazyad, A., Halman, L., & Alsaeed, A. (2023). Probe Attack Detection Using an Improved Intrusion Detection System. *Computers, Materials & Continua*, *74*(3).
4. Babbar, H., Rani, S., & AlQahtani, S. A. (2022). Intelligent edge load migration in SDN-IIoT for smart healthcare. *IEEE Transactions on Industrial Informatics*, *18*(11), 7224-7230.
5. Mladenov, B., & Iliev, G. (2022). Studying the effect of internal DoS attacks over SDN controller during switch registration process. In *Proceedings of the International Symposium on Networks, Computers and Communications (ISNCC)* (pp. 1-4). IEEE.
6. Domínguez-Limaico, H., Pazos-Arias, J. J., & García-Duque, J. (2022). Intruder detection system based on artificial neural network for software defined network. *IEEE*.
7. Mehdi, S. A., & Hussain, S. Z. (2022, September). Survey on intrusion detection system in IoT network. In *Proceedings of the International Conference on Innovative Computing and Communications: ICICC 2022* (pp. 721-732). Singapore: Springer Nature Singapore.
8. Ponnusamy, V., Humayun, M., Jhanjhi, N. Z., Yichiet, A., & Almufareh, M. F. (2022). Intrusion detection systems in Internet of Things and mobile ad-hoc networks. *Computer Systems Science & Engineering*, *40*(3), 1199-1215. https://doi.org/10.32604/csse.2022.018518
9. Radoglou-Grammatikis, P., Sarigiannidis, P., Lagkas, T., & Moscholios, I. (2022). Modeling, detecting, and mitigating threats against industrial healthcare systems: A combined software-defined networking and reinforcement learning approach. *IEEE*.
10. Raja, S., Balamurugan, B., & Swarnalatha, P. (2022). Real-time DDoS detection and mitigation in software defined networks using machine learning techniques. *IEEE*.
11. Khondoker, R., Zaalouk, A., Marx, R., & Bayarou, K. (2014, January). Feature-based comparison and selection of software defined networking (SDN) controllers. In *Proceedings of the World Congress on Computer Applications and Information Systems (WCCAIS)* (pp. 1-7). IEEE.
12. Mekki, T., Jabri, I., Rachedi, A., & Chaari, L. (2021). Software-defined networking in vehicular networks: A survey. *Transactions on Emerging Telecommunications Technologies*, *33*(10), 1-10. https://doi.org/10.1002/ett.4265
13. Ghaffar, Z., Alshahrani, A., Fayaz, M., Alghamdi, A. M., & Gwak, J. (2021). A topical review on machine learning, software defined networking, Internet of Things applications: Research limitations and challenges. *Electronics*, *10*(8), 880. https://doi.org/10.3390/electronics10080880
14. Li, C.-S., & Liao, W. (2013). Software defined networks [Guest Editorial]. *IEEE Communications Magazine*, *51*(2), 113.
15. Rehmani, M. H., Davy, A., Jennings, B., & Assi, C. (2019). Software defined networks-based smart grid communication: A comprehensive survey. *IEEE Communications Surveys & Tutorials*, *21*(3), 2637-2670.
16. Eliyan, L. F., & Di Pietro, R. (2021). DoS and DDoS attacks in software defined networks: A survey of existing solutions and research challenges. *Future Generation Computer Systems*, *122*, 149-171. https://doi.org/10.1016/j.future.2021.03.011
17. Benton, K., Camp, L. J., & Small, C. (2013). OpenFlow vulnerability assessment. In *Proceedings of the 2nd ACM SIGCOMM Workshop on Hot Topics in Software Defined Networking (HotSDN '13)* (pp. 151-152). https://doi.org/10.1145/2491185.2491222
18. Mladenov, B., & Iliev, G. (2022, July). Studying the effect of internal DoS attacks over SDN controller during switch registration process. In *Proceedings of the International Symposium on Networks,*

***Corresponding Author:** Varshith Veerabomma

Computers and Communications (ISNCC) (pp. 1-4).
19. Malasri, K., & Wang, L. (2009). Securing wireless implantable devices for healthcare: Ideas and challenges. *IEEE Communications Magazine*, *47*(7), 74-80.
20. Yin, D., Zhang, L., & Yang, K. (2018). A DDoS attack detection and mitigation with software-defined Internet of Things framework. *IEEE Access*, *6*, 24694-24705.
21. Mousavi, S. M., & St-Hilaire, M. (2015, February). Early detection of DDoS attacks against SDN controllers. In *Proceedings of the International Conference on Computing, Networking and Communications (ICNC)* (pp. 77-81).

***Corresponding Author:** Varshith Veerabomma