E-ISSN: 2583-9667
Indexed Journal
Peer Reviewed Journal
https://multiresearchjournal.theviews.in

Received: 11-01-2025
Accepted: 20-02-2025

INTERNATIONAL JOURNAL OF ADVANCE RESEARCH IN MULTIDISCIPLINARY

Volume 3; Issue 2; 2025; Page No. 208-211

Detection of water-bed cyber-attacks using artificial neural networks

[1]Senthilkumar J and [2]SK Piramupreethika

[1]PG Scholar, Department of Computer Science, Vels Institute of Science, Technology and Advanced Studies, Pallavaram, Chennai, Tamil Nadu, India
[2]Assistant Professor, Department of Computer Science, Vels Institute of Science, Technology and Advanced Studies, Pallavaram, Chennai, Tamil Nadu, India

DOI: https://doi.org/10.5281/zenodo.15576143

Corresponding Author: Senthilkumar J

Abstract

Cyber threat intelligence gathered from previous erattacks may provide light on the methods and tools employed by cybercriminals, which can aid in both the reconstruction of assaults and the prediction of their future trajectory. Consequently, to mitigate these consequences, cyber security analysts use threat intelligence, alert correlations, machine learning, and enhanced visualisations. The impact and development of machine learning algorithm are booming in the current scenario. These algorithm are working perfectly by identifying the pattern based on instance based or model based learning. Well the model based learning is more efficient then the instance based learning. Because the instance based learning identify the pattern by memorising its pattern where the model based training try to form a boundary between these and try to classify them. In addition to the utilization of machine learning algorithms, the integration of advanced analytics techniques such as anomaly detection and behavior analysis further fortifies cyber defense mechanisms.
Anomaly detection algorithms sift through vast datasets to identify deviations from normal behavior, flagging potentially malicious activities that might evade traditional rule-based systems. Meanwhile, behavior analysis algorithms scrutinize user actions and system interactions in real-time, discerning subtle deviations indicative of suspicious or unauthorized behavior.

Keywords: Detection, water-bed, cyber-attacks, artificial, neural

Introduction

The primary aim of this project is to design, implement, and evaluate an effective cyberattack detection system leveraging the power of Artificial Neural Networks (ANNs). The system will analyze network traffic patterns and behavior to accurately identify and classify potential cyber threats, enhancing the security posture of the targeted network. The primary objectives of implementing an Artificial Neural Network (ANN)-based system for cyber-attack detection are to enhance proactive threat identification, improve the accuracy of anomaly detection in network traffic, and establish a resilient defense mechanism against evolving cyber threats. This involves training the ANN to recognize patterns indicative of attacks, ensuring real-time monitoring capabilities, and creating an adaptive model that can evolve with the dynamic nature of cyber threats, ultimately fortifying cybersecurity measures for safeguarding sensitive digital assets. The scope of "Detection of Cyber Attacks Using Artificial Neural Networks" involves developing and implementing an artificial neural network-based system to identify and thwart cyber threats. This encompasses the design, training, and evaluation of the neural network for effective detection, contributing to enhanced cybersecurity measures. The focus is on leveraging advanced machine learning techniques to augment existing security frameworks and mitigate the evolving challenges posed by cyber-attacks.

Literatu Resurvey

Reference 1
Title: Mitigating Adversarial Attacks on DataDriven Invariant Checkers for Cyber-Physical Systems.
Author: Rajib Ranjan Maiti, Cheah Huei Yoong
Year: 2023

Description: The use of invariants in developing security mechanisms has become an attractive research area because of their potential to both prevent attacks and detect attacks

in CyberPhysical Systems (CPS). In general, an invariant is a property that is expressed using design parameters along with Boolean operators and which always holds in normal operation of a system, in particular, a CPS. Invariants can be derived by analysing operational data of various design parameters in a running CPS, or by analysing the system's requirements/design documents, with both of the approaches demonstrating significant potential to detect and prevent cyber-attacks on a CPS. While data-driven invariant generation can be fully automated, design-driven invariant generation has a substantial manual intervention. In this paper, we aim to highlight the shortcomings in data-driven invariants by demonstrating a set of adversarial attacks on such invariants. We propose a solution strategy to detect such attacks by complementing them with design-driven invariants. We perform all our experiments on a real water treatment testbed. We shall demonstrate that our approach can significantly reduce false positives and achieve high accuracy in attack detection on CPSs.

Reference 2:
Title: Cyber Restoration of Power Systems: Concept and Methodology for Resilient
Observability.
Author: Shamsun Nahar Edib, Graduate Student
Member IEEE, Yuzhang Lin
Year: 2023

Description: 17 In order to have a properly functioning cyber– physical power system, the operational data need to be properly measured, transmitted, and processed. In case of a malicious event on the cyber layer of the power system, such as the wide-area monitoring system, cyber components, such as phasor measurement units (PMUs), communication routers, and phasor data concentrators (PDCs) may be compromised, leading to an unobservable power system. This article proposes the concept of cyber restoration of power systems, and an optimal restoration scheme to recover the system observability swiftly after massive interruptions. The cyber restoration problem is formulated as a mixed integer linear programming (MILP) problem considering PMU measurability, communication network connectivity, and PDC processability conditions, as well as cyber restoration resources as constraints. Results in the IEEE 57- bus system validate that the proposed optimization method can provide solutions that recover system observability much faster than heuristic methods, demonstrating the need for systematic cyber restoration planning research and implementation.

Reference 3
Title: Attack Hypotheses Generation Based on Threat Intelligence Knowledge Graph.
Author: Florian Klaus Kaiser, Uriel Dardik, AviadElitzur, PolinaZilberman, Nir Daniel, Marcus Wiens, Frank Schultmann, Yuval Elovici, and Rami Puzis.
Year: 2022

Description: Cyber threat intelligence on past attacks may help with attack reconstruction and the prediction of the course of an ongoing attack by providing deeper understanding of the tools and attack patterns used by attackers. Therefore, cyber security analysts employ threat intelligence, alert correlations, machine learning, and advanced visualizations in order to produce sound attack hypotheses. In this paper, we present AttackDB, a multi-level threat knowledge base that combines data from multiple threat intelligence sources to associate high-level ATT&CK techniques with lowlevel telemetry found in 18 behavioral malware reports. We also present the Attack Hypothesis Generator which relies on knowledge graph traversal algorithms and a variety of link prediction methods to automatically infer ATT&CK techniques from a set of observable artifacts. Results of experiments performed with 53K VirusTotal reports indicate that the proposed algorithms employed by the Attack Hypothesis Generator are able to produce accurate adversarial technique hypotheses with a mean average precision greater than 0.5 and area under the receiver operating characteristic curve of over 0.8 when it is implemented on the basis of AttackDB. The presented toolkit will help analysts to improve the accuracy of attack hypotheses and to automate the attack hypothesis generation process. Index Terms—cyber threat intelligence, data fusion, attack hypotheses, link prediction of the future which leads to a very vast change.

Reference 4: Title: A Study of Cyber Security Challenges and Its Emergning Trends on Latest Technologies.
Author: G. Nikhita Reddy1, G.J. Ugander Reddy 2
Year: 2021

Description: Cyber Security plays an important role in the field of information technology. Securing the information have become one of the biggest challenges in the present day. When ever we think about the cyber security the first thing that comes to our mind is 'cyber crimes' which are increasing immensely day by day. Various Governments and companies are taking many measures in order to prevent these cyber crimes. Besides various measures cyber security is still a very big concern to many. This paper mainly focuses on challenges faced by cyber security on the latest technologies. It also focuses on latest about the cyber security techniques, ethics and the trends changing the face of cyber security. Keywords: cyber security, cyber crime, cyber ethics, social media, cloud computing, android apps.

Existing System
The utilization of invariants in the development of security mechanisms has garnered significant interest in the context of Cyber-Physical Systems (CPS), owing to their potential to prevent and identify attacks. Invariants are properties expressed using design parameters and Boolean operators, which remain true during normal CPS operation. These invariants can be derived from operational data or system requirements/design documents. While data-driven invariant generation is automated, design-driven methods require manual input. This paper exposes vulnerabilities in datadriven invariants by showcasing adversarial attacks. To address this, the paper proposes a solution involving both data-driven and designdriven invariants, aiming to enhance attack detection accuracy. Experiments conducted on an actual water treatment testbed demonstrate the effectiveness of this approach in reducing false positives and achieving reliable attack detection for CPSs.

Drawbacks

- They have used ROC algorithm which is one of the machine learning algorithm.
- They did not implement the deployment process. Implementing a hierarchical network with both communication and physical layers in a distributed and decentralized manner can introduce increased complexity to the system design and operation.
- This complexity might lead to challenges in system maintenance, troubleshooting, and scalability.

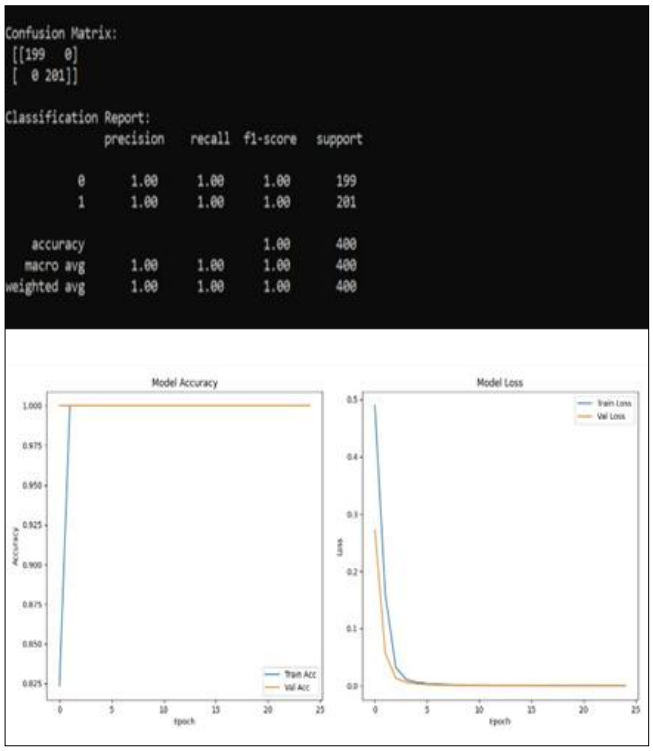
Proposed System

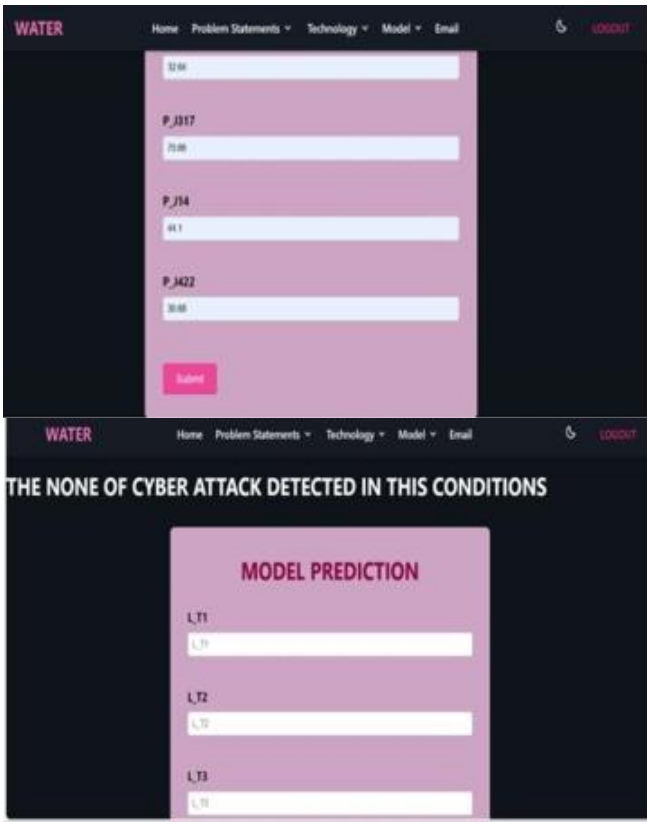
The proposed system focuses on utilizing Artificial Neural Networks (ANNs) for the detection of cyber-attacks. ANNs are a type of machine learning technique inspired by the human brain's neural structure. The objective here is to leverage ANNs to identify and counteract cyber-attacks effectively. This research 22 acknowledges the rising threat of cyber-attacks and aims to enhance cybersecurity by using ANNs as a robust and adaptable tool. The study likely explores how ANNs can learn patterns from historical attack data and subsequently identify deviations from normal behaviour, enabling timely detection and response to potential cyber threats. Overall, the abstract highlights the potential of ANNs to contribute significantly to cyber-attack detection and prevention strategies.

Advantages

- We implemented ANN architecture algorithm which can handle more hierarchical data.
- We implemented the one of best architecture of neural network to reduce the attack based on the cyber security in water management.
- We develop a framework based application for deployment purpose.

Results and Discussion





Conclusion

In conclusion, the utilization of Artificial Neural Networks (ANNs) for cyber attack detection represents a promising and effective approach. The ability of ANNs to analyze complex patterns in real-time data has shown great potential in enhancing the accuracy and speed of cyber threat identification. This method offers a proactive defense mechanism against evolving cyber threats, providing a robust layer of security. While challenges such as model interpretability and training data quality exist, ongoing research and advancements in neural network architectures continue to address these concerns. The integration of ANNs into cyber defense strategies is crucial for staying ahead in the constantly evolving landscape of cyber threats. As we move forward, further refinements and collaborative efforts between academia and industry will play a pivotal role in optimizing the performance and resilience of ANNbased cyber attack detection systems.

Future Enhancement

In future work, the refinement and optimization of artificial neural network architectures for cyber attack detection will be explored, aiming to enhance both accuracy and efficiency. Investigating the integration of advanced anomaly detection techniques and evolving the neural network models to adapt to emerging cyber threats will be a focal point. Additionally, research will focus on developing strategies for real time threat identification and response, further strengthening the system's proactive defense capabilities. Continuous exploration of novel datasets and the incorporation of federated learning approaches may offer insights into improving the adaptability and robustness of the detection system. Ongoing efforts will be directed towards achieving a comprehensive and resilient cyber

defense framework by embracing advancements in artificial intelligence and cybersecurity.

References

1. Maiti RR, Young CH. Mitigating adversarial attacks on data-driven invariant checkers for cyber-physical systems. IEEE/CAA J Autom Sinica. 2023;10(3):637–642.
2. Edib SN, Lin Y. Cyber restoration of power systems: Idea and approach for resilient observability – a survey. Computers & Security. 2018;78:101567.
3. Kaiser FK, Dardik U, Elitzur A, Zilberman P, Daniel N. Attack hypotheses generation based on threat intelligence knowledge graph: A survey. IEEE Trans Syst Man Cybern Syst. 2021;11(1):216–250.
4. Reddy N, Reddy U. A study of cybersecurity challenges and its emerging trends on latest technologies. IEEE Access. 2017;5:46375–46378.
5. Li Y, Liu Q. A comprehensive review study of cyber attacks and cybersecurity: Emerging trends and recent developments. IEEE Trans Neural Netw Learn Syst. 2021.
6. Zhang J, Pan L, Han QL, Chen C, Wen S, Xiang Y. Deep learning-based attack detection for cyber-physical system cybersecurity: A survey. IEEE/CAA J Autom Sinica. 2021;9(3):377–391.
7. Boyaci O, Umunnakwe A, Sahu A, Narimani MR, Ismail M, Davis KR, Serpedin E. Graph neural networks-based detection of stealth false data injection attacks in smart grids. IEEE Syst J. 2021;16(2):2946–2957.
8. Fan FL, Xiong J, Li M, Wang G. On interpretability of artificial neural networks: A survey. IEEE Trans Radiat Plasma Med Sci. 2021;5(6):741–760.
9. Bhamare D, Zolanvari M, Erbad A, Jain R, Khan K, Meskin N. Cybersecurity for industrial control systems: A survey. Computers & Security. 2020;89:101677.
10. Corallo A, Lazoi M, Lezzi M. Cybersecurity in the context of Industry 4.0: A structured classification of critical assets and business impacts. Computers in Industry. 2020;114:103165.
11. Lin Y, Tu Y, Dou Z. An improved neural network pruning technology for automatic modulation classification in edge devices. IEEE Trans Veh Technol. 2020;69(5):5703–5706.
12. Gupta M, Abdelsalam M, Khorsandroo S, Mittal S. Security and privacy in smart farming: Challenges and opportunities. IEEE Access. 2020;8:34564–34584.
13. Nguyen TT, Reddi VJ. Deep reinforcement learning for cybersecurity. IEEE Trans Neural Netw Learn Syst. 2021.
14. Zubaidi SL, Abdulkareem IH, Hashim KS, AlBugharbee H, Ridha HM, Gharghan SK, *et al*. Hybridised artificial neural network model with slime mould algorithm: A novel methodology for prediction of urban stochastic water demand. Water. 2020;12(10):2692.