International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2022): 7.942

Harnessing AI and Machine Learning for Intrusion Detection in Cyber Security

Sunil Chahal

ConceptsIT, Inc.

Abstract: ***The study helps to investigate the performance of ML and AI to detect IDS using different segments. The first segment helps to inform the project aim, objective, and issues in a comprehensive way. The second segment helps to inform the background of the study, different critical factors, and theoretical factors effectively. The third segment helps to inform all the methods that have been chosen to implement the project. The result segment illustrated different themes related to the topic and the last segment provided different information that can be implemented in the future to facilitate the work.***

Keywords: IDS, ML, AI, Cybersecurity

1. Introduction

a) Project Specification

Using AI and ML for intrusion detection in cybersecurity entails equipping networks with sophisticated algorithms that detect and counteract malicious activity on their own. This is vital as conventional approaches frequently fall behind the ever-evolving nature of cyber threats. Systems powered by AI that perform real-time analysis of massive datasets, resulting in improved detection and reaction times. They are able to change and learn from different types of cyberattacks, making them a proactive defense.

b) Aim and Objectives

Aim

The aim of this project is to use AI and machine learning ML to create a reliable Intrusion Detection System (IDS) for cyber defense.

Objectives

- To evaluate the performance of ML and AI in the real world
- To investigate the performance of ML and AI for IDS in cyber defense
- To analyze the purpose of developing a cybersecurity protocol

c) Research Question

- How to evaluate the performance of ML and AI in real-world applications?
- What is the process for investigating the performance of ML and AI for IDS in cyber defense?
- Why cybersecurity protocol development is important?

d) Research Rationale

What is the issue?

The growing sophistication of cyber-attacks is a big problem in intrusion detection since it makes it difficult for traditional rule-based systems to keep up with new attack tactics [1]. Security personnel may feel overwhelmed by the sheer volume of data that must be analyzed in real-time.

Why is the issue?

Traditional rule-based systems struggle to properly recognize and respond to growing cyber threats because attackers are continually developing new tactics and evasion strategies [2]. Keeping networks safe from ever-evolving cyber threats calls for innovative measures like AI-driven intrusion detection.

What is the issue now?

The exponential growth of IoT gadgets has presented a new difficulty in cyber defenses and due to their often-weak security measures, these gadgets are easy targets for hackers.

2. Literature Review

a) Research background

The use of AI systems in daily life for the use of making people's lives easy provides a simple load of work and helps people trust the AI system and be generous to each other. The AI system used for machine learning gives real value to the learning algorithms creates deep learning method and provide a better function of the work [3]. The system used by the AI is very unstable for any intrusion to come through and damage the system or steal any important file. The AI system is used in Cybersecurity to detect the intrusion of a hacker and provide steps to get rid of that hacker.

b) Critical Assessment

AI system for many years has increased the frequency of the detection of cybersecurity system and many other aspects which includes cyber phishing, intrusion detection, malware detection, and threat analysis. AI, however, is being practiced more and more with the help of SVM, decision trees, and deep neural networks to improve the performance and accuracy of the detection system [4]. The adaptability and detection are also generally increased with the help of Natural Language Processing (NLP). NPL is also used for training the AI to counter phishing by having the knowledge of patterns of language and scientific features.

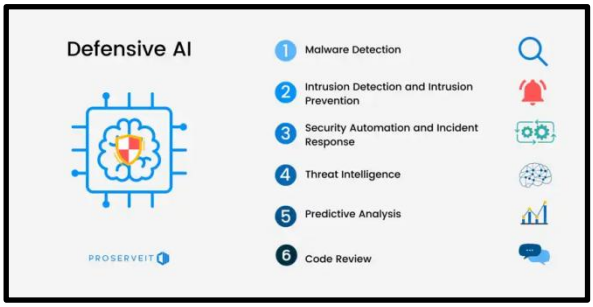

Figure 1: The good AI and the bad AI

c) Linkage to Aim

Cybersecurity is a risky thing to handle and perform. The hacker who counters the cyber-attack sometimes gets into trouble by being taken down from the system and the system remains intact for the hacker to pass through. This is why the use of an AI system is very important for the cause of defeating the hacker, not letting the hacker at all, and helping the programmer and user who are having problems dealing with the hacker. The AI system is very intelligent and with reasonable help from using machine learning and training the AI, the AI is able to withstand outsiders very well and keep safe from any intrusion.

d) Implementation purpose of the Intrusion detection system in Cybersecurity

In order to proactively detect and respond to unauthorised or malicious actions within a network or system the primary goal of deploying an IDS in cybersecurity. A crucial line of defence against cyber-attacks, an IDS works by constantly monitoring and analysing network traffic [7]. It quickly alerts security staff to suspected security breaches by spotting abnormalities, strange trends or known attack signatures. With an early warning system in place, corrective actions have been taken quickly, limiting harm and protecting private information. An IDS helps with forensic analysis that is essential for deducing the specifics of attacks and improving an organization's security in general.

e) Theoretical Framework

The use of AI and its techniques allows the user to build further models to train the AI. The new models or adaptive models like adaptive phishing are used to learn the AI for the detection of these attacks and help the user by defending against the attack until and unless the attacker gets destroyed or runs away from the server [8]. The AI uses data preprocessing and checks the content of an email one by one and finds out the possible features that help in to fight against adaptive phishing.

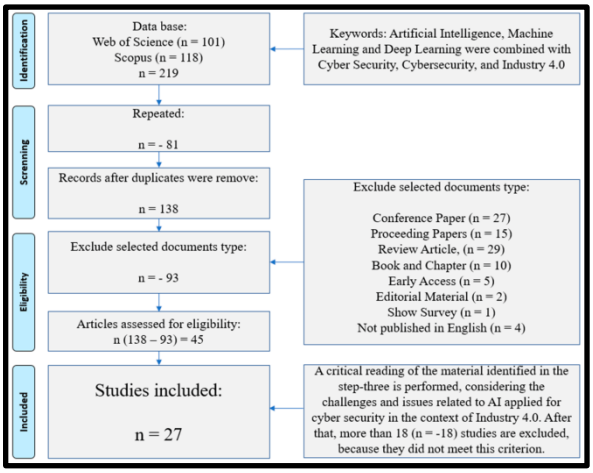

Figure 2: Artificial Intelligence-based Cyber Security

f) Literature Gap

Extra features like the extensive use of deep learning algorithms to make the AI far better and also more extensive use of adaptive phishing is able to be done are not provided [9]. The use of adaptive phishing is to check and format the given data to remove any incompetencies, redundancies, and error which has the ability to bring down the algorithm. AI also does not want to build newer models over and over for the models are pretty much the same from one another [10]. AI learning from machine learning is able to use the deep learning model methods to enhance its speed in the choice of decisions and help to make a better world.

3. Methodology

a) Research philosophy

This research is completely processed with new ideas to develop the cybersecurity system and its performed actions. The development of this research is correspondingly done to make a system well-equipped with ML technologies [11]. Cybersecurity acts have to be updated with new types of features to stop the continuous actions of data intruders [12]. The data is collected from self-experiments depending on the research articles and journal papers regarding cybersecurity. A neat and clean concept about AI and cyber technologies with hands-on knowledge is required to develop this project nicely. Thus, a positivist philosophy is applied during this research and its analysis work.

b) Research approach

The research is improved for a better analysis of all deterministic projects related to AI technologies. The data crisis has been a greater aspect by means of data privacy and protection acts. Nowadays much research is working on protection technologies with AI equipment to protect the data from data intruders [13]. These technologies of cybersecurity are implemented on the basis of a detailed study of cyber hacking actions. The privacy detection system is enhanced to make this software available to all kinds of users with simplified latest technologies [14]. Thus, a deductive approach

is used in this research related to cybersecurity topics with optimized analysis of cyber tools and techniques.

The project has used a "deductive research approach" since it is more organised and hypothesis-driven. This method is a well-defined theory or hypothesis, such as the idea that AI and ML greatly improve cybersecurity intrusion detection [15]. The study begins with this hypothesis and uses deductive reasoning to go forward with data collection and analysis in an effort to verify or disprove it. In projects, well-established principles must be used, such as the use of AI and ML in cybersecurity because they permit thorough testing and confirmation of theoretical notions. The deductive method lays the groundwork for drawing conclusions and offering suggestions that are grounded on actual data and sound reasoning [5].

c) Research design

This research is required to develop AI-based functionalities over cybersecurity models to enhance security systems. The ML technologies are tried to implement using lots of classification and regression algorithms [16]. These technologies are made sufficient for all types of user systems to make cyber apps easy to use for all users.

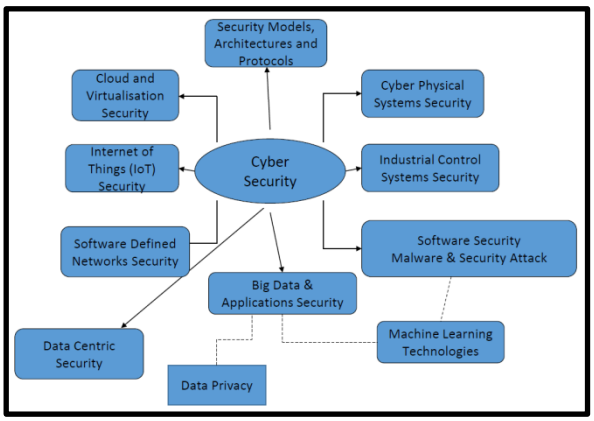

Figure 3: Cyber Research Design

Hence some important journal papers and research articles are used for the references of the cyber-based research. Thus, a descriptive design is accomplished for this research and all kinds of concepts are briefly analyzed throughout this project [17]. The whole development of this project is finalized on the optimization of detection models for cybersecurity.

The project has used a "descriptive research design" since it is best suited to provide an all-encompassing understanding of current occurrences. Descriptive research allows for the methodical collection and analysis of data to provide a picture of the state of cybersecurity and intrusion detection as it stands at the present time [18]. It helps scientists identify cyber threats and network traffic patterns, behaviours and trends. This data is essential for creating AI and ML models that meet the unique requirements of a business. A descriptive study methodology provides helpful insights into the efficiency of the tactics that have been applied, allowing for better decisions and future improvements to the cybersecurity architecture[6].

d) Data Analysis and Collection Method

Hence the whole research is getting regulated for the detailed analysis of research data based on cybersecurity models. The data for this research is secondary because this data is not compared with any other experiment [19].

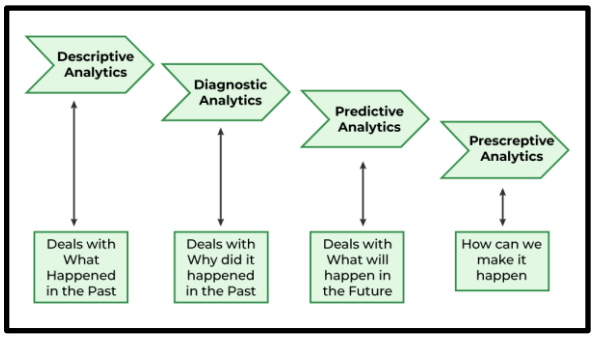

Figure 4: Data Analysis and Collection Method

This information has covered a wide range of system and network activities [20]. Firewalls, intrusion detection systems, and server logs are examples of data sources. Tools for real-time monitoring record system events and network activity. Data cleansing, feature extraction, and normalization are all components of preprocessing [21]. The data is subsequently analyzed using machine learning methods, including supervised models such as "Random Forest" and "unsupervised models" like clustering algorithms. Anomaly detection techniques also reveal odd patterns.

e) Ethical considerations

The use of AI and machine learning for intrusion detection in cybersecurity needs to be done with the maximum ethical care. The privacy and security of people's sensitive data throughout the intrusion detection procedure have been secured [22]. The ethical requirements for data collection and processing included full disclosure and informed permission. It is important to be on the lookout for algorithmic biases that have led to false positives or negatives because they can have detrimental effects [23]. Model development transparency, auditing, and ongoing review to reduce biases are ethical obligations. Cooperation and security have been promoted through sharing threat intelligence and AI-powered intrusion detection techniques while preserving intellectual property rights.

4. Results

a) Critical Analysis

Conventionally, apparatus learning techniques have been categorized into two classes including commanded as well as unsupervised knowledge. In supervised knowledge, information samples are tagged according to their course. Apprenticeship data, along with data labeling is utilized and performed manually, instructing humans to notice data marks with their styles [24]. The prepared data is input to the

algorithm to make a mathematical operation, that has output the defined classes provided by recent data samples [25]. Machine learning processes data very simply through the determining factor that is commonly called function [26]. The information input is the process for a table regarding a row as well as the column, from that row, serving like information simply along with that column representing that function.

5. Finding and Discussion

A dissimilar technique is a *"Rule-Learning"* approach, that aspires to encounter a decor of characteristic discounts considering each iteration that maximizes the score which represents the variety of result's quality for standard, the numeral of incorrectly categorized data representatives [27]. The benefit of that rule-learning design is that this could factor in human specialist recommendations in breeding regulations. Similarly, the procedure is typically utilized as an interpretation standard for different machine learning procedures in witnessing grid intrusions [28].

Theme 1: ML Techniques to Glimpse Attacks
There are various through to make security inside UAV webs as well as utilizing anomaly detection use from ML algorithms inside directives to the growth the accuracy regarding 5G transferred packets [29]. Anomaly detection exists not an unknown meadow of examination inside ML systems, as well as recent analysis has concentrated on a comprehensive capacity to consider ML through applications.

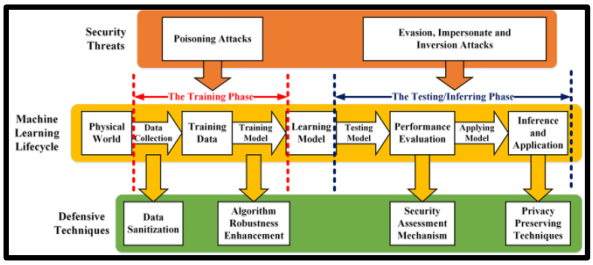

Figure 5: Analyze security threats and application of defensive technique

Theme 2: ML Utilize Inside Cyber Security
The majority regarding "Artificial Intelligence (AI)" as well as ML instruments is conducted to a cybersecurity peninsulae ethnicity [30]. Both assailants along with defenders are discovering the prospect of AI including ML to improve their qualifications.

Theme 3: Using Anomaly Detection Algorithms to Strengthen Cybersecurity
The rising complexity of cyber threats calls for cutting-edge methods of intrusion detection in the field of cybersecurity [31]. The use of AI and ML algorithms, in particular anomaly detection, is one of the most promising methods now available.

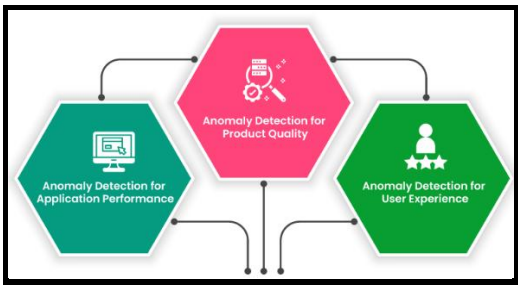

Figure 6: Three different business segments for the Anomaly Detector

"Anomaly detection" operates on the premise that data outliers represent malicious intrusion attempts. "Anomaly detection" enabled by AI is essential since traditional rule-based systems can't keep up with rapidly changing threats. Computers also learn to discern regular behaviour from suspicious behaviour by employing ML models like SVMs or deep learning techniques such as CNNs [32]. These models help to recognise normal-looking patterns in network traffic using massive datasets. They are able to spot discrepancies from the norm and trigger warnings for further inquiry during presented with fresh information. This method drastically decreases the number of false positives, freeing up security staff to concentrate on real dangers.

Theme 4: In-Stream Threat Detection Using AI
The rapid evolution of cyber threats necessitates a real-time response from cybersecurity measures. The combination of AI and stream processing yields a potent tool for early warning of potential danger. Data has been continuously analysed as it travels via a network thanks to stream processing. This is of paramount importance during times of crisis, such as "distributed denial of service (DDoS)" assaults. They are able to instantly evaluate incoming data for harmful intent during the time AI algorithms are included in the stream processing pipeline. In order to examine temporal trends in network traffic, for instance, learners use recurrent neural networks. These algorithms are able to send out notifications immediately by spotting anomalies such as abrupt increases or changes in trend [33]. This method enables real-time threat identification, giving security teams the ability to respond rapidly and limit the impact of assaults.

Theme 5: The Human-AI Synergy in Intrusion Detection
AI and ML certainly have their place in cybersecurity and they are at their most useful when combined with human knowledge. Together, human knowledge and AI-driven intrusion detection offer a powerful barrier against cyberattacks. The contextual expertise and intuition that human analysts possess are crucial when trying to separate false positives from actual dangers [34]. They also use their expertise in the field to inform the development of "machine learning models", helping to fine-tune such models to the particulars of a given organization's infrastructure. The AI-generated notifications also be checked by human experts. On the other hand, by incorporating human judgement, the system

fine-tuned over time to increase accuracy and decrease false positives.

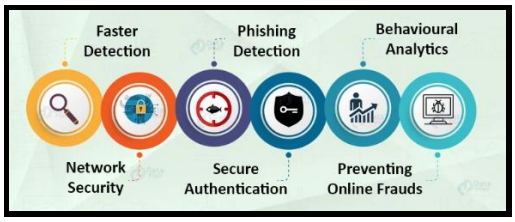

Figure 7: Application of AI in Cyber Secuirity

AI and humans are working together in the quest for potential dangers and A.I. is great at finding outliers, but human analysts are experts at figuring out what drives and guides attackers. The two work together in harmony to improve a company's defences against cyberattacks. In order to sum up, the use of AI and ML in intrusion detection is changing the face of cybersecurity in profound ways. Organisations have strengthened their defences against the ever-changing panorama of cyber threats by using anomaly detection algorithms, real-time threat identification, and the synergy between human intelligence and AI [35]. These motifs illustrate the various methods that have been used to produce a powerful cybersecurity plan.

Evaluation

The AI along with ML could be utilized to detect abnormalities including pessimistic activity in the application and method procedures, appeals/retorts, or web traffic which can predict a cyber invasion is underway. User Commodity, as well as Behavior Analytics outlets, generally utilize AI including ML to define logs along with determining outlandish and forgotten logins, unauthorized admission attempts, and different pessimistic activities.

6. Conclusion

In order to keep up with cyber threats, it is crucial to incorporate AI and ML into intrusion detection for cybersecurity. Real-time analysis is made possible by these technologies, leading to faster identification and resolution. The complexity of modern threats exceeds the capabilities of rule-based systems. In addition, a new security hole has been exposed by the explosion of IoT gadgets.

The use of AI and ML for intrusion detection in cybersecurity is an exciting meeting of cutting-edge hardware and human knowledge. Powered by sophisticated ML models, anomaly detection systems can filter through massive datasets and reliably discern between regular operations and possible threats. Timely responses to ever-evolving cyber threats are made possible by real-time threat identification made possible by stream processing and AI integration. On the other hand, by providing context, intuition, and topic experience, human analysts can improve AI systems and verify alarms. Together, they provide a strong barrier against the ever-changing cyber environment. This symbiotic relationship between technology and human inventiveness represents a major step forward in cybersecurity, protecting businesses from a constantly evolving set of cyber threats.

7. Research Recommendation

Maintaining AI systems' ability that can help to detect intrusions and respond to new types of threats requires constant monitoring and updates. Taking a Team Effort to Improve IDS Performance Encourage communication and cooperation between cybersecurity professionals, AI researchers, and system administrators. User education and awareness campaigns can able to teach people how to protect themselves and their devices from cyber threats posed by Internet of Things gadgets. Maintain close coordination between the IDS and incident response procedures to facilitate prompt responses to discovered intrusions.

8. Future Work

Improved ML Models Look at deep learning and reinforcement learning to see if they can help the intrusion detection system perform better. Build and deploy unique security controls for IoT devices to reduce risks and strengthen the network's defenses. In order to better distinguish between regular and suspect network activity, behavioral analysis can be implemented. Study and implement steps to meet ever-changing cybersecurity legislation and requirements.

References

[1] A. Pinto et al, "Survey on Intrusion Detection Systems Based on Machine Learning Techniques for the Protection of Critical Infrastructure," Sensors, vol. 23, (5), pp. 2415, 2023. Available: https://www.proquest.com/scholarly-journals/survey-on-intrusion-detection-systems-based/docview/2785235857/se-2. DOI: https://doi.org/10.3390/s23052415.

[2] d. A. Antonio João Gonçalves et al, "Artificial Intelligence-Based Cyber Security in the Context of Industry 4.0—A Survey," Electronics, vol. 12, (8), pp. 1920, 2023. Available: https://www.proquest.com/scholarly-journals/artificial-intelligence-based-cyber-security/docview/2806520841/se-2. DOI: https://doi.org/10.3390/electronics12081920.

[3] U. AlHaddad et al, "Ensemble Model Based on Hybrid Deep Learning for Intrusion Detection in Smart Grid Networks," Sensors, vol. 23, (17), pp. 7464, 2023. Available: https://www.proquest.com/scholarly-journals/ensemble-model-based-on-hybrid-deep-learning/docview/2862728946/se-2. DOI: https://doi.org/10.3390/s23177464.

[4] R. S. Sangwan, Y. Badr and S. M. Srinivasan, "Cybersecurity for AI Systems: A Survey," Journal of Cybersecurity and Privacy, vol. 3, (2), pp. 166, 2023. Available: https://www.proquest.com/scholarly-

journals/cybersecurity-ai-systems-survey/docview/2829814088/se-2. DOI: https://doi.org/10.3390/jcp3020010.

[5] V. M. Pilla et al, "Leveraging Computational Intelligence Techniques for Defensive Deception: A Review, Recent Advances, Open Problems and Future Directions," Sensors, vol. 22, (6), pp. 2194, 2022. Available: https://www.proquest.com/scholarly-journals/leveraging-computational-intelligence-techniques/docview/2642665939/se-2. DOI: https://doi.org/10.3390/s22062194.

[6] Z. Amiri et al, "The Personal Health Applications of Machine Learning Techniques in the Internet of Behaviors," Sustainability, vol. 15, (16), pp. 12406, 2023. Available: https://www.proquest.com/scholarly-journals/personal-health-applications-machine-learning/docview/2857444945/se-2. DOI: https://doi.org/10.3390/su151612406.

[7] J. Kwon et al, "Anomaly Detection in Multi-Host Environment Based on Federated Hypersphere Classifier," Electronics, vol. 11, (10), pp. 1529, 2022. Available: https://www.proquest.com/scholarly-journals/anomaly-detection-multi-host-environment-based-on/docview/2670137839/se-2. DOI: https://doi.org/10.3390/electronics11101529.

[8] M. Kuzlu, C. Fair and O. Guler, "Role of Artificial Intelligence in the Internet of Things (IoT) cybersecurity," Discover Internet of Things, vol. 1, (1), 2021. Available: https://www.proquest.com/scholarly-journals/role-artificial-intelligence-internet-things-iot/docview/2730345656/se-2. DOI: https://doi.org/10.1007/s43926-020-00001-4.

[9] C. Hesselman et al, "A Responsible Internet to Increase Trust in the Digital World," Journal of Network and Systems Management, vol. 28, (4), pp. 882-922, 2020. Available: https://www.proquest.com/scholarly-journals/responsible-internet-increase-trust-digital-world/docview/2784112060/se-2. DOI: https://doi.org/10.1007/s10922-020-09564-7.

[10] M. Ienca, "Democratizing cognitive technology: a proactive approach," Ethics and Information Technology, vol. 21, (4), pp. 267-280, 2019. Available: https://www.proquest.com/scholarly-journals/democratizing-cognitive-technology-proactive/docview/2056907577/se-2. DOI: https://doi.org/10.1007/s10676-018-9453-9.

[11] M. Pieter-Jan et al, "Resource Management in a Containerized Cloud: Status and Challenges," Journal of Network and Systems Management, vol. 28, (2), pp. 197-246, 2020. Available: https://www.proquest.com/scholarly-journals/resource-management-containerized-cloud-status/docview/2376094890/se-2. DOI: https://doi.org/10.1007/s10922-019-09504-0.

[12] J. Bugeja, A. Jacobsson and P. Davidsson, "PRASH: A Framework for Privacy Risk Analysis of Smart Homes," Sensors, vol. 21, (19), pp. 6399, 2021. Available: https://www.proquest.com/scholarly-journals/prash-framework-privacy-risk-analysis-smart-homes/docview/2581056027/se-2. DOI: https://doi.org/10.3390/s21196399.

[13] J. Rochford, "Accessibility and IoT / Smart and Connected Communities," AIS Transactions on Human-Computer Interactions, vol. 11, (4), pp. 253-263, 2019. Available: https://www.proquest.com/scholarly-journals/accessibility-iot-smart-connected-communities/docview/2500444291/se-2. DOI: https://doi.org/10.17705/1thci.00124.

[14] N. Chouliaras et al, "Cyber Ranges and TestBeds for Education, Training, and Research," Applied Sciences, vol. 11, (4), pp. 1809, 2021. Available: https://www.proquest.com/scholarly-journals/cyber-ranges-testbeds-education-training-research/docview/2534620537/se-2. DOI: https://doi.org/10.3390/app11041809.

[15] E. Batista et al, "Sensors for Context-Aware Smart Healthcare: A Security Perspective," Sensors, vol. 21, (20), pp. 6886, 2021. Available: https://www.proquest.com/scholarly-journals/sensors-context-aware-smart-healthcare-security/docview/2584556310/se-2. DOI: https://doi.org/10.3390/s21206886.

[16] E. Ukwandu et al, "Cyber-Security Challenges in Aviation Industry: A Review of Current and Future Trends," Information, vol. 13, (3), pp. 146, 2022. Available: https://www.proquest.com/scholarly-journals/cyber-security-challenges-aviation-industry/docview/2642426919/se-2. DOI: https://doi.org/10.3390/info13030146.

[17] R. T. Vinay Simha et al, "A Review on Emerging Communication and Computational Technologies for Increased Use of Plug-In Electric Vehicles," Energies, vol. 15, (18), pp. 6580, 2022. Available: https://www.proquest.com/scholarly-journals/review-on-emerging-communication-computational/docview/2716531426/se-2. DOI: https://doi.org/10.3390/en15186580.

[18] E. Jaw and X. Wang, "Feature Selection and Ensemble-Based Intrusion Detection System: An Efficient and Comprehensive Approach," Symmetry, vol. 13, (10), pp. 1764, 2021. Available: https://www.proquest.com/scholarly-journals/feature-selection-ensemble-based-intrusion/docview/2584553053/se-2. DOI: https://doi.org/10.3390/sym13101764.

[19] A. Samarakkody, D. Amaratunga and R. Haigh, "Technological Innovations for Enhancing Disaster Resilience in Smart Cities: A Comprehensive Urban Scholar's Analysis," Sustainability, vol. 15, (15), pp. 12036, 2023. Available: https://www.proquest.com/scholarly-journals/technological-innovations-enhancing-disaster/docview/2849117694/se-2. DOI: https://doi.org/10.3390/su151512036.

[20] I. A. Elaalami, S. O. Olatunji and R. M. Zagrouba, "AT-BOD: An Adversarial Attack on Fool DNN-Based Blackbox Object Detection Models," Applied Sciences, vol. 12, (4), pp. 2003, 2022. Available:

https://www.proquest.com/scholarly-journals/at-bod-adversarial-attack-on-fool-dnn-based/docview/2632200209/se-2. DOI: https://doi.org/10.3390/app12042003.

[21] J. Brás, R. Pereira and S. Moro, "Intelligent Process Automation and Business Continuity: Areas for Future Research," Information, vol. 14, (2), pp. 122, 2023. Available: https://www.proquest.com/scholarly-journals/intelligent-process-automation-business/docview/2779561954/se-2. DOI: https://doi.org/10.3390/info14020122.

[22] X. M. Liu and D. Murphy, "A Multi-Faceted Approach for Trustworthy AI in Cybersecurity," Journal of Strategic Innovation and Sustainability, vol. 15, (6), pp. 68-78, 2020. Available: https://www.proquest.com/scholarly-journals/multi-faceted-approach-trustworthy-ai/docview/2472179568/se-2.

[23] J. Hance et al, "Distributed Attack Deployment Capability for Modern Automated Penetration Testing," Computers, vol. 11, (3), pp. 33, 2022. Available: https://www.proquest.com/scholarly-journals/distributed-attack-deployment-capability-modern/docview/2642354732/se-2. DOI: https://doi.org/10.3390/computers11030033.

[24] S. Coghlan, T. Miller and J. Paterson, "Good Proctor or "Big Brother"? Ethics of Online Exam Supervision Technologies," Philosophy & Technology, vol. 34, (4), pp. 1581-1606, 2021. Available: https://www.proquest.com/scholarly-journals/good-proctor-big-brother-ethics-online-exam/docview/2607925766/se-2. DOI: https://doi.org/10.1007/s13347-021-00476-1.

[25] M. Altoub et al, "An Ontological Knowledge Base of Poisoning Attacks on Deep Neural Networks," Applied Sciences, vol. 12, (21), pp. 11053, 2022. Available: https://www.proquest.com/scholarly-journals/ontological-knowledge-base-poisoning-attacks-on/docview/2771659834/se-2. DOI: https://doi.org/10.3390/app122111053.

[26] L. Almuqren et al, "Sine-Cosine-Adopted African Vultures Optimization with Ensemble Autoencoder-Based Intrusion Detection for Cybersecurity in CPS Environment," Sensors, vol. 23, (10), pp. 4804, 2023. Available: https://www.proquest.com/scholarly-journals/sine-cosine-adopted-african-vultures-optimization/docview/2819482554/se-2. DOI: https://doi.org/10.3390/s23104804.

[27] K. A. Alissa et al, "Feature Subset Selection Hybrid Deep Belief Network Based Cybersecurity Intrusion Detection Model," Electronics, vol. 11, (19), pp. 3077, 2022. Available: https://www.proquest.com/scholarly-journals/feature-subset-selection-hybrid-deep-belief/docview/2724230242/se-2. DOI: https://doi.org/10.3390/electronics11193077.

[28] A. Al-Malaise Al-Ghamdi S., M. Ragab and M. F. S. Sabir, "Enhanced Artificial Intelligence-based Cybersecurity Intrusion Detection for Higher Education Institutions," Computers, Materials, & Continua, vol. 72, (2), pp. 2895-2907, 2022. Available: https://www.proquest.com/scholarly-journals/enhanced-artificial-intelligence-based/docview/2646011103/se-2. DOI: https://doi.org/10.32604/cmc.2022.026405.

Websites

[29] https://www.newcastle.edu.au/research/cen

H. Hanafi *et al*, "IDSX-Attention: Intrusion detection system (IDS) based hybrid MADE-SDAE and LSTM-Attention mechanism," *International Journal of Advances in Intelligent Informatics*, vol. 9, *(1)*, pp. 121-135, 2023. Available: https://www.proquest.com/scholarly-journals/idsx-attention-intrusion-detection-system-ids/docview/2803350539/se-2. DOI: https://doi.org/10.26555/ijain.v9il.942.

[30] Z. Wang *et al*, "A Survey on Programmable Logic Controller Vulnerabilities, Attacks, Detections, and Forensics," *Processes*, vol. 11, *(3)*, pp. 918, 2023. Available: https://www.proquest.com/scholarly-journals/survey-on-programmable-logic-controller/docview/2791700076/se-2. DOI: https://doi.org/10.3390/pr11030918.

[31] T. K. Tala and N. Kaabouch, "A Comparative Analysis of Supervised and Unsupervised Models for Detecting Attacks on the Intrusion Detection Systems," *Information*, vol. 14, *(2)*, pp. 103, 2023. Available: https://www.proquest.com/scholarly-journals/comparative-analysis-supervised-unsupervised/docview/2779562123/se-2. DOI: https://doi.org/10.3390/info14020103.

[32] M. N. Alatawi *et al*, "Cyber Security against Intrusion Detection Using Ensemble-Based Approaches," *Security and Communication Networks*, vol. 2023, 2023. Available: https://www.proquest.com/scholarly-journals/cyber-security-against-intrusion-detection-using/docview/2779948244/se-2. DOI: https://doi.org/10.1155/2023/8048311.

[33] T. Kim, J. Kim and I. You, "An Anomaly Detection Method Based on Multiple LSTM-Autoencoder Models for In-Vehicle Network," *Electronics*, vol. 12, *(17)*, pp. 3543, 2023. Available: https://www.proquest.com/scholarly-journals/anomaly-detection-method-based-on-multiple-lstm/docview/2862245484/se-2. DOI: https://doi.org/10.3390/electronics12173543.

[34] Y. Wang *et al*, "A Combined Multi-Classification Network Intrusion Detection System Based on Feature Selection and Neural Network Improvement," *Applied Sciences*, vol. 13, *(14)*, pp. 8307, 2023. Available: https://www.proquest.com/scholarly-journals/combined-multi-classification-network-intrusion/docview/2842954273/se-2. DOI: https://doi.org/10.3390/app13148307.

[35] H. Yang *et al*, "SPE-ACGAN: A Resampling Approach for Class Imbalance Problem in Network Intrusion Detection Systems," *Electronics*, vol. 12, *(15)*, pp. 3323, 2023. Available: https://www.proquest.com/scholarly-journals/spe-acgan-resampling-approach-class-imbalance/docview/2849024208/se-2. DOI: https://doi.org/10.3390/electronics12153323.