Enhancing Intrusion Detection in Organizational Information Systems through AI-Powered Traffic Analysis

Valentyn Sobchuk[1,†], Serhii Gakhov[2,†], Yevhen Smoliev[2,†] and Halyna Haidur[2,*,†]

[1] *Taras Shevchenko National University of Kyiv, 60 Volodymyrska Str., Kyiv, 01033, Ukraine*

[2] *State University of Information and Communication Technologies, 7 Solomyanska, Str., Kyiv, 03110, Ukraine*

Abstract

In the current digitized world, the massive volumes of data present considerable challenges to cyber security for the information systems of organizations. The sophistication of attacks and anomalies has complicated the development of efficient methods for their detection. Traditional methods such as signature-based intrusion detection and anomaly-based intrusion detection methods have been commonly used to detect attacks and secure networks and information systems. However, the advent of artificial intelligence, especially machine learning and deep learning has presented encouraging outcomes in terms of enhancing speed, accuracy, and efficiency in intrusion detection. This secondary research explores how AI-powered intrusion detection methods are enhancing traffic analysis and anomaly detection to protect organizational information systems. Thus, the major aim of this research is to explore how AI-driven analysis and anomaly detection methods enhance intrusion detection in organizations. The study uses data from carefully selected recent studies on AI-based intrusion techniques, particularly Machine learning-based and deep learning-based intrusion detection methods. The search strategy retrieved 15 studies that were used for data collection. The findings of the study reveal that there is a great enhancement in accuracy and efficiency in traffic analysis and detection of anomalies when AI-based intrusion detection methods are used compared to traditional intrusion detection systems. There are however challenges such as the inability to catch multiple attacks simultaneously and therefore future research is recommended to address these challenges.

Keywords

Intrusion detection, intrusion detection systems, traffic analysis, artificial intelligence, machine learning, deep learning.

1. Introduction

In the contemporary digital age, where cyber threats are rampant, organizations face a constant battle against complex threats and intrusions and, therefore, require strong security measures to protect their valuable assets [1]. Research has identified intrusion detection as one of the robust measures that can be undertaken by organizations to safeguard their assets [2]. Intrusion detection is the process of checking and analyzing network traffic, systems, and the behavior of users to identify and respond to possible security breaches or cyber-attacks [2]. The major goal of intrusion detection is the identification of any unauthorized or malevolent happenings that may compromise the privacy, reliability, or accessibility of the company assets. Intrusion detection is vital in securing the information systems of companies because it guarantees consistent checking of network actions for unauthorized access, identification of breaches, control of data breaches, prevention of infections by malware, detection of intruder threats, prompt response to attacks, adherence to regulations, securing intellectual property, preservation of business continuity, and enhanced reputation and trust [1, 3].

Information Technology and Implementation (IT&I-2024), November 20-21, 2024, Kyiv, Ukraine

[*] Corresponding author.

[†] These authors contributed equally.

sobchuk@knu.ua (V. Sobchuk); gakhovsa@gmail.com (S. Gakhov); smolev99@mail.com (Y. Smoliev); gaydurg@mail.com (H. Haidur)

0000-0002-4002-8206 (V. Sobchuk); 0000-0001-9011-8210 (S. Gakhov); 0009-0006-6270-9148 (Y. Smoliev); 0000-0003-0591-3290 (H. Haidur)

Intrusion detection is implemented by tools called Intrusion Detection Systems (IDS). The most common systems are Network-based Intrusion Detection Systems (NIDS) and Host-based Intrusion Detection Systems (HIDS). The NIDS monitors network traffic, analyzing packets in real-time to spot any suspicious or malevolent actions, while the HIDS focuses on single hosts or endpoints, checking system logs, file integrity, and other host-specific attributes to identify any signs of compromise or unauthorized access [4]. Generally, IDS plays a vital role in the identification and response to potential security breaches to safeguard the information systems of an organization. The IDS can clear extant malware and spot social engineering attacks that manipulate users into disclosing delicate information [2].

While these traditional IDS have been the most used technique for discovering assaults and offering safety, the rise of Artificial Intelligence (AI), especially Machine Learning (ML), Deep Learning (DL), and ensemble learning, promises more efficient measures of detecting attacks through AI-powered or AI-based intrusion detection [1]. The AI-powered IDS utilizes ML algorithms to analyze network traffic and identify anomalous patterns. AI has proven to be beneficial in cyber security since it enhances the technologies used by organizations to combat cybercriminals and assists organizations in safeguarding their data and that of customers [5]. AI-powered intrusion detection can improve cybersecurity defense by offering early detection of advanced threats, real-time response, lower false positives, and adaptability. Thus, AI-powered traffic analysis would provide a transformative improvement to intrusion detection systems through the leveraging of advanced ML and DL methods. Through the analysis of network traffic patterns, AI algorithms would be able to promptly identify anomalous behaviors, locate possible threats, and distinguish between genuine and suspicious activities [2].

This work aims to conduct research on enhancing intrusion detection in organizational information systems through AI-powered Traffic Analysis. This secondary research will select and evaluate recent relevant literature to highlight how organizations are or can use AI-powered traffic analysis to enhance intrusion detection to safeguard their information systems. The paper will contain a literature review, methodology, results, discussion, recommendations, and conclusion sections.

Aims and Objectives

The major objective of this study is to determine how AI-driven analysis and anomaly detection methods enhance intrusion detection in organizations.

To achieve the objectives above, the specific objectives of the study will include:

To determine the various AI-powered intrusion detection methods currently used.

To compare and contrast the impact of various AI-based intrusion detection methods in enhancing traffic analysis and anomaly detection

To determine the challenges of using AI-driven intrusion detection methods as compared to traditional intrusion detection methods

To find possible solutions to overcome identified challenges

Literature Review

Overview of intrusion detection methods in organizational information systems

With the rising number of cyberattacks and intrusions, monitoring and protecting organizational networks and information systems has become more important. In the year 2021, the FBI's Internet Crime Complaint Centre (IC3) got over eight hundred thousand complaints concerning data breaches, malware, and many others [6]. The complaints totaled about 7 billion US dollars and those only represented the cases that were reported. For years, organizations have been using various traditional intrusion detection methods to protect their information systems and their clients' data. A review of literature from diverse sources has established numerous different types of IDS and 3 methods of intrusion detection.

Types of IDS

Although all IDS have the same purpose, their mode of function differs in various ways. Research has established that there are numerous types of IDS such as NIDS, HIDS, Network Node IDS (NNIDS), Perimeter IDS (PIDS), Virtual Machine-Based IDS (VMIDS), and Stack-Based IDS (SBIDS) among others [2, 4, 7, 8]. However, the two most common conventional IDS types used by organizations across the world:

Network Intrusion Detection System (NIDS)

The NIDS sanctions intrusion detection through the organization's whole network with the use of all packet metadata and contents to define threats (4). To use NIDS, it has to be installed on a piece of hardware within the organization's network infrastructure. After it has been installed, the NIDS will sample every packet that goes through it. NIDS are the most popular type of IDS because they can analyze all incoming and outgoing traffic, they detect actions in real-time which enables quicker responses, they are difficult to detect by intruders, and they can be placed strategically in critical locations (8). The major limitations of NIDS however, are hands-on maintenance and low specificity.

Host-Based Intrusion Detection System (HIDS)

The HIDS passes intrusion detection via a specific endpoint, checks network traffic to and from the machine, observes running processes, and inspects the system logs to and from a chosen device (4). However, the visibility of a HIDS is restricted to its host machine and this lowers the presented setting for decision-making even though it has deep visibility into the internals of the host computer. The major advantages of the HIDS are that it can be set up on computers or servers, it can identify the attacked device, it alerts the administrators when analytical files are tampered with, and it is specifically effective against insider threats (2, 7, 8). The proper usage of HIDS needs frequent monitoring.

Methods of Intrusion Detection

After gathering data, the IDS is intended to monitor network traffic and match traffic patterns to recognized assaults. Depending on the IDS type chosen by the organization, the security solution will depend on the following separate detection methods to keep the organizational network or information system safe:

Signature-Based Intrusion Detection (SIDS)

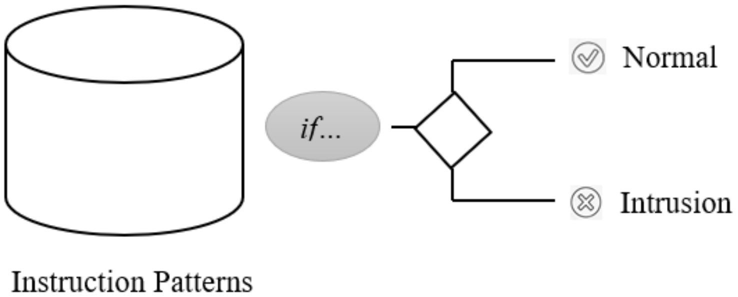


Figure 1: Conceptual working of SIDS approaches

This method of detection aims to detect patterns and compare them with established proof of intrusions. The SIDS method is dependent on a database of past intrusions (fig.1). If the activity within the organization's network matches the "signature" of an assault or breach from the database, the network administrator will be notified by the detection system [9]. The database is the mainstay of the SIDS and hence database updates are frequently required since the SIDS is only able to identify attacks that are recognizable to it. However, this is considered the key limitation of this method because if the company is targeted by a new intrusion method, no volume of updates on the database will safeguard it [10].

Anomaly-Based Intrusion Detection (AIDS)

Literature has established that the major advantage of AIDS over SIDS is that AIDS is able to identify those new zero-day intrusions. The AIDS method utilizes ML and statistical data to develop a model of "normal" behavior such that any traffic deviating from this normal behavior is flagged by the system as suspicious. [9] however argued that the major challenge with AIDS vs SIDS is the possibility for false positives. The author argued that at the end of the day, not all alterations are caused by malevolent happenings and that some are just signs of alterations in the conduct of the organization. However, since AIDS does not have a database of previous assaults for referencing, it may convey every anomaly as intrusions [10].

Hybrid Intrusion Detection

The hybrid detection method is a combination of SIDS and AIDS. The hybrid system looks at patterns and one-off events and flags new and extant intrusion strategies [11]. However, [10] points out that this system has the major limitation of an even bigger uptick in flagged issues. Despite that, taking into consideration that the goal of IDS is flagging possible infringements, it is difficult to view this rise in flags as a downside [9].

In summary, the SIDS uses a database of previous attacks as a reference to detect possible threats, the AIDS pinpoints new breaches such as new malware and adapts to them on the fly using ML, whereas hybrid IDS combines AIDS and SIDS to enlarge the scope of the intrusion detection.

Introduction to AI techniques for traffic analysis and anomaly detection

Traffic analysis has numerous purposes including assessing the performance and security of network processes and management [12]. Anomaly detection is important because inconsistencies in data are transferred to considerable, and usually crucial actionable information in a broad range of application spheres. The emergence of AI, especially ML and DL has provided more efficient measures of detecting attacks through AI-powered or AI-based intrusion detection [13, 14]. The AI-powered IDS utilizes ML algorithms to analyze network traffic and identify anomalous patterns. As contemporary threats and intrusions become more sophisticated than in the past, more and more experts are now recommending the use of AI-powered network traffic analysis and anomaly detection to solve the challenges of protecting devices and detecting intrusions into networks and information systems of organizations [1]. There are various AI techniques for analyzing traffic and detecting anomalies and these techniques have revolutionized how companies detect and respond to network security threats (fig. 2). [11] note that these AI techniques harness the power of ML and DL algorithms to scrutinize large volumes of networks in real time. For instance, ML algorithms like Support Vector Machines (SVM) and Random Forest are utilized in the identification of patterns in network traffic which enables deviations from "normal" behavior to be detected [5]. Similarly, DL models such as Recurrent Neural Networks (RNN) and Convolutional Neural Networks (CNN) are efficiently used to recognize sophisticated developing anomalies [15, 16]. According to [3], the idea behind the use of AI techniques such as ML algorithms is to make machines capable of learning by themselves and differentiate between normal and abnormal behavior in the system.

Case studies and research findings demonstrating the impact of AI in enhancing detection

Research findings indicate that many companies are now merging cybersecurity with AI or using AI-powered techniques to enhance the detection of intrusions and anomalies. For instance, Darktrace which is a company with over 30 offices across the world and headquartered in San Francisco, California has been using an AI platform that scrutinizes network data to make computations and identify patterns [17]. The data is utilized by ML algorithms incorporated in the platform to help companies identify threats and detect deviations from normal behavior. This company has reported that the use of AI-based traffic analysis for its clients has resulted in more than 40% reduction in false positives, hence increased accuracy and efficiency [17].

Blue Hexagon which is another company in Sunnyvale, California, was established on the assumption that DL will extremely transform cybersecurity and the company offers real-time network threat protection to its customers which provides anomaly detection within a second. The organization uses AI to create malware founded on universal threat data and the dark web and then uses this to test its systems and push its proficiencies to the utter limit. Studies conducted by the organization show that AI-powered algorithms are more efficient in detecting advanced threats that could be missed by conventional IDS methods [6].

Cybereason, a company based in Boston, Massachusetts, uses AI-powered detection technology to determine if an organization is under attack. The company uses a cybersecurity analytics platform to monitor, detect, and analyze threats. As a result, the company has been able to achieve early identification of intrusions and averted potential data breaches for the organizations it serves [6]. These and many other cases have demonstrated how AI has enhanced detection by increasing efficiency, improving accuracy, reducing costs, providing real-time threat detection and response, and improving scalability.

2. Methodology

This study employed a secondary research approach to examine how AI-powered traffic analysis enhances intrusion detection in organizational information systems. As secondary research, it entailed selecting and evaluating relevant sources of literature such as extant research, case studies, government publications, and industry reports in the area of cybersecurity and AI-powered intrusion detection

Search Strategy

Relevant databases including Google Scholar were electronically searched for studies published within the last 7 years. Further, the bibliographies of the identified studies were also examined for other relevant articles. The articles were limited to those published between January 2016 and July 2023. The search strategy involved the following search terms: enhanced intrusion detection, AI-powered intrusion detection, AI-based techniques for intrusion detection, AI-driven detection of anomalies, and AI-powered traffic analysis. The search terms were combined with Boolean operators. For studies to be included, they had to have been published in English. Therefore, the inclusion selection criteria were such that articles were only considered if they were primary studies, government documents, or industry reports, published in English, not older than 7 years, and contained information on AI-powered or AI-driven intrusion detection in organizations. Thus, the exclusion criteria involved articles not published in English, older than 7 years, not available in full text, and not relevant to the research topic.

Screening/Study Selection

The first phase of screening involved reviewing the titles and abstracts of the retrieved articles to determine eligibility. Secondly, the full texts of all the possibly relevant articles were obtained and reviewed against the selection criteria for final inclusion. All research journals, government documents, and government reports that reported on the use of AI in intrusion detection or the enhancement of intrusion detection using AI tools and techniques were included in the study. Duplicates were discarded.

Data Analysis

Data analysis was done using the thematic analysis method. This involved critically reviewing the data to identify patterns, inclinations, and trends that were coded and used to establish the key themes related to the use of AI to enhance intrusion detection in organizational information systems. The analysis and identification of patterns and trends focused on aspects such as the AI techniques and tools implemented, the benefits of using AI-based intrusion detection, case studies and examples of successful implementations, and the impact of AI on intrusion detection capabilities in organizations. The patterns in the data were then organized to form key themes that would later be interpreted in the results and discussion sections of the research. Research journals, industry reports, and case studies were all analyzed using the same thematic analysis method.

3. Results and Discussion

Overview of Research Findings

Security is a necessity for organizational information systems because of the extensive usage of data and the internet. In the previous sections of this report, it was established that one of the major goals of the IDS is detecting network packets through a critical inspection and reporting them to administrators by producing alarms. While numerous IDS have been in use, this research has been founded on the premise and hypothesis that AI-based intrusion detection offers an improved and attractive solution for traffic analysis and detection of anomalies. Hence, this study was conducted to verify this premise. The search strategy retrieved 15 relevant studies, published between 2016 and 2023. Data was extracted from this study based on the research objectives and analyzed using thematic analysis. The overview and discussion of the findings are provided in the following subsections.

AI Techniques and Impact

Machine Learning based intrusion detection methods

Findings indicate that cybersecurity utilizes ML algorithms to make numerous crucial calculations to stop breaches by dropping the data to evade cyber-attacks [1, 5, 18, 19, 20, 21]. The research findings indicate that ML has been established to be the most potent security instrument in the detection of assaults, and comprehending the semantic features of the systems appears vital for developing an IDS [1, 5, 21]. AI, especially ML techniques, considers the styles of learning to model the algorithm. The findings of this study indicate that ML provides majorly supervised and unsupervised algorithms for categorization depending on the available training data. The study by [1] provided detailed explanations of the two. They indicated that supervised learning is taught via teach-student associations where the training dataset teaches the target dataset and categorizes the labeled dataset. According to [1, 5], supervised learning produces accurate performance in classifying tasks in the detection of intrusion and it is one of the crucial models in the detection of anomaly. On the other hand, unsupervised learning handles unlabeled data and enables the use to classify the data on the basis of similarity. This form of learning is ideal for efficient analysis of undiscovered patterns [1, 5].

The most common supervised ML methods for intrusion detection include support vector machine (SVM), logistic regression, KNN algorithm, Bayesian, and Random forest algorithm [1, 5, 21]. This study has established that all these supervised ML methods provide a protected tool for detecting invaders in the cloud and also in networking. They contain a feature reduction and dimensionality reduction which offer an additional benefit in the detection and categorization of assaults. This finding aligns with the findings by [22] who concluded that the use of feature reduction and dimensionality reduction in supervised ML intrusion detection methods strengthens the mechanism for attack detection.

This study also found that the most common unsupervised ML techniques for intrusion detection include the Fuzzy C-means clustering algorithm and K-means clustering algorithm [1, 5, 18, 21]. The former allows data points to be allotted to one or more clusters and it aims to give higher classification accuracy and solidity when tried and trained with the KDD 99 Cup dataset whereas the latter splits the K unlabeled dataset into K clusters and allots a membership for evert data section to a cluster depending on the resemblances. A comparison between the two techniques conducted by [1] revealed that the K-means clustering method showed the best results as it attained a higher accuracy for classification. A further comparison between the supervised and the unsupervised ML intrusion detection methods performed by [1] showed that KNN is the best method for detecting intrusions as it provides an accuracy of 99.89% (fig. 3).

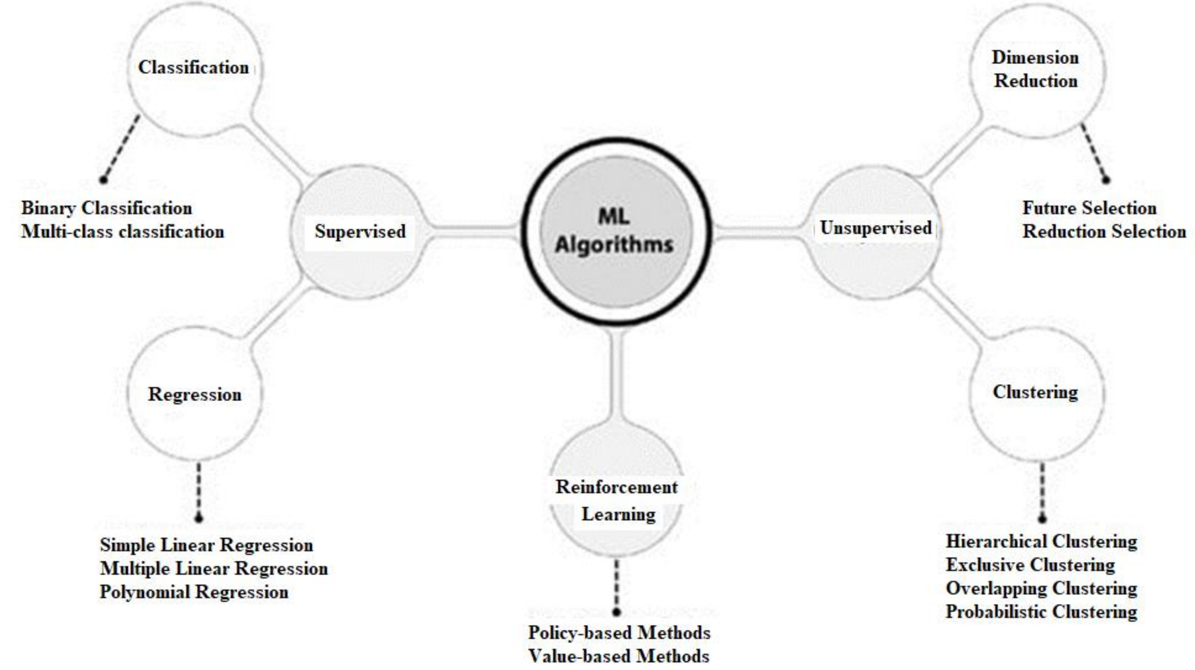


Figure 2: Machine Learning Algorithms

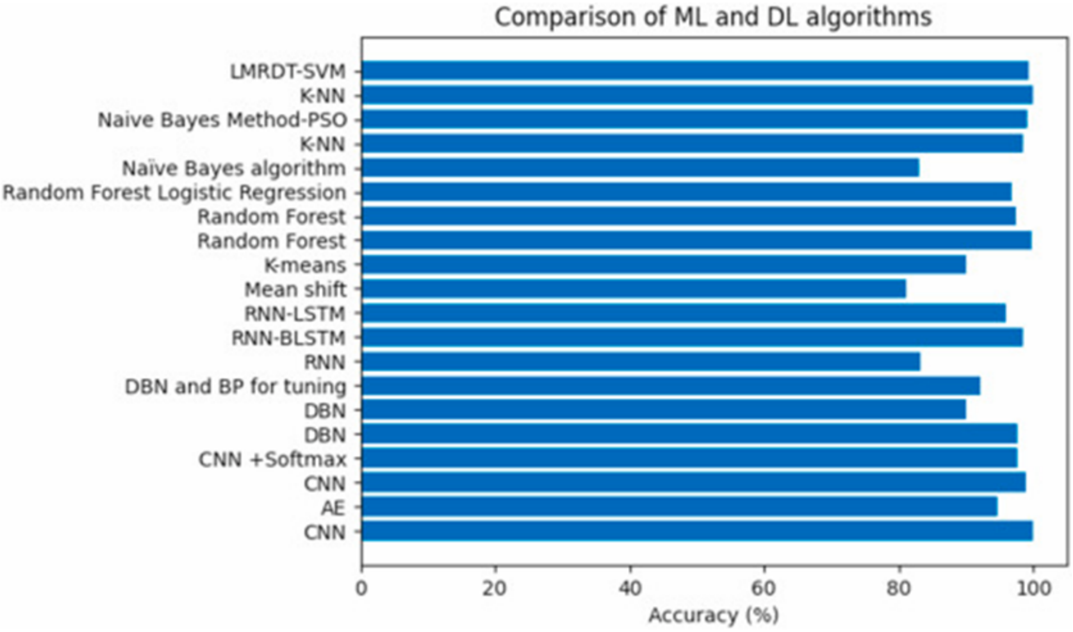


Figure 3: Comparison between DL and ML-based intrusion techniques in terms of accuracy performance

However, this research has established that although the KNN-supervised approach demonstrated superior accuracy, it is constrained to to a select set of attacks such as R2L, U2R, DoS, and Probe.

Deep Learning- based intrusion detection techniques

Deep Learning (DL) is a subsection of ML and it can be considered a sophisticated progression of ML algorithms [1, 11, 13, 15, 16, 23, 24, 25]. Literature has described DL as an enhanced form of ML that undertakes feature extraction and classification jobs with numerous successive layers in the absence of any human intervention [1]. The study by [24] in their survey on deep learning for anomaly detection, highlighted two important new categories of deep anomaly detection techniques. The first one was the Deep Hybrid Models (DHM) which utilize deep neural networks, especially autoencoders as feature extractors [1, 11, 16]. According to [16], the DHM utilizes the pre-trained transfer learning models as feature extractors with massive success. [24] established that the hybrid models provide greater scalability and computational efficiency compared to the traditional IDS because the linear or non-linear kernel models function on lowered input dimensions. [24] observed that while this AI technique enhances the detection of anomalies, its biggest limitation is that it does not have a trainable objective tailored for the detection of anomalies and hence is unable to extract rich differential features for the detection of outliers. The second technique was One-Class Neural Networks (OC-NN) which is motivated by kernel-based one-class classification that utilizes a combination of the deep networks' ability to mine an increasingly rich illustration of data with the one-class aim of developing a tight envelope around normal data [1, 16, 24]. The authors found this method to enhance the accuracy and efficiency of irregularity discovery and this finding was in agreement with the findings of previous studies like [26] and [27]. According to [24] one advantage of using the OC-NN deep learning detection intrusion technique is that this model is able to jointly train a deep neural network while enhancing a data-enclosing hypersphere or hyper-plane in output space (fig.3). However, the considerable disadvantage of this technique as established by [24] is that it takes long to train and update the models for greater dimensional input data. Studies have also highlighted other various deep anomaly detection techniques that are effective and promising such as transfer-learning-based anomaly detection, clustering-based anomaly detection, and deep reinforcement learning (DRL) based anomaly detection among others [11, 13, 15, 16].

The findings above were echoed by [25] who in their study on DL-based intrusion detection for IoT networks concluded that deep learning as a smart method solves the intrusion detection issue that is available for IoT networks. Previous studies have emphasized the importance of cyber security for IoT in contemporary information technology systems [28, 29, 30]. The studies also emphasized the necessity for the application of AI to promptly detect malicious attacks. The study by [25] has provided evidence indicating that the use of deep learning which is an AI is a smart technique that has enhanced the efficiency, speed, and accuracy of intrusion detection. However, despite this progress in using AI techniques to enhance intrusion detection for IoT networks, [19], following their survey ML-based intrusion detection methods observed that intrusion detection within the IoT setting is still a problem. The authors noted that despite the numerous positive outcomes realized from the application of AI techniques in the setting of security in information systems and IoT networks, particularly intrusion detection, the rate of false positives is still a challenge that further studies should address. According to [19], some AI techniques are able to lower the rate of false positives but, in contrast, increase the classification and training time. [19] observed that certain AI-based intrusion techniques stabilize the false positive rate but cause a high computational load for training and testing. This is a significant issue in intrusion detection as real-time identification of threats is a relevant factor.

AIDS was initially developed as an improved method to overcome the limitations of the SIDS such as requiring regular maintenance of the database. Recent developments, especially the introduction of AI have brought further improvements to the AIDS technique compared to how the technique has traditionally been utilized. In their study on IDS in a cloud environment, [3] assessed the improvements that have been made to the traditional methods of intrusion detection, particularly AIDS and SIDS. For instance, [3] reviewed the proposed AIDS technique in which AIDS uses a machine-learning technique based on static program behavior analysis. This technique has two stages. First, the programs are decoded and second, context-free grammar is created to represent the process flow. Two feature selection techniques- Information Gain (IG) and Document Frequency) are employed separately as suggested by [31]. Another AI-driven AIDS technique reviewed by [3] was the entropy-based IDS whose purpose is to detect unknown attacks in the cloud environment. The authors reported high accuracy levels for this technique, noting that with an accuracy rate of 98%, this method is able to detect intruders. However, they observed that the limitation of these methods is that they can only detect traffic attacks like DoS/DDoS and IP spoofing with no consideration for worms, viruses, and rootkits.

AI-driven AIDS

Further analysis by [3] based on an earlier primary study by [32] showed that combining fuzzy C-means with artificial neural networks (ANN) reduces false alarms and enhances IDS accuracy. In this technique, the huge database is broken down into groups that are then used in training the different ANN modules. The fuzzy segment is then utilized to bring together the outcomes of numerous ANNs. According to [3], the outcomes show that this approach is able to detect a broad array of hypervisor attacks with greater accuracy of detection and a reduced portion of false alarms.

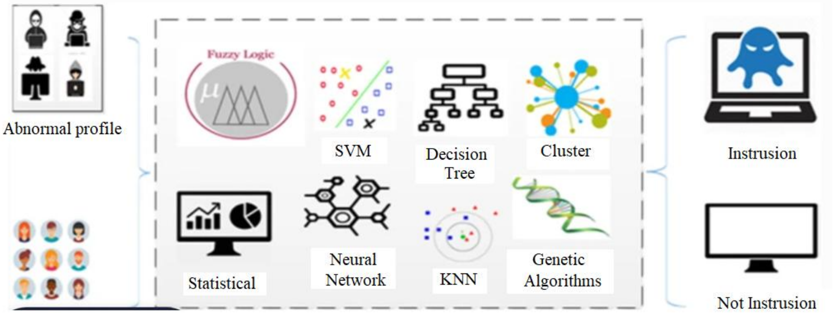


Figure 4: Conceptual working of AIDS based on ML

Challenges

The findings and discussion above indicate that AI is playing a vital role in intrusion detection by giving superior accuracy rates in IDS. However, analysis of findings despite enhancing intrusion detection, AI use presents several challenges, especially concerning the effective detection of multiple attacks. The study has found that AI-based intrusion detection approaches prioritize accuracy and fail to consider other essential performance metrics like F1 score, recall, FAR, and precision. Three key challenges presented by AI have been established in this study. The first challenge is catching multiple attacks. [1] and [11] explained that it is accurate to detect one assault with an AI-based IDS but it is difficult to detect numerous attacks simultaneously. The second challenge is poor performance caused by noisy data. [1] and [11] discovered that the freely accessible datasets for the detection of attacks are big and are likely to have noisy data which can harm the performance of the system [11]. The third challenge is failing to consider the influence of time intricacy and the use of CPU [32]. This study found that the majority of the AI frameworks ignore the influence of time intricacy and the use of CPU on the performance of the system.

Possible solutions

Detecting Multiple Attacks

The challenge of detecting multiple attacks simultaneously is a major concern in intrusion detection. Traditional AI-based IDSs often struggle to identify and differentiate between various types of attacks occurring concurrently. This limitation can be attributed to the complexity of attack patterns and the evolving nature of cyber threats. However, hybrid classification approaches can address this challenge by combining the strengths of different classification algorithms.

For instance, the study proposes a hybrid approach that combines K-means clustering and Adaptive Support Vector Machine (A-SVM) algorithms. The K-means algorithm clusters similar data points based on their behavior, while the A-SVM algorithm classifies the data into normal or anomalous categories. This hybrid approach leverages the clustering capabilities of K-means to group similar attacks together, making it easier for the A-SVM algorithm to identify and classify them.

Another approach combines Support Vector Machines (SVM) and k-Nearest Neighbor (k-NN) algorithms. The hybrid method leverages the strengths of both classifiers, where SVM is used for initial classification, and k-NN handles instances that are difficult to classify. This two-step approach improves detection rates and reduces false positives, offering a robust solution for handling large and complex datasets. A notable study demonstrated this by applying the hybrid method to the NSL-KDD dataset, a benchmark for IDS performance evaluation. The results showed that the hybrid model outperformed traditional methods and several recent hybrid approaches. The use of SVM provided a reliable initial classification, while k-NN further refined the classification of uncertain instances, leading to improved overall performance.

The goal is to create a hybrid intrusion detection system (IDS) that first uses SVM to classify data and then employs k-NN for refining uncertain classifications (fig. 5, 6).

Support Vector Machine (SVM)

Objective Function: Maximization of the margin between classes.

$$\min_{w,b} \frac{1}{2} \|w\|^2 \quad (1)$$

Subject to:

$$y_i(w \times x_i + b) \geq 1 \quad \forall_i \quad (2)$$

where w is the weight vector, b is the bias,x_i is the feature vector, and y_i is the label.

Classification of the data points using:

$$f(x) = sign(w \times x + b) \quad (3)$$

Definition of the margin for classification certainty:

$$\gamma = \frac{y_i(w \times x + b)}{\|w\|} \quad (4)$$

if γ < threshold pass the instance to k-NN.

k-Nearest Neighbors (k-NN)

Calculation of the distance between instances.

$$\mathrm{d}(x_i, x_j) = \sqrt{\sum_{k=1}^{n} (x_{ik} - x_{jk})^2}$$

Classification based on the majority label of the k-nearest neighbors.

$$\mathrm{f}(x) = mode(y_{k\_nearest})$$

Hybrid Algorithm

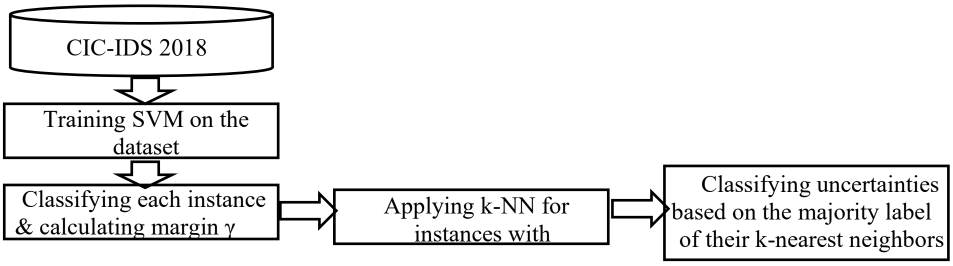
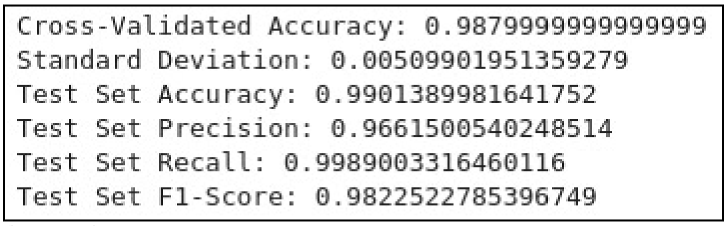

CIC-IDS 2018
Training SVM on the dataset
Classifying each instance & calculating margin γ
Applying k-NN for instances with
Classifying uncertainties based on the majority label of their k-nearest neighbors

Figure 5: An Enhanced Approach Combining SVM and k-NN



```
Cross-Validated Accuracy: 0.9879999999999999
Standard Deviation: 0.00509901951359279
Test Set Accuracy: 0.9901389981641752
Test Set Precision: 0.9661500540248514
Test Set Recall: 0.9989003316460116
Test Set F1-Score: 0.9822522785396749
```

Figure 6: Result achieved using the hybrid algorithm

Mitigating the Impact of Noisy Data

The presence of noisy data in intrusion detection datasets is another significant challenge. Noisy data can introduce errors and inconsistencies, leading to inaccurate classifications and reduced system performance. Hybrid classification approaches can mitigate the impact of noisy data by incorporating data preprocessing and feature selection techniques.

In the study, a hybrid IDS system is proposed that integrates nature-inspired algorithms and machine learning approaches. The system employs a Genetic Algorithm (GA) for feature selection, which helps to identify and remove irrelevant or noisy features from the dataset. By focusing on the most informative features, the system can improve its classification accuracy and robustness against noisy data. Additionally, the use of Discrete Wavelet Transform (DWT) with Artificial Bee Colony (ABC) further refines the data by dividing it into categories and filtering out irrelevant features.

Addressing Time Complexity and CPU Usage

The disregard for time complexity and CPU usage in AI frameworks is a critical challenge that can hinder the real-time performance of intrusion detection systems. Hybrid classification approaches can address this challenge by incorporating optimization techniques and efficient algorithms.

For example, the study explores different hybrid classification techniques using the Gray Wolf Optimizer (GWO) algorithm. The GWO algorithm is a nature-inspired optimization technique that mimics the leadership hierarchy and hunting mechanism of gray wolves. By incorporating the GWO algorithm, the hybrid classification approaches can optimize the feature selection process and improve the efficiency of the classifiers, thereby reducing time complexity and CPU usage.

4. Conclusions

Intrusion detection has been identified as one of the robust measures that can be undertaken by organizations to safeguard their assets. AI has proven to be beneficial in cyber security since it enhances the technologies used by organizations to combat cybercriminals and assists organizations in safeguarding their data and that of customers. This paper aimed to determine how AI-driven analysis and anomaly detection enhances intrusion detection in organizations.

A literature review was conducted that analyzed the existing findings on intrusion detection methods in organizational information systems, the types of IDS and methods of intrusion detection, the AI techniques currently in use for traffic analysis and anomaly detection, and case studies that show the impact of AI in enhancing intrusion detection. A secondary research methodology was used to find articles that were used to complete the study. Data from the articles was analyzed using thematic analysis. The findings established and categorized the AI-driven intrusion methods into four major groups namely- ML-based methods, DL-based methods, and AI-driven AIDS. The research findings indicate that ML has been proven to be the most potent security instrument in the detection of attacks.

ML-based techniques have been found to have enhanced accuracy in detection, with KNN in particular achieving a 99.89% accuracy rate. DL-based methods are enhanced forms of ML-based intrusion detection and hence are more efficient and more accurate in providing timely analysis of traffic and detection of anomalies.

AI-based AIDS is better than traditional AIDS as it is able to detect a broad array of hypervisor attacks with greater accuracy of detection and a reduced portion of false alarms. The study also found three key challenges presented by the use of AI-based intrusion detection methods. They include catching multiple attacks, poor performance caused by noisy data, and failing to consider the effect of time complexity and utilization of CPU. Hybrid classification approaches offer promising solutions to overcome the challenges faced by AI-based intrusion detection systems.

By combining the strengths of different classification algorithms, incorporating data preprocessing and feature selection techniques, and addressing time complexity and CPU usage, these approaches can enhance the accuracy, robustness, and real-time performance of IDSs.

5. Declaration of Competing Interests

The author declares that to the best of their knowledge, there are no competing personal associations or monetary interests that could have appeared to influence the work reported in this study.

6. Funding

This work was fully funded by the author and received no external funding.

Declaration on Generative AI

The authors have not employed any Generative AI tools.

References

[1] Sowmya, T. and Anita, E.M., (2023). A comprehensive review of AI-based intrusion detection system. Measurement: Sensors, p.100827.

[2] Yeo, L.H., Che, X. and Lakkaraju, S., (2017). Understanding modern intrusion detection systems: a survey. arXiv preprint arXiv:1708.07174.

[3] Lata, S. and Singh, D., (2022). Intrusion detection system in cloud environment: Literature survey & future research directions. International Journal of Information Management Data Insights, 2 (2), p.100134.

[4] Singh, A.P. and Singh, M.D., (2014). Analysis of host-based and network-based intrusion detection systems. International Journal of Computer Network and Information Security, 6(8), pp. 41-47.

[5] Verma, A. and Ranga, V., (2020). Machine learning based intrusion detection systems for IoT applications. Wireless Personal Communications, 111, pp. 2287-2310.

[6] Sajid, H., (2023). AI in cybersecurity: 5 crucial applications. https://www.v7labs.com/blog/ai-in-cybersecurity

[7] Bridges, R.A., Glass-Vanderlan, T.R., Iannacone, M.D., Vincent, M.S. and Chen, Q., (2019). A survey of intrusion detection systems leveraging host data. ACM Computing Surveys (CSUR), 52 (6), pp. 1-35.

[8] Liu, M., Xue, Z., Xu, X., Zhong, C. and Chen, J., (2018). Host-based intrusion detection system with system calls: Review and future trends. ACM Computing Surveys (CSUR), 51(5), pp. 1-36.

[9] Ahmed, M., Mahmood, A.N. and Hu, J., 2016. A survey of network anomaly detection techniques. Journal of Network and Computer Applications, 60, pp. 19-31.

[10] Cahyo, A.N., Sari, A.K. and Riasetiawan, M., 2020, October. Comparison of hybrid intrusion detection system. In 2020 12th International Conference on Information Technology and Electrical Engineering (ICITEE) pp. 92-97.

[11] Khraisat, A., Gondal, I., Vamplew, P. and Kamruzzaman, J., (2019). Survey of intrusion detection systems: techniques, datasets, and challenges. Cybersecurity, 2(1), pp. 1-22.

[12] Alqudah, N. and Yaseen, Q., (2020). Machine learning for traffic analysis: a review. Procedia Computer Science, 170, pp. 911-916.

[13] Bakshi, A. and Sunanda, (2019). A comparative analysis of different intrusion detection techniques in cloud computing. In Advanced Informatics for Computing Research: Second International Conference, ICAICR 2018, Shimla, India, July 14–15, 2018, Revised Selected Papers, Part II 2 pp. 358-378. Springer Singapore.

[14] Deepa, V. and Radha, N., (2021). A Survey on Network Intrusion System Attacks Classification Using Machine Learning Techniques. In IOP Conference Series: Materials Science and Engineering.Vol. 1022, No. 1, p. 012036. IOP Publishing.

[15] Javaid, A., Niyaz, Q., Sun, W. and Alam, M., 2016, May. A deep learning approach for network intrusion detection system. In Proceedings of the 9th EAI International Conference on Bio-inspired Information and Communications Technologies (formerly BIONETICS) pp. 21-26.

[16] Lifandali, O. and Abghour, N., 2021, December. Deep learning methods applied to intrusion detection: survey, taxonomy, and challenges. In 2021 International Conference on Decision Aid Sciences and Application (DASA) pp. 1035-1044.

[17] Ramaswamy, S., (2017). How companies are already using AI. https://hbr.org/2017/04/how-companies-are-already-using-ai

[18] Amouri, A., Alaparthy, V.T. and Morgera, S.D., (2020). A machine learning based intrusion detection system for mobile Internet of Things. Sensors, 20 (2), p. 461.

[19] Da Costa, K.A., Papa, J.P., Lisboa, C.O., Munoz, R. and de Albuquerque, V.H.C., (2019). Internet of Things: A survey on machine learning-based intrusion detection approaches. Computer Networks, 151, pp. 147-157.

[20] Islam, N., Farhin, F., Sultana, I., Kaiser, M.S., Rahman, M.S., Mahmud, M., SanwarHosen, A.S.M. and Cho, G.H., (2021). Towards Machine Learning Based Intrusion Detection in IoT Networks. Computers, Materials & Continua, 69 (2).

[21] Jamalipour, A. and Murali, S., (2021). A taxonomy of machine-learning-based intrusion detection systems for the internet of things: A survey. IEEE Internet of Things Journal, 9(12), pp.9444-9466.

[22] Lin, W.C., Ke, S.W. and Tsai, C.F., (2015). CANN: An intrusion detection system based on combining cluster centers and nearest neighbors. Knowledge-based systems, 78, pp. 13-21.

[23] Awajan, A., (2023). A novel deep learning-based intrusion detection system for IOT networks. Computers, 12(2), p. 34.

[24] Chalapathy, R. and Chawla, S., (2019). Deep learning for anomaly detection: A survey. arXiv preprint arXiv:1901.03407.

[25] Ge, M., Fu, X., Syed, N., Baig, Z., Teo, G. and Robles-Kelly, A., 2019, December. Deep learning-based intrusion detection for IoT networks. In 2019 IEEE 24th pacific rim international symposium on dependable computing (PRDC) pp. 256-25609.

[26] Ruff, L., Vandermeulen, R., Goernitz, N., Deecke, L., Siddiqui, S.A., Binder, A., Müller, E. and Kloft, M., 2018, July. Deep one-class classification. In International conference on machine learning. pp. 4393-4402. PMLR.

[27] Chalapathy, R., Menon, A. K., & Chawla, S. (2018). Anomaly detection using one-class neural networks. arXiv preprint arXiv:1802.06360.

[28] Fischer, E.A., 2014. Cybersecurity issues and challenges: In brief.

[29] Salam, A. and Salam, A., (2020). Internet of things for sustainability: perspectives in privacy, cybersecurity, and future trends. Internet of Things for sustainable community development: Wireless communications, sensing, and systems, pp. 299-327.

[30] Usmonov, B., Evsutin, O., Iskhakov, A., Shelupanov, A., Iskhakova, A. and Meshcheryakov, R., 2017, November. The cybersecurity in development of IoT embedded technologies. In 2017 International Conference on Information Science and Communications Technologies (ICISCT) pp. 1-4.

[31] Wu, H., 2019. Towards integrating learning algorithms into computer system design (Doctoral dissertation, UNSW Sydney).

[32] Pandeeswari, N. and Kumar, G., 2016. Anomaly detection system in cloud environment using fuzzy clustering-based ANN. Mobile Networks and Applications, 21, pp. 494-505.

[33] Shone, N., Ngoc, T.N., Phai, V.D. and Shi, Q., 2018. A deep learning approach to network intrusion detection. IEEE transactions on emerging topics in computational intelligence, 2 (1), pp. 41-50.

[34] Jasmeen K. Chahal, Amanjot Kaur, "A Hybrid Approach based on Classification and Clustering for Intrusion Detection System", International Journal of Mathematical Sciences and Computing(IJMSC), Vol.2, No.4, pp.34-40, 2016.DOI: 10.5815/ijmsc.2016.04.04.

[35] Singh, Abhishek & Singh, Maheep & Berwal, Krishan. (2021). A Hybrid Method for Intrusion Detection Using SVM and k-NN. 10.1007/978-3-030-67187-7_13.

[36] Kajal, A., Nandal, S.K. (2020). A hybrid approach for cyber security: improved intrusion detection system using Ann-Svm. Indian J. Comput. Sci Eng 11(4), 412–425.

[37] Durgesh Srivastava, Rajeshwar Singh and Vikram Singh, (2019). "Analysis of different Hybrid methods for Intrusion Detection System," International Journal Of Computer Sciences And Engineering 7(5):757-764, May 2019.