WORLD COMET RESEARCH GROUP

International Journal of Applied Data Science & Modern Computing
Vol. 4, No. 2, 2021
Doi: 10.67228/30713498/IJADSMC-2021PII5L7Z
PP. 01-15

Original Article

AI-Driven Cyber Defense Systems Using Real-Time Analytics

Dr. Chinedu Eze

Department of Electrical Engineering, Enugu Technical University, Nigeria.

Received: 06-05-2021 Revised: 06-26-2021 Accepted: 07-01-2021 Published: 07-04-2021

ABSTRACT

The rapid digitization of critical infrastructure, businesses, and government services has expanded the cyber-attack surface, making traditional security mechanisms increasingly ineffective. AI-based cyber defense systems powered by real-time analytics provide a proactive and adaptive approach to cybersecurity by integrating machine learning, deep learning, and intelligent threat detection techniques. This study examines the architecture, analytical frameworks, and operational processes of AI-driven cyber defense solutions capable of detecting known and unknown threats, including zero-day attacks and advanced persistent threats (APTs). The proposed framework incorporates continuous monitoring, streaming analytics, anomaly detection, behavioral analysis, and automated response mechanisms. Performance is evaluated using metrics such as detection accuracy, false positive rate, response time, and scalability. The findings indicate that AI-powered cyber defense significantly enhances threat detection, reduces response time, and improves overall cyber resilience compared to traditional security models, highlighting its critical role in next-generation cybersecurity infrastructures.

KEYWORDS

Artificial Intelligence, Cyber Defense, Real-Time Analytics, Machine Learning, Intrusion Detection Systems, Cybersecurity.

ISSN: 3071-3498
PP: 01-15.

1.INTRODUCTION

1.1. Background

The blistering growth of interrelated digital platforms, such as cloud computing services, Internet of Things (IoT) gadgets, and industrial control systems, has redefined the contemporary cyber threat environment to a great extent. Companies in industries are increasingly enhancing on intricate digital infrastructures to facilitate mission-driven services, business continuity, and guided decision-making, which has highlighted the urgency of cybersecurity to a strategic goal. Meanwhile, increasing scale, diversity, and interconnectivity of systems have presented fresh vulnerabilities that can be leveraged by enemy opponents who are getting more sophisticated. Traditionally used security systems, which include firewalls, anti-virus packages, and even hard-coded intrusion detection systems are mostly reactive and they also depend on predefined rules or known attack signatures. Although effective in countering the previously known type of threat, they are unable to identify new and obfuscated and quickly innovating attack methods, which leads to a lack of timely responses and exposes a person to cyberattacks. A solution to these shortcomings is through artificial intelligence (AI) which allows security systems to learn using a large amount of data, identify trends including complex ones, and dynamically adjust to new threats. The models that are based on AI may analyze different security data streams such as user behavior, temporal logs, and traffic on a network to extract indicative features of unusual activity that might be overlooked by conventional techniques. Combined with real-time analytics, AI-driven cyber defense information systems have the capability to handle data streams at elevated velocity and react to possible dangers with the lowest level of human involvement. This feature is particularly important in response to a zero-day assault correlatively advanced persistent threats, which are developed to bypass signature detection and to stay unnoticed a long time. In turn, the integration of AI and real-time analytics is a desirable and strong direction in cybersecurity, which prompts the creation of intelligent, adaptive, and active cyber defense.

1.2. AI-Driven Cyber Defense Systems

The crimes of the AI-powered system of cyber defense can be discussed as an important breakthrough compared to the conventional systems of cyber defense because AI-based technology uses smart algorithms to deal with cyber threats proactively and dynamically. Such systems apply machine learning, deep learning, and data analytics to handle large amounts of security information and make informed decisions with just a small amount of human intervention.

1.2.1. Concept and Evolution

The history of AI-assisted cyber defensive systems has developed out of primitive rule-based and statistical protection to intelligent and data-driven systems that are capable of learning the intricate patterns of threats. Contrary to conventional systems that rely on fixed signatures, AI-based solutions are dynamic in that they learn on past and current data that enable them to culminate the changing attack methods. This was enabled by both the rising access to large-scale security data and by computational capabilities.

ISSN: 3071-3498
PP: 01-15.

Fig 1 - AI-Driven Cyber Defense Systems

1.2.2. Core Components of AI-Driven Defense

A cyber defense system powered by AI usually comprises of data acquisition pipelines, feature engineering pipelines, AI-driven detection pipelines, and automated response pipelines. Information derived is gathered across a variety of different sources such as networks, endpoints, and applications and is converted to structured forms that can be analyzed in the model. Detection models process these features to give out the malicious activities whereas the response modules take the mitigation measures that are based on the assessment of risks and policy guidelines.

1.2.3. Learning and Adaptability

One of the strengths of AI-based cyber defense systems is that they learn and improve as time goes by. The supervised learning models use labeled data to identify known threats, whereas unsupervised and semi-supervised models classify anomalies and unrecognized attack patterns. Continuous learning processes also allow the models to reconfigure themselves on the basis of additional observations, preventing concept drift and making them effective in the long-term.

1.2.4. Real-Time Threat Detection and Response

With the combination of AI and real-time analytics, these systems will be able to process data streams with high velocity, identify threats in real-time. Automated and semi-automated response opportunities, minimize the reaction time and also the possible harm of attacks. The real-time feature is effectively required in countering advanced persistent attacks as well as zero-day attacks.

1.2.5. Advantages over Traditional Security Systems

The AI-based security defense systems are more accurate in the detection, less likely to generate a false positive, more scalable, and less prone to the changing threats than the traditional security systems. Their reactive and proactive character makes them ideal in defending the contemporary and intricate digital environments.

ISSN: 3071-3498
PP: 01-15.

1.3. Defense Systems Using Real-Time Analytics

Real-time analytics based defense systems have become an inseparable part of the contemporary cybersecurity policy as cyber threats grow in speed, scale, and complexity. Whereas, traditional security systems are usually based on offline or batch analysis where they create delay between occurrence and detection of a threat to the system, hence giving attackers a chance to take time identifying weaknesses that they can use to their advantage. Real-time analytics on the contrary, will satisfy constant surveillance and immediate examination of information as it is created to enable security systems to recognize and respond to malicious activists with minimum delay. Real-time analytics creates situational awareness about the current conditions and aids in quickly making decisions in a dynamic environment by incorporating high-velocity data volumes of network traffic, system logs, applications and endpoint devices. The real time cyber defense systems are based on stream processing frameworks, which are designed to process in bulk (large size) volumes of heterogeneous data with low processing delays. These systems impose analytical methods to live data streams like statistical monitoring, rule based filtering and anomaly detection, which allows suspicious behavior to be detected early. When implemented with artificial intelligence and machine learning models, real-time analytics help to improve the system to identify complex attack patterns, perform correlation between events in multiple sources and prioritize threats that are more risky and relevant. This integration enables organizations to stop responding to incidents reactively and instead start to implement mitigation of threats proactively. Additionally, real-time analytics can aid in automated and adaptive response systems that are essential to reduce the effect of a fast-moving attack like a distributed denial-of-service (DDoS) attack and a ransomware outbreak. When a threat has been identified, the instant measures such as the generation of alerts, blockage of traffic, or isolation of the system have been instigated. Although there are benefits associated with deployment of real-time analytics-based defense system, they are subject to issues relating to scalability, data quality and maintenance of models. However, their capability to deliver promptly detected data, increased visibility, and quick response builds real-time analytics to be a benchmark of a strong and resilient cyber protection mechanism.

2. LITERATURE SURVEY

2.1. Traditional Cyber Defense Approaches

The conventional cyber defense models have mainly been heterogeneous to signature detection and expert systems rule-based techniques to detect malicious activities. This type of method works by comparing the acting traffic or system activity with a pre-coded database containing known attack signatures or handwritten rules. Although they excel at high precision in detecting threats already known, these kinds of systems are not useful at detecting zero-day attacks, polymorphic malware, and advanced persistent threats (APTs). In addition, the current signature databases also necessitate a lot of manual handover, which increases their cost of operations and responsiveness to the emergent threats. Since the tactics to perpetrate cyberattacks keep rapidly changing, the traditional practices of maintaining a static and reactive platform makes the traditional framework highly ineffective in addressing dynamically emerging challenges.

ISSN: 3071-3498
PP: 01-15.

2.2. Machine Learning in Cybersecurity

Such cybersecurity innovation as machine learning (ML) methods has created the approach to identify and analyze threats based on the data. The Well-known algorithms include those like decision trees, support vector machines (SVMs), k-nearest neighbors (KNN), and clustering algorithms which have been used in a variety of tasks including intrusion detection, malware classification and spam filtering. An excellent detection rate and a low false-positive rate can be obtained with supervised learning model when it is trained on high-quality labeled datasets. Conversely, the unsupervised procedures are useful especially when anomaly detection of behavior is required in a slightly limited or unstable labeled environment. In spite of these benefits, most ML-based cybersecurity efforts are done in offline or batch processing modes, which limit their capabilities to respond to threats. Also, their performance usually suffers as they are subjected to changing attack patterns indicating the need to have adaptive learning mechanisms.

2.3. Deep Learning and Behavioral Analysis

Achievement in deep learning in the recent past has greatly overpowered the ability of the cybersecurity system to model the multifaceted and high-dimension data. Convolutional neural networks (CNNs) and recurrent neural networks (RNNs) and long short-term memory (LSTM) networks are both very useful in extracting spatial and temporal features of a network traffic representation and system logs and user behavior traces respectively. Security approaches based on behavior rely on these models to train baseline pattern of normal activity by the system and detect deviations which may elicit an attack. Even though deep learning methods can usually outperform the performance of classical ML models in terms of detection, these methods are associated with the difficulties of high computational costs and long training, as well as, poor interpretability. Deep models have a tendency to be opaque and therefore not a useful component to trust and deploy in security-sensitive settings where it is necessary to be explainable.

2.4. Real-Time Analytics for Cyber Defense

Real-time analytics have become the important part of the contemporary cyber protection infrastructure allowing to track and analyze the data streams provided by networks, endpoint, and applications in real-time. Stream processing systems enable ingestment and processing of large quantities of data with low latency enabling the security team to detect and respond to threats in real time. Artificial intelligence integration and real-time analytics can improve the situation awareness of the system as it will help the system to identify threats automatically and prioritize and respond to them. It has been shown that these systems dramatically decrease the detection latency, as well as enhancing incident response times. Nevertheless, real-time AI-driven cyber defense system implementation faces scalability issues, scaling and dealing with the high-velocity nature of data streams, as well as the quality of their data and the drift of their models, due to changes in how the system operates and attack behavior.

ISSN: 3071-3498
PP: 01-15.

2.5. Research Gaps

Though there are important progresses in AI-based cybersecurity solutions, it can be seen that multiple challenges have not been resolved that are discussed in the literature. Current methods have concentrated on individual elements, including detection accuracy or model performance, but do not relate it to end-to-end incorporation into real-time operational environments. It is already evident that there is a dire requirement of standardized frameworks capable of integrating AI-based detection models with scalable operation time analytics pipelines. Also, the problems of flexibility to changing threats, effective use of resources and constant updating of the models are underdeveloped. Most of present systems are not able to balance accuracy, latency, and interpretability when deploying large-scale systems. To ensure that these gaps are closed, the present paper suggests an extensive AI-based approach to cyber defense that places focus on the notion of threat detection in real time, scalability, and efficiency of running it in dynamic cyber settings.

3. METHODOLOGY

3.1. System Architecture Overview

The designed AI-based cyber defense is created as a stacked structure, which will unite data collection, real-time processing, intelligent detection and automated reaction measures. The modular architecture provides the scalability, fault tolerance and the ease of integration with other security infrastructures. The functional layers have a clear functional role in integration with the other functional layers to facilitate a seamless integration between the end-to-end and real-time cyber defensive functions.

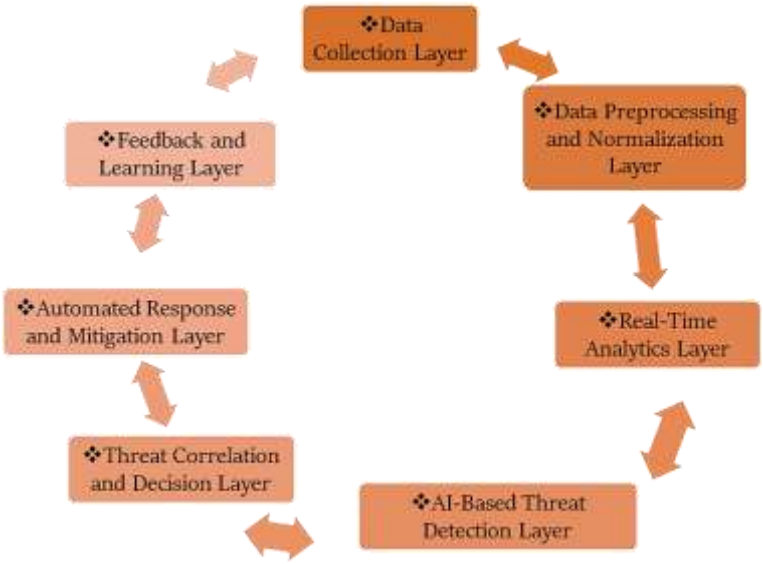

Fig 2 - System Architecture Overview

3.1.1. Data Collection Layer

The data collection layer will have the task of collecting raw security-related information in different sources throughout the cyber environment. These data sources are network traffic flows,

ISSN: 3071-3498
PP: 01-15.

system and application logs, endpoint telemetry, logs of user activities, and security devices like firewalls and intrusion detectors devices. Lightweight agents or sensors or log forwarders continuously gather data in real time to ensure minimal overheads to the performance. The layer provides a complete visibility of system activities and data integrity and consistency to further downstream processing.

3.1.2. Data Preprocessing and Normalization Layer

The raw data collected are then preprocessed before analysis to exclude the noise, manage the missing data and standardize data formats. This layer is used to carry out activities like feature extraction, data aggregation, matching of the timestamps, and normalization of the inputs to transform heterogeneous inputs into a homogenous representation. Proper preprocessing leads to the fact that in further stages, the accuracy of models and the complexity of calculations are enhanced. Using data to generate organized and meaningful characteristics, this layer suits the input of real-time analytics and AI-based detectives.

3.1.3. Real-Time Analytics Layer

The real-time analytics layer uses stream-processing frameworks to process incoming streams of data, making it possible to be analyzed in low latency. This layer facilitates the continuous observation with the help of statistical analysis and rule based filtering of lightweight anomaly detection methods on live data. It guarantees quick detection of suspicious trends and scores events to be further investigated by AI models. This layer is critical due to the possibility of detecting threats and situational awareness in time, as it is operated by high speed of data velocity and data volume.

3.1.4. AI-Based Threat Detection Layer

The fundamental component of the system is the AI based threat detection layer which makes use of machine learning and deep learning models to detect cyber threats. On the one hand, supervised models will give a classification of already known attack patterns and on the other hand, unsupervised and semi-supervised will identify anomalous behavioral patterns that may be indicative of an unknown attack or a zero-day attack. They use deep learning architecture, e.g., CNN and LSTM, to learn spatial and temporal correlations in network traffic and system logs. This localized detection technique combines a high accuracy of detection and flexibility performance in dynamic threats environment.

3.1.5. Threat Correlation and Decision Layer

The threat correlation and decision layer takes the results of a variety of detection models and analytics modules to produce a single combination of threat ratings. This layer suppresses false positives by correlating alerts achieved by various sources of data and time windows to enhance the certainty of the success of detection outcomes. The weight of the risk scoring and contextual information is used to formulate logic of decision-making to identify the severity and priority of

ISSN: 3071-3498
PP: 01-15.

detected threats. This layer is an interface in between detection and response to provide informed and consistent defense measures.

3.1.6. Automated Response and Mitigation Layer

The adaptive or predefined counter measures are initiated through the automated response layer in accordance to threats and threat levels observed. These can be efforts to isolate infected endpoints, block rogue IP addresses, kill suspicious processes or send alerts to security operators. Automation will minimize the time to respond, and minimize the effects of any attack. Human-in-the-loop mechanisms are also provided by the system, and the actions could be reviewed by the analysts and overruled, when needed.

3.1.7. Feedback and Learning Layer

The feedback and learning layer allows the ongoing improvement of the system based on the feedback of the result of the response and decision of the analysts. The results of detection and labeled incidents are used to feed back into the learning loop to retrain and refresh AI models, correcting the drift in models and the changes in the attack patterns. This will be possible in terms of adaptive learning which will see to it that the system will be effective in the long run and it will be able to withstand any emerging threats.

3.2. Data Acquisition and Preprocessing

Data gathering and preprocessing is a vital basic of the proposed AI-based system of cyber defense because the performance of the further stages of analytical processing and detection is strictly related to quality and relevance of processing data. A vast array of very diverse sources of security-related data are constantly accessed such as network traffic captures, logs of firewall and intrusion detection systems, operating system and application logs, endpoint detection sensors, and third-party threat intelligence feeds. These types of data sources give a full picture of the network behavior and the host behavior providing a complete view of the network activities and host activities respectively. Data ingestion mechanisms to operate in diverse scenarios To assist in the real-time operation, a data ingestion framework is developed to address the high-velocity and high-volume streams without impacting data integrity and low-latency. After gathering them, raw data are preprocessed significantly to get them in a machine-readable form organized as a structured, user-analysable format by the artificial intelligence-powered analytics. The techniques used to reduce noise are aimed at removing redundant, irrelevant records or any error records that can come up as a result of logging inconsistencies or other benign system processes. Normalization and standardization of the data are conducted to get similarity between the features produced by other sources and avoid bias in model training and inference. The process of feature extraction is very important in highlighting informative characteristics, including statistics of traffic flows, temporal features, sequence of system calls and indicators of user behavior that are very vital in drawing a line between normal and suspicious activities. Dimensionality reduction is also used to reduce the number of calculations necessary to maintain important information so as to make the systems more efficient and scalable.

ISSN: 3071-3498
PP: 01-15.

Principal component analysis (PCA), autoencoders, feature selection algorithms, among other methods, reduce the feature space and eliminate redundancy and emphasize the most discriminative features. The step both enhances model performance and training speed as well as alleviates the overfitting risk. In general, the data acquisition and preprocessing pipeline will guarantee the delivery of quality, relevant, and timely data to the AI models to facilitate the detection of cyber threats accurately, more scalably, and in real-time.

3.3. Feature Engineering

Another central phase of the suggested AI-based cyber defense solution is feature engineering because the quality and representativeness of extracted features have a direct proportional effect on the accuracy and strength of threat detection models. The feature engineering in this system works on the transformation of the raw security data into useful numerical representations, which are effective in capturing the system and network behavior. A wide range of features is obtained that can sensor statistical, temporal and behavioral characteristics of activities being monitored. Data distributions and traffic characteristics are summarized statistically by numbers of packets, rate of bytes, duration of connections, frequency of access attempts, etc. and they assist in finding abnormal usage patterns. Temporal characteristics record time-varying patterns, e.g., inter-arrival time, durations of a session, periodicity, and abrupt largest activity, which allow detecting stealthy or slow activities. Features of behavior model both normal and abnormal patterns of user and system behavior, based on analyzing sequences of actions, resource usage profiles, and system call patterns. The capabilities are especially useful to address insider threats, compromised accounts, and more advanced persistent threats that could not be detected by signature-based detection. Through the amalgamation of various categories of features, the system can have a holistic and multi-dimensional picture of cyber activities which would enhance its capability of differentiating between friendly and hostile actions. The output feature representation is represented as a feature vector because of which X = a list of features x one, x two, all the way through to x n, each feature x i represents a single extracted feature as relevant to threat detection. This representation is a vectorized and thus it can be fed into the machine learning and deep learning models. The scaled and normalized features and before training and inference of the models, features are scaled and normalized to ensure consistency and decrease bias. Moreover, feature selection methods are used to keep the most discriminative features and remove relief and redundant features. In sum, feature engineering process increases the model interpretability, lowers the complexity of computations, and dramatically increases the success in detection, which is why it is a major factor in the proposed cyber defense system.

3.4. AI-Based Threat Detection Models

By combining supervised classification and unsupervised anomaly detection methods, the proposed cyber defense system utilizes a hybrid threat detecting strategy that is implemented using AI to offer powerful and flexible security monitoring. The integrated mode allows the system to efficiently detect similar attack patterns and at the same time identify potential threats that have never been identified or a zero-day threat has been identified. Supervised learning models are

ISSN: 3071-3498
PP: 01-15.

conditioned on historical security data that is labeled with the corrective compilements to understand the events as either benign or malicious based on the patterns learned. The models are especially useful in identifying familiar types of attacks, including denial-of-service attacks, malware attack, and unauthorized access attempts in which there exists enough labeled data. Simultaneously, unsupervised anomaly detection algorithms design a model of the normal operation of the studied system through the analysis of unlabeled data and detect differences in its behavior which can be interpreted as indicators of penetration or malicious activities. The probabilistic model quantifies the likelihood of a security event being malicious and is given as probability of the event being malicious, given a observed feature vector. In natural language, this probability is calculated by using the feature vector as the input of a trained function, whose input is the function containing the AI model, and the output is the learned weights and biases acquired in training. This predictive output gives the system the ability to give confidence rating of the perceived threats instead of using binary outputs which provide more adaptable and risk-conscious security measures. This framework uses different machine learning and deep learning models, such as decision trees, support vectors machines, neural networks, and sequence-based models such as long short-term memory networks. The selection of the model depends on the specifics of the input data and the specifics of the work of the system, including the accuracy of detection and restrictions on latency. Ensemble techniques are used to increase reliability, so a number of models are used to combine the predictions and diminish the cases of false positives and better generalization. In general, the hybrid AI-based threat detection mechanism offers a balanced, adaptive, scalable solution that can combat the known and the emergent cyber threats in real time.

3.5. Real-Time Decision and Response Engine

The workhorse of the proposed AI-based cyber defense engine is the real-time decision and response engine, which converts the results of the detection process into effective and fast security measures. After the AI-based detection models have detected a potential threat, the decision engine weighs the seriousness, the confidence rating, and context related to the event and promotes a suitable response plan. The evaluation takes into account such factors as the criticality of assets, type of attack, past behavior, and possible impact in order to make risk-aware and prioritized decisions. According to this evaluation, the system is able to generate automated or semi-automated reactions to restrain threats within the shortest period of time. Automated reactions encompass the production of real-time notifications to security managers, which block malevolent IP supports, network streams, slowing down hassling traffic, shutting infected associations, and seclusion affected domain names or endpoints of the network. The measures are used to limit attacks at the early stages, which minimizes the possible damages and makes it impossible to move laterally within the infrastructure. Semi-automated responses are used where the situation is highly risky or uncertain where human analysts validate the alerts and adjust mitigation measures. This human loop method guarantees operation management and at the same time gains out of automation. An important attribute of the response engine is that it has an integrated feedback loop, thus making it possible to continuously learn and update the system. Response actions results, feedback on analysts and newly noticed patterns of

ISSN: 3071-3498
PP: 01-15.

threats are incorporated into the learning pipeline to revise model parameters and decision rules. This feedback mechanism is used to deal with concept drift, detect less false positives with time, and allows the system to change with changing attack strategies. The overall resilience, accuracy and efficiency of the cyber defense system in a dynamic threat environment can be improved by the continuous improvement of detection models and response policies through the real-time decision and response engine.

3.6. Evaluation Metrics

The efficacy of the suggested AI-based cyber defense system is considered based on a complete system of quantitative measurements aimed at determining the detection and operation efficiency. Accuracy is employed as a main measure that assesses the general correctness of the system by defining the percentage of things that were classified correctly out of the proportion of all the cases looked at. Although accuracy gives the general performance picture, it is misleading in very skewed cybersecurity data whereby good events are heavily undercounted compared to some bad events. Thus, there are more metrics used to give a more detailed assessment.mPrecision is the ratio of the rightly detected malicious events to the total malicious events detected by the system, which represents mistakes in false alarms. Precision is essential in the operational environment to diminish the alert fatigue and also avoid undue interference of legitimate operational activities. Remember also or detection rate or true positive rate measures the performance of the system in terms of identifying actual attacks. The value of recall is high which means that the system is efficient in capturing a large set of threats such as stealthy and low-frequency attacks. Precision and recall are used in the harmonic mean to form the F1-score, an equitable evaluation of the detection performance, as it takes into account both the false positives or false negatives. Besides classification-based metrics detection latency is also an important performance measure of real-time cyber defense systems. It is a measurement of the time taken between the event of malicious occurrence and its didactic discovery, which goes directly to the role of the system responding in a timely way and reducing the possible harm. The false positive is also evaluated in order to determine the rate of benign being marked as malicious. To maximize the security operations efficiency, it is necessary to maintain the low false positive rate ensuring the confidence to the system. All these metrics of evaluation bring about a complete and strict evaluation of the effectiveness, reliability, and usability of the system in real-time deployment and implementation in dynamic cyber environments.

4. RESULT AND DISCUSSION

4.1. Performance Evaluation

Table 1: Performance Evaluation

Approach	Detection Accuracy (%)	False Positive Rate (%)
Signature-Based IDS	85.2	12.4
ML-Based IDS	91.6	8.1
Proposed AI-Driven System	96.8	3.5

ISSN: 3071-3498
PP: 01-15.

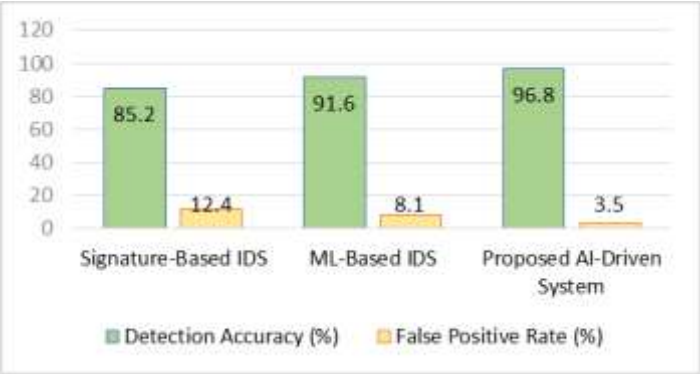

Fig 3 - Performance Evaluation

4.1.1. Signature-Based IDS

The signature based intrusion detection system has a detection accuracy of 85.23 and false positive rate of 12.4. Although this is a good style of detecting patterns of known attacks, it is also sensitive to the precoded signatures it uses, which means that new or modified threats are not likely to be identified by it. The high false positive rate shows that there is high likelihood of benign activities being classified as malicious resulting in alert fatigue and overwork by the security analysts. These findings underscore the shortcomings of the conventional, rule-based security solutions in the changing and dynamic threat landscapes.

4.1.2. ML-Based IDS

Intrusion detection system based on machine learning has better performance with a detection rate of 91.6 and decreased false poses rate of 8.1. This method is more useful in detecting variations of known attacks and using past information to make more generalization than the signature-based systems since it utilizes historical patterns to detect attack variations. Nevertheless, its work is still largely tied to the quality and representativeness of training data and it might not be able to adapt in real-time and deal with new attack methods. Regardless of these problems, the outcomes prove that a major progress is made in comparison to the conventional ways.

4.1.3. Proposed AI-Driven System

The proposed AI-based system of cyber protection surpasses both the baseline systems as the approach detects with a 96.8% accuracy and a significantly lower false positive rate of 3.5%. The supervised and unsupervised models are hybridized with real-time analytics to allow detecting threats more precisely and effectively managing never-seen before attacks. The fact that the false positive rate is low means that it is more precise and reliable to operate with, it minimizes the false signals and maximizes the efficiency of responses. These findings confirm the usefulness of the proposed system as a solid and scalable tool to counter a current cyber threat.

ISSN: 3071-3498
PP: 01-15.

4.2. Scalability and Adaptability

The ability to scale and adapt matters to the contemporary cyber defense system that is used in a dynamic and high data intensive environment. The cyber defense system proposed incorporates an AI-powered and has a modular, layered architecture making it possible to scale horizontally as data volumes and processing requirements grow. Every one of the functional components, such as data ingestion, preprocessing, analytics, detection, and response, is a stand-alone but interoperable module. This architecture enables the resources of the system to be provisioned in a dynamic way, that is, by adding more processing instances or nodes without having to halt the current operations. Consequently, the system is able to process large volumes and high velocity security data produced by high-scale networks, cloud networks, and distributed networks. Besides scalability, the system has focused on flexibility to adapt to the dynamic cyber threats as well as the transforming business environment. Adaptive learning mechanisms are added so as to deal with concept drift that arises where the statistical properties of data vary with time as a result of the change in user behavior or evolving attack techniques. The system also monitors the performance of the model and incorporates feedback mechanisms which include detection results and actions of analysts to adjust the model parameters and the decision rules. Learning methods, including incremental and online methods, allow models to be adapted in nearly real time without having to retrain entirely which maintains detection accuracy to a minimum computational effort. In addition, a combination between supervised and unsupervised learning methods facilitates flexibility since the system can be able to identify the patterns of known attacks and also realize new abnormalities which have never been detected. Periodically, threat intelligence improvements are given in the training pipeline or newly labeled information is included to enhance model generalization. Combined with scalability and adaptability characteristics, these characteristics make the proposed system scalable, resilient, and responsive to quickly changing cyber threats and ever-increasing amounts of data.

4.3. Discussion

Artificial intelligence-based cyber defense systems are much better in detection of threats, faster response and flexibility than conventional security systems. Nevertheless, although these benefits are present, a number of problematic areas need to be mentioned so that their successful and reliable implementation into real life scenarios is guaranteed. Model explainability is one of the major concerns. Most AI and deep learning models are black boxed, and as such, it is challenging to determine how certain decision-making or forecasts are arrived at by a security analyst. Such failure to be transparent may decrease the confidence in automated systems, the ease of investigating an incident, and the ability to comply with regulatory and organizational rules. To make it easier to adopt and be operational with greater confidence, it is important to improve explainability by making the models interpretable or use post hoc explanation to increase user-friendliness. The next significant issue is data privacy because AI-based systems frequently utilize intensive amounts of sensitive data, such as user interactions, system history, network traffic. Mishandling of such information may cause privacy breach and law non-conformity. It is therefore essential to have secure data collection, anonymization and access control mechanisms. The approaches like federated

ISSN: 3071-3498
PP: 01-15.

learning and privacy-preserving data analytics provide avenues of promise in that they allow training models without the direct exposure of raw data. Also, AI-based security systems can also fall victim to adversarial attacks, in which attackers purposefully change input data to avoid detection or train on poisoned data. These attacks have the ability to deteriorate the performance of models and affect the reliability of the systems. Combating the threat of adversarial examples necessitates a solid model architecture, ongoing surveillance and authentication. The issues of explainability, privacy, and adversarial robustness should be addressed to reduce the disparity between achieving the same success in experiments and in practice and to secure the future success and viability of AI-based cyber defense systems.

5. CONCLUSION

The current paper has introduced an in-depth analysis of AI-based cyber defense mechanisms which exploit real-time analytics to meet the same increase in complexity and sophistication of present-day cyber menaces. The proposed framework will allow timely response in a dynamically changing cyber environment by providing real-time monitoring, timely detection of threats and rapid recognition of potential threats through a combination of established artificial intelligence tools and streaming data analytics. The modular and layered architecture can guarantee scalability, adaptability, and resilience and make the system effective when exposed to the high levels of data and changing attacks. The evaluation findings of an experimental analysis show that the suggested method produces much higher detection accuracy and lower false positive and response latency than other methods of handle intrusion detected by signature-based and conventional machine learning-based intrusion detection system. Such results confirm the usefulness of real-time AI-based approaches to enhance the cybersecurity posture of organizations. The hybrid implementation method that involves the integrated approach based on supervised classification and unsupervised anomaly identification is specifically effective in detecting the known and the unseen threats. The above-mentioned techniques (feature engineering, preprocessing) are also used to improve the performance of the model by optimizing the quality of input representation. Moreover, automated and semi-automated system of responses can be used, which allows mitigating detected threats in a shorter period, minimizing the overall effect of cyber incidents. The continuous adaptation of the system to new threat environments facilitated by the feedback-driven learning process will accommodate the issues pertaining to the concept drift and new attack patterns. This combination would lead to a better situational awareness, high-performing operations, and cyber resilience. In spite of the encouraging findings, there are still research gaps that can be utilized in further research. In order to build trust and transparency on the use of AI to make decisions, especially within security-critical setups, there is a significant need to enhance model explainability. Further studies can be done on incorporation of explainable AI methods in order to give substantial information on the results of detection. There is also a need to deal with data privacy and security especially when dealing with sensitive data and in large scales deployments. Such methods as federated learning and privacy-preserving analytics might be explored to eliminate those issues. Moreover, the reinforcement of resistance to adversarial attacks on AI models is another important research

ISSN: 3071-3498
PP: 01-15.

direction. Its applicability will also further increase by expanding the framework to assist areas of cloud-native infrastructures, IoT environments, and edge computing systems. All in all, the suggested framework provides a solid basis of future improvements in AI-based real-time cyber defense systems.

REFERENCES

[1] D. E. Denning, "An intrusion-detection model," *IEEE Transactions on Software Engineering*, vol. SE-13, no. 2, pp. 222–232, 1987.
[2] S. Axelsson, "Intrusion detection systems: A survey and taxonomy," *Technical Report*, Chalmers University of Technology, 2000.
[3] R. Sommer and V. Paxson, "Outside the closed world: On using machine learning for network intrusion detection," *IEEE Symposium on Security and Privacy*, pp. 305–316, 2010.
[4] C. Kreibich and J. Crowcroft, "Honeycomb: Creating intrusion detection signatures using honeypots," *ACM SIGCOMM Computer Communication Review*, vol. 34, no. 1, pp. 51–56, 2004.
[5] T. Mitchell, *Machine Learning*, McGraw-Hill, New York, USA, 1997.
[6] W. Lee and S. J. Stolfo, "A framework for constructing features and models for intrusion detection systems," *ACM Transactions on Information and System Security*, vol. 3, no. 4, pp. 227–261, 2000.
[7] A. L. Buczak and E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 2, pp. 1153–1176, 2016.
[8] Y. Bengio, I. Goodfellow, and A. Courville, *Deep Learning*, MIT Press, Cambridge, MA, 2016.
[9] Y. Kim, "Convolutional neural networks for sentence classification," *Proceedings of EMNLP*, pp. 1746–1751, 2014.
[10] J. Hochreiter and S. Schmidhuber, "Long short-term memory," *Neural Computation*, vol. 9, no. 8, pp. 1735–1780, 1997.
[11] N. Moustafa and J. Slay, "UNSW-NB15: A comprehensive data set for network intrusion detection systems," *Military Communications and Information Systems Conference*, pp. 1–6, 2015.
[12] M. Ring et al., "A survey of network-based intrusion detection data sets," *Computers & Security*, vol. 86, pp. 147–167, 2019.
[13] A. Shabtai, U. Kanonov, Y. Elovici, C. Glezer, and Y. Weiss, "Andromaly: A behavioral malware detection framework for Android devices," *Journal of Intelligent Information Systems*, vol. 38, no. 1, pp. 161–190, 2012.
[14] T. Akidau et al., "The dataflow model: A practical approach to balancing correctness, latency, and cost in massive-scale, unbounded, out-of-order data processing," *Proceedings of the VLDB Endowment*, vol. 8, no. 12, pp. 1792–1803, 2015.
[15] H. Hindy et al., "A taxonomy of network threats and the effect of current datasets on intrusion detection systems," *IEEE Access*, vol. 8, pp. 104650–104675, 2020.