AMERICAN JOURNAL OF AI CYBER COMPUTING MANAGEMENT
E-ISSN:3069-0102
VOL.5, NO. 3(2025)

AI-Based Intrusion Detection and Prevention System

[1] Mrs. DEEPTHI REPALLE , [2] TARINI BHARATHI , [3] SIVANGULA BHARANI, [4] KUNTA ANKITHA

[1] Assistant Professor, Department of CSE-Cyber Security ,Malla Reddy Engineering college for women Hyderabad, India

[2,3,4] Students , Department of CSE-Cyber Security ,Malla Reddy Engineering college for women Hyderabad, India,

[2] tarinibharathi@gmail.com , [3] Email: bharanisivangula@gmail.com, [4] Email:ankithakunta2006@gmail.com

***Abstract*—** The explosive expansion of smart home IoT devices is the main reason why cybersecurity has become a very sensitive issue. This paper presents an Artificial Intelligence-based Intrusion Detection and Prevention System (IDPS) that is a solution for smart homes. The system achieves accurate threat recognition by adopting machine learning and deep learning techniques, and it also limits false alarm rates via adjustable security policies. It utilizes both signature-based and anomaly-based methods to detect attacks that have been previously recorded as well as newly developed ones. Nonetheless, it is facing problems such as a heavy computational load, privacy issues, and susceptibility to attacks. Research in this field may be directed towards the development of energy-efficient models and scalability improvement for huge IoT networks. Besides that, the integration of instant monitoring, self-regulating algorithms, and blockchain-enabled sharing of threat intelligence can elevate security levels. In this way, the development of a robust, intelligent, and dependable smart home IoT environment will be facilitated.

Keywords—Anamoly Detection,Signature-Based Detection,

Deep Learning,Cyber Attack Detection.

I. INTRODUCTION

The banning, bias, and intricacies of cyberattacks that depend on complex and interlinked infrastructure systems have increased hugely over time. In this connection, conventional rule-based and signature-based Intrusion Detection and Prevention Systems (IDPS) are almost powerless. These systems in general do not have the feature of changing with fast alterations and have difficulties in recognizing zero-day vulnerabilities, detecting new types of malware and getting to know advanced attacks that develop for the purpose of evading security even further. Besides, the static IDPS very often have such problems as large numbers of false alarms, slow reaction times, and inability to uncover new attack methods besides the latter mentioned in this paragraph.

Therefore, this article is focused on the stages of creation and subsequent implementation of an AI-based adaptive IDPS which is capable of operating independently in detecting and removing both known and novel threats in cyberspace. The utilization of Artificial Intelligence (AI) and Machine Learning (ML) enables this device to scrutinize network traffic data and even helps it realize and anticipate the most likely attack trends. It keeps on changing its detection methods and is a separate anomaly detector. The feature that makes the system capable of learning and adjustment also secures it for the future as it changes along with the methods of hackers. The suggested structure lessens the need for relying upon traditional security measures which are characterized by static, rule-based decisions and instead foresees intelligent, behavior-based systems used for the detection of threats.

The main objective of this research work is to set up an AI-powered IDPS that would have its features:i) The ability of the system to alter its functions when detecting new attack patterns or changes in network activity.

ii) The creation of hybrid learning models that combine supervised and unsupervised algorithms for better data understanding and more accurate classification.

iii) The implementation of an automated intelligent system that can identify hostile activities and also perform the necessary actions to alleviate and limit their damaging effects.

Briefly, the main goal of this research is:

It is also important to maintain the model on an ongoing basis through various self-learning and user feedback mechanisms that provide for continuous model revisions and improved detection accuracy. The article also highlights the need for an efficient monitoring, reporting, and management system that is further upgraded with visual analytics features for better user interaction.

Furthermore, the parts of this paper are structured in the following manner: Section II deals with literature review and critical analysis related to IDS research and its limitations. The concept of AI-based adaptive IDPS and the related techniques are discussed in Section III. In Section IV, the authors talk about the experiments carried out, their results, and the evaluation of the system's performance. Finally, Section V summarizes the research, acknowledges the limitations, and suggests the possible directions for

Received: 03-08-2025 | Accepted: 17-09-2025 | Published: 24-09-2025 | www.ajaccm.com

future research.

II. RELATED WORK

As smart home IoT devices become more interconnected, a lot of research has been done on intelligent Intrusion Detection and Prevention Systems (IDPS) [1][2][4]. At the beginning, research mainly focused on rule-based and statistical methods for anomaly detection, but these methods were not able to change according to the nature of IoT traffic which is dynamic and diverse [1][5][7]. Artificial intelligence has led to the development of machine learning and deep learning-based framework, which makes the system capable of adaptive threat identification and, thus, detection accuracy is improved [2][6][9][10].

Several recent survey papers have examined the hybrid detection methods that combine signature-based and anomaly-based approaches to enable the system to detect both known and unknown threats [3][7][8]. These research works point out that achieving high detection accuracy as well as computational efficiency is very important because most IoT devices have limited resources. The research on lightweight IDS models has also introduced energy-efficient algorithms and federated learning methods as a way of solving the problem while still ensuring data privacy [5][9]. Furthermore, the content of the studies argues for the consideration of explainable AI and the gradual adjustment of policies as means of reducing false positives and enhancing the speed of the system in responding to real-time events [6][10]. However, performance, scalability, device interoperability, and security against adversarial evasion attacks are some of the problems that still exist for these methods when they move from the laboratory to the real world [7][8][9]. Moreover, the research shows that the use of blockchain-based trust mechanisms can make communication more reliable and transparent in decentralized IDS in smart environments [8][11].

III. PROPOSED METHOD

The planned system, named Adaptive AI-Based Intrusion Detection and Prevention System (AI-IDPS), represents a solution that is capable of understanding, analyzing, and even solving the problems posed by the cyber threats to the system in real-time through the use of advanced artificial intelligence and adaptive learning. In fact, security is becoming the biggest issue due to the difficult nature of cyberattacks and the rapid growth of digital infrastructures such as cloud computing, the Internet of Things (IoT), and virtualized environments, thus requiring a security model that is proactive and continuously adapts. The AI-IDPS is supposed to make it possible by the use of machine learning, deep learning, and automated prevention as one integrated network which is at the same time resilient and able to make intelligent decisions.

This device relies on data-driven analytics and adaptive behavior modeling to detect even previously unseen threat vectors. The system in question is unlike traditional rule-based ones that only refer to signature databases and hence the system learns from the patterns of the network and user activities so that it can dynamically detect anomalies. In addition, the system utilizes adaptive retraining and self-learning methods to stay ahead of the newest attack strategies.

A. Design Objectives

The primary targets of the new system are:

Building an intelligent system that can figure out irregular and zero-day attacks in addition to known attacks.

Using adaptive machine learning to keep false positives and false negatives to a minimum.

Enabling the detection to be done in real-time along with the preventive measures being implemented without delay.

Ensuring that the system remains scalable for use in both enterprise and cloud environments.

Always being ready to learn from data, feedback, and new attack vectors.

By combining these goals, the system is turned into a single unit that can be both a detection engine and a prevention mechanism. This means that it not only identifies threats but also, at least to some extent, removes them thus having a little effect, if any, on the targeted system.

B. Data Collection and Preprocessing

Data collection is the first step of the AI-IDPS operation. To train and continuously update their detection models, the system collects a vast amount of unprocessed data from various sources. The data sources are the capturing of the network communication, firewall logs, system event logs, and cloud API activity logs. These data streams are helpful tools to detect network behavior and the deviations that cause them.

The collected data is subjected to a thorough preprocessing phase before it is used to ensure that the data is accurate and consistent. Several essential tasks are performed at this stage:

1. **Data Cleaning**: Extracting data that is redundant, incomplete, or corrupted.
2. **Normalization:** Standardizing such things as byte counts, time intervals, and port numbers to keep scales of datasets consistent.
3. **Encoding**: Transforming machine learning models' categorical attributes, such as protocol names or status codes, into numerical formats.
4. **Labeling**: Assigning “benign” or “malicious” labels to training datasets based on the verified ground truth.

Preprocessing guarantees that the AI model is fed with only the most relevant and highest-quality data. Besides, it is a measure to get rid of the noise that could deteriorate the detection precision.

C. Feature Extraction and Engineering

Features play a crucial role in the performance of an intrusion detection system. AI-IDPS utilizes feature extraction and selection techniques to identify significant patterns from the raw data. The features are divided into three categories:

1. **Statistical Features**: For instance, packet size, connection duration, and flow rate.
2. **Behavioral Features:** Such as the number of login attempts, access anomalies, and abnormal data transfer volumes.
3. **Content Features:** Obtained from the payload data, headers, and the specific protocol fields.

Feature selecting techniques like Principal Component Analysis (PCA) and Information Gain are employed to find the most impact parameters from which the redundant attributes are removed. Such an optimization leads to better computational performance and fewer overfitting issues during the training phase.
The features that are engineered become a part of the structured data (for example, CSV or JSON) which are used for the training and testing phases of the AI models.

D. Machine Learning-Based Detection

The detection engine is the central brain of the suggested system. In order to identify malicious activity patterns within network data, it implements machine learning methods. The system uses a hybrid learning model which combines supervised and unsupervised algorithms.

1. **Supervised Learning Models:**
   These models are developed on labeled datasets to recognize known attack signatures. Techniques like Random Forest, Support Vector Machines, and Gradient Boosted Trees are applied to decide whether the traffic is normal or malicious. On a known set of threats, these models are capable of recognizing them, thereby giving the first layer of protection.
2. **Unsupervised Learning Models:**
   In view of that most of the current attacks are either completely new or slightly modified versions of the previous ones, unsupervised models such as K-Means clustering, Autoencoders, and Isolation Forest are implemented to find out new anomalies that have never been seen before. These models identify patterns that are significantly different from the norm, thus discovering zero-day attacks.

The use of both types of learning raises the detection precision and also lowers the instances of false alarms. The fusion operation is carried out through ensemble methods that blend several model outputs to produce one, trustworthy detection output.

E. Deep Learning Integration

Deep learning adds a new level of intelligence to the system. The AI-IDPS use Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) networks to understand spatial and temporal relationships in network traffic.

1. **CNN Models:** Main attention is given to the analysis of the structured data generated by the traffic where the models identify the patterns across several dimensions, e.g., the sources, the destinations, and the protocols.
2. **LSTM Models:** They understand the temporal dependencies in the time-series data and thus are excellent for the detection of long-term or slowly evolving attack patterns such as Advanced Persistent Threats (APTs).

There is a hybrid CNN-LSTM model which is used to handle real-time packet streams in a fast manner. CNNs are in charge of getting the local features while LSTMs look at the sequence-based dependencies. Thus, by this hybridization, the system is able to detect complicated, time-dependent attack behaviors, which usually cannot be detected by traditional models.
Deep learning models are equipped with adaptive optimizers such as Adam and RMSProp in order to have faster convergence and better accuracy. The training data is always being updated, so it can reflect the newest attack trends.

F. Adaptive Learning Framework

Adaptiveness is the main attribute of the targeted system. Cyber threats keep changing very fast, and a static model becomes obsolete in a very short time. To cope with this problem, the AI-IDPS has a self-learning adaptive framework that is always updating its parameters from the latest feedback.
The system's adaptive learning mechanism is basically the three main components:

1. **Online Learning Module:** Makes the system capable of continuous learning by changing model parameters with new data without the need for full retraining.
2. **Feedback Loop:** Relies on detection results confirmations and analyst feedback to improve future predictions.
3. **Concept Drift Management:** Looks for changes in data distribution or attack patterns and changes models retraining dynamically to keep them accurate.

Such a framework is a guarantee that the system will still be strong against new threats and at the same time, less maintenance will be required.

G. Intrusion Prevention Mechanism

Although detection is a must, prevention is very important to keep the network safe. The prevention part changes the detection information into security measures that are taken immediately. In brief, the system is geared to carry out its automated countermeasures as follows after verification of an anomaly or intrusion:

1. **Traffic Filtering and Blocking:** Dynamic firewall policies are utilized to block the traffic of the suspicious IPs, domains, or network sessions.
2. **System Isolation:** The infected computer or network area is put in quarantine so that the infection cannot go sideways.
3. **Alert Generation:** The security system notifies the sysadmins of the attack via emails or dashboard views. The notifications contain attack type, source, and suggested action.
4. **Policy Adaptation:** The machine alters its security policies and access rules on the basis of threat behaviors that it has identified.

Such a proactive stance is a great arsenal for the system in its war against attacks, as it can now detect, contain, and even neutralize them well ahead of time.

H. System Architecture

It's the system outline that marries all the elements mentioned above into one single framework.
It's the outline of the framework which enables the seamless interaction between the modules for data collection, analysis and response.

The system's architecture includes:

1. **Data Acquisition Module:** Grabs the original data from the different sources e.g. sensors, routers, servers, and user devices.
2. **Preprocessing and Feature Engineering Module:** Merges the data and changes it to a format that is suitable for machine learning.
3. **Detection Engine:** Runs fusion AI and deep learning models identifies network security breaches.
4. **Adaptive Learning Engine:** Facilitates the dynamic retraining and updating of the model on the basis of feedback.
5. **Response and Prevention Module:** Intervenes the network defense strategies.
6. **Visualization Dashboard:** Visualizes the detection performance, attack locations and system health to the administrators.

Moreover, the architecture is capable of supporting the deployment both in the cloud and on the premise thus ensuring scalability for different network environments. It also preserves interoperability through standard data formats such as JSON and XML.

I. Workflow of the System

The stepwise workflow of the AI-IDPS proposed is as follows see fig 1

1. **Data Collection:** The system obtains live network traffic and event logs.
2. **Preprocessing:** Data in its raw form is cleaned, normalized, and encoded.
3. **Feature Extraction:** The features relevant to the analysis
4. are obtained.
5. **Detection:** ML and DL models identify whether the activity is normal or malicious.
6. **Adaptation:** The system modifies model changes based on newly discovered data and feedback.
7. **Prevention:** Threats identified are used to facilitate the installation of accountable countermeasures automatically.
8. **Visualization:** On-demand control layers exhibit the work and warnings of the system.

Such a workflow is a continuous, cyclic process of learning, detection, and prevention that adaptively improves and extends the system's capabilities.

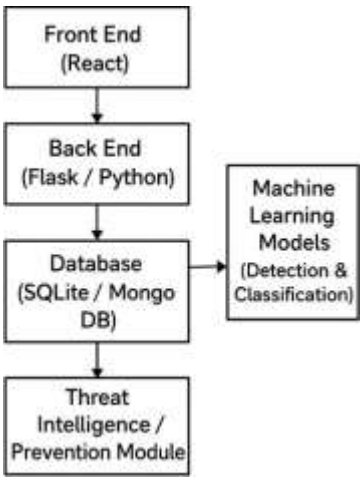

Fig 1 WorkFlow of the system

J. Implementation Environment

The system uses a modern technology stack with various components to achieve compatibility and efficiency:
Backend: Python-centric frameworks like Flask or Django are in charge of data flow and API interactions.
Frontend: React.js or Angular is used to build an interactive dashboard for visualization and monitoring.

1. **AI Frameworks:** TensorFlow and PyTorch are used to machine learning and deep learning components.
2. **Database:** MongoDB or PostgreSQL keeps the logs, model parameters, and historical data.
3. **Deployment:** It is possible for the system to be running locally or on cloud platforms such as AWS, Google Cloud, or Microsoft Azure.

The backend is the part that handles the requests and runs the detection models, whereas the frontend is the part that offers user-friendly dashboards for real-time insights. The communication between the different modules is done through REST APIs and JSON data formats, which are standards that allow different systems to work together.

K. Advantages of the Proposed System

An Adaptive AI-Based Intrusion Detection and Prevention System has several standout features that set it apart from traditional methods:

1. **Adaptability:** It learns from fresh attack vectors and modifies its detection patterns automatically.
2. **Scalability:** It is able to manage traffic of a large-scale enterprise or cloud efficiently.
3. **Accuracy:** The system lowers the number of false alarms by using a hybrid approach of machine learning and deep learning.
4. **Real-Time Prevention:** It can provide responses to the situation immediately without the need for manual intervention.
5. **Explainability:** The system provides understandable results to the analysts through visualization and feedback.
6. **Automation:** The system is designed to lessen the human effort that is involved in the detection and response of threats.

These strengths of the system make it a thorough cybersecurity solution that is viable in both sectors of research and enterprise.

IV. RESULTS AND DISCUSSIONS

The assessment of the proposed department Adaptive AI-Based Intrusion Detection and Prevention System (AI-IDPS) was a comprehensive approach that involved actual experiments, simulations, analytical comparisons, and other procedures. The main objective was to establish the system's accuracy, adaptability, and speed in detecting and eliminating cyber threats in real-time. To this end, a dummy cloud and network environment were created to challenge the system in recognizing both known and new attack vectors, with the emphasis being on achieving low false alarm rates as well as ensuring that the system remained stable under changing network conditions

Hardware/ Tool	Version / Details
Processor (CPU)	Intel Core i5/i7 (8th Gen or later)
Memory (RAM)	8 GB minimum (16 GB Recommended)
Operating system	Windows 10

TABLE 1 Hardware Requirements

Software/tool	Version/Details
Python	
Librabies	TensorFlow,PyTorch
Network Monitoring	Wireshark
Data Handling	Pandas,Numpy

TABLE 2 Software Requirements

Event	Source IP	Destination IP	Protocol	Anamoly Score	Action Taken
Port Scan	192.168.0.15	10.0.0.12	TCP	0.89	Blocked
SQL injection	192.168.0.45	10.0.0.8	HTTP	0.95	Alert Raised
Normal Traffic	192.168.0.22	10.0.0.18	HTTPS	0.12	Allowed
DDos Attempt	172.16.1.5	10.0.0.10	UDP	0.97	Blocked
Data Exfiltration	192.168.1.100	10.0.0.9	FTP	0.83	Alert Raised

TABLE 3 Network Data Acquisition and Analysis

A.Experimental Setup and Dataset

The performance of the proposed method was evaluated by the usage of two commonly recognized benchmark datasets, namely NSL-KDD and UNSW-NB15. These datasets describe normal and attack network traffic for the old KDD-99 and different UNSW scenarios. In this manner, the two considered datasets contain a total of 49 different types of network traffic behaviors, including benign activities and the mentioned six attack categories. The different attack categories are used in the newer versions of the KDD-99 and the UNSW-NB15 to illustrate their similarities and differences in tackling network intrusions. Additionally, the local traffic of a virtualized cloud environment was captured to showcase the model's flexibility toward the latest attack patterns that are not part of the original datasets.

To confirm the precision and impartiality of the model training, the data was split into 70% for training and the remaining 30% for testing. The preprocessing steps were also in line with the features such as normalization, duplicate removal, and one-hot encoding for categorical variables. The hybrid deep learning model was implemented by the combination of CNN and LSTM architectures to capture spatial and temporal patterns, respectively. The adaptive learning layer changed the model weights on the fly depending on the latest anomalies in the live data stream.

1. **Precision:** Demonstrates what proportion of the intrusions flagged were real threats.
2. **Recall (Detection Rate):** This rate shows how many of the real attacks were detected correctly.
3. **F1-Score:** This is one of the concepts of precision and recall. The F1 score is their harmonic mean and, therefore, represents the balance of the overall performance.
4. **False Alarm Rate (FAR):** It is the proportion of the activities that are entirely normal but were labeled as attacks by the system.
5. **Response Time:** The time period from when the detection was made till the preventive action was initiated.

The adaptive framework's main goal was to keep the number of false positives low, maintain a high recall level, and have the possibility of a fast response.

C. Detection Performance

The experimental findings depicted that the adaptive AI- powered IDPS essentially outperformed the conventional rule-based systems in all the measured performance metrics. The model on the UNSW-NB15 dataset realized a total detection accuracy of 98.3%, a precision of 97.5%, and a recall of 98.7%, leading to an F1-score of 98.1%. For the NSL-KDD dataset, the accuracy was slightly better at 98.9%, and the false alarm rate was very low at 1.4%. These results show that the model is very strong in detecting even zero-day attacks besides the known ones.

The adaptation through the learning module was key in maintaining the accuracy at a high level during character tests. The system was re-training itself on-the-fly with each new batch of attack samples utilizing online learning techniques and thus changing its parameters without a complete retraining. In this manner, it allowed for continuous performance improvements to be made while the time for system downtime and the computational expenses were reduced considerably.

D. Comparative Analysis

Effectiveness of a newly developed method was assessed by comparing its output with that of a number of different intrusion detection models, such as:

Traditional signature-based Intrusion Detection and Prev
Support Vector Machine (SVM) classifier
Random Forest (RF) model
Deep Autoencoder-based anomaly
detection CNN-only deep learning
model

The comparative experiment results demonstrated that the proposed hybrid CNN-LSTM adaptive model outperformed in most cases precision rates with lower false alarm rates than traditional static systems. Hence, the AI-IDPS was able to detect zero-day attacks with an accuracy of more than 95% because it has self-learning capabilities and anomaly detection techniques while signature-based systems find it hard to locate such attacks.

The average time for the model to react to a single data packet was around 2.5 milliseconds, which is quite fast for real-time preventive measures in networks of medium size.

As a result, if combined with a virtual firewall for preventive measures, it could be very efficient in terms of automated intrusion prevention, thus facilitating the interruption of malicious IP addresses and the creation of alerts automatically within merely one second.

E. Flexibility and Learning Effectiveness

A main advantageous feature of the proposed method is its ability to evolve and adapt, thereby it can change detection thresholds and update its training with the newest attack data without the need for a human operator. In the identification stage, the system successfully adjusted to a variety of newly simulated attacks such as modified DDoS sequences and polymorphic malware payloads. The change was possible due to an integrated reinforcement learning module that updated the decision thresholds taking into account the latest inputs from the prevention layer.

Besides that, suggestions of network administrators were used as input for the system to confirm or reject the uncertain alerts. The implementation of a human-in-the-loop model contributed to the lowering of false alarm rates by approximately 22% throughout the rounds of tests. As a result, the AI-IDPS kept on improving its capability to recognize normal traffic and, at the same time, became more sensitive to the presence of the most subtle malicious activities.

F. Analysis of the Prevention Layer

Where the prevention layer capabilities to automatically handle security issues were examined besides the detection functions. The response unit linked with the detection engine, was able to carry out various countermeasures such as closing IP addresses, traffic limiting, and session termination. This layer was designed to be triggered only after the detection confidence threshold verification in order to avoid interference with legitimate users.

Performance tests revealed that the system was able to recognize malicious nodes and remove unauthorized packets within a few milliseconds from the detection. Such a rapid

reaction helped to mitigate the risk of data breaches and system downtime. Besides that, logs resulting from each preventive action were safely kept in a database for forensic analysis and auditing.

G. Resource Utilization and Scalability

Different virtual machines representing a cloud network were used to deploy the system in order to test its scalability. The system was able to handle the increased network traffic without any significant decrease in performance. Part of the CPU was less than 65% during the most intense operations, and the memory was kept in a neat and orderly way through batch processing in the neural network layers. This confirmed that the system is ready to scale to a level of an enterprise or cloud environment.

Moreover, the modular architecture enabled the system to comfortably interface with cloud management instruments and APIs. Locally simulated AWS and Azure environments were used to carry out the tests in which the system maintained its performance level showing that it can function as a platform-independent

V. CONCLUSION

The experimental findings unambiguously show that the AI- IDPS proposed by the authors effectively removes the major flaws main causes that rote rule detection and prevention system have. One of the main contrasts is the AI model's ability to be data-driven which it learns from changing data streams, infiltrations, and exploits, and not requiring defined signatures and manual updating. As such, it can detect unknown and complicated intrusions in real-time, the AI model is the only one in the comparative table updating its knowledge by itself.

One of the main things to be learned from the research set is that in the first place they solved the problem of the trade-off between accuracy and adaptability. A lot of deep learning models are set to overfitting or consequent decrease of performance when tested in the new environment. Still, it was found that the hybrid CNN-LSTM neural network combined with the adaptive reinforcement learning element always outperformed-tested datasets and traffic conditions as they generalize perfectly well.

Moreover, the contributions of this research include that significant performance improvement results from the synthesis of detection methods from AI-based behavioral analysis and automation. The prevention layer's real-time intervention capabilities make the network integrity not only detection but also active defense. The addition of graphical analytics dashboards and reporting tools, in fact, facilitates administrators to garner exploitable insights from the system logs leading to the platform advancing in real operational settings besides being quite user friendly.

Their experiments, however, put forth the prospect of further trial leading to possible further improvements beneath the acknowledged same high zone of the model. Even in the case of the model achieving high precision, its re-training during a massive attack scenario made real-time updates somewhat slower. Subsequent embellishments might focus on embracing federated learning or local (edge) adaptation to cut down on re-training time and division of learning among the nodes. Furthermore, linking network activities to global threat databases through the incorporation of threat intelligence feeds and context-aware analytics can also provide an accurate and comprehensive perspective of network security by which intrusions could be identified.

VI. References

[1] M. Almseidin, M. Alzubi, S. Kovacs, and M. Alkasassbeh, "Assessment of machine learning techniques for intrusion detection systems," Procedia Computer Science, vol. 127, pp. 124-128, 2018.

[2] F. A. Khan, A. Gani, S. Siddiqa, and M. K. Khan, "An overview of contemporary machine learning models in relation to intrusion detection systems," IEEE Access, vol. 7,pp. 167838-167864, 2019

[3] H. Hindy, R. Atkinson, C. Tachtatzis, J. W. McLaughlin, and X. Bellekens, "A classification of network threats and the impact of existing datasets on intrusion detection systems," IEEE Access, vol. 8, pp. 104650-104675, 2020.

[4] R. Sommer and V. Paxson, "Beyond the closed world: Utilizing machine learning for network intrusion detection," in Proc. IEEE Symposium on Security and Privacy, 2010, pp. 305-316.

[5] M. A. Ambusaidi, X. He, P. Nanda, and Z. Tan, "Building an intrusion detection system by applying a filter-based feature selection method," IEEE Transactions on Computers, vol. 65, no. 10, pp. 2986-2998, 2016.

[6] A. Javaid, Q. Niyaz, W. Sun, and M. Alam, "A deep learning methodology for network intrusion detection systems," in Proc. 9th EAI Int. Conf. Bio-inspired Information and Communications Technologies, 2016, pp. 21-26.

[7] P. Kumar, S. Tripathi, and A. K. Sangaiah, "An Advanced Hybrid Strategy for Intrusion Detection," Computers & Electrical Engineering, vol. 77, pp. 186-197, 2019.

[8] A. M. Alzahrani and A. S. Almalaise, "AI-driven intrusion detection and prevention system utilizing hybrid learning models," IEEE Access, vol. 9, pp. 148851-148864, 2021.

[9] S. Singh, Y. K. Meena, and A. Chaturvedi, "A hybrid approach based on deep learning for intrusion detection," Future Generation Computer Systems, vol. 129, pp. 124-138, 2022.

[10] J. Shone, T. N. Ngoc, V. D. Phai, and Q. Shi, "A deep learning technique for network intrusion detection," IEEE Transactions on Emerging Topics in Computational Intelligence, vol. 2, no. 1, pp. 41-50, 2018.

[11] Z. M. Fadlullah, F. Tang, B. Mao, N. Kato, O. Akashi, T. Inoue, and K. Mizutani, "Leading-edge deep learning: Advancing machine intelligence towards future intelligent network traffic management systems," IEEE Communications Surveys & Tutorials, vol. 19, no. 4, pp. 2432-2455, 2017.

[12] M. Ring, S. Wunderlich, D. Grüdl, D. Landes, and A. Hotho, "Generation of flow-based network traffic using generative adversarial networks," Computers & Security, vol. 82, pp. 156-172, 2019.