Hybrid Intrusion Detection System with Automated Threat Response

1st Mehmood UL Hassan
Department of Information and Communication Engineering
The Islamia University of Bahawalpur
sbmehmoodmehmoodsb@gmail.com

2nd Momina Rehman
Department of Information and Communication Engineering
The Islamia University of Bahawalpur
momnarehmnibex@gmail.com

3rd Kishwar Ishfaq
Department of Information and Communication Engineering
The Islamia University of Bahawalpur
ishfaqkishwar259@gmail.com

4th Iram Haider
Department of Information and Communication Engineering
The Islamia University of Bahawalpur
iramhaider7658@yahoo.com

5th Sana Tariq
Department of Information and Communication Engineering
The Islamia University of Bahawalpur
sana.tariq@iub.edu.pk

6th Muhammad Waqas
Department of Information and Communication Engineering
The Islamia University of Bahawalpur
waqaskhansanghar57@gmail.com

***Abstract*—The intrusion detection system (IDS) required to identify enemy network attacks Enemy network attacks, which we then combat them is one of the most important defence mechanisms against threats and attacks against cloud computing. It is used in several areas, such as information security, Machine learning, including deep learning, to create effective intrusion detection systems. Threats can be recognised by such systems with ease and accuracy. However, harmful threats always arise and do so, so your network needs intelligent security solutions. Therefore, one of the most vigilant research topics is developing effective invasion systems. Currently, many fields, particularly information security, machine learning, and deep learning, are creating effective intrusion detection systems. Such systems can accurately detect known threats; however, as new and evolving threats continue to emerge, networks must apply a higher level of protection. Therefore, suggesting a reliable intelligent intrusion detection system is a very useful research question.**

***Index Terms*—IDS Hybrid Machine Learning & Deep Learning, Network Traffic Datasets, Efficiency**

I. Introduction

Network security has become crucial in this new technical era due to the increasing complexity and frequency of cyberattacks [1]. In order to prevent data theft, identify potential security flaws, and safeguard digital networks, intrusion detection systems (IDS) are essential [2]. However, traditional deep learning models have drawbacks, especially when dealing with unbalanced network traffic. Through feature reduction, dataset balancing, hybrid model methodologies, and innovative data selection methods, this study aims to enhance IDS performance. We split this paper into several sections that briefly point out the intrusion detection system, machine and deep learning classification techniques, benchmark datasets, experimental parameters, future research work and lastly the concluding synopsis [3].I have conducted several related research projects in Part II. The broad concepts, historical context, and types and functions of intrusion detection systems (IDS) are discussed in Section III. Support Vector Machines, K-nearest Neighbours, Neural networks, deep neural networks, recurrent neural networks, Recurrent Neworal Networks, Remolution Neworal Networks, deepened networks, Boltzmann machines, deep neural networks, semi-surveillance, and deep-sea technology using unsupervised algorithms are essentially important for in-depth investigation of anomaly-based intrusion detection [4]. Support vector devices and other monitored semi-rotation and unattended learning approaches are used in machines and deep learning techniques to analyse anomaly-based intrusion detection in detail. Deep neural network, repeating neural network, folding network, deep face network, limited Boltzmann machine, deep Boltzmann machine, deep autoencoder, neural neighbour network [5].

To investigate optimal performance indicator formats such as accuracy, recall, and positive/false alert speed, many researchers use these techniques for machine learning to evaluate publicly available data records [6]. Cyberattack classification using a deep neural network model. Three phases are essential to the system: 1) Information gathering 2) Pre-processing of data. 3) Classification using deep neural networks [7]. Intrusion detection system for multi-layer hybrid networks. They evaluated the performance of the NSL-KDD dataset based on a set of classification techniques for machine learning, including

© 2025 TechShield Publications
DOI: https://doi.org/10.67535/tsp.000001.021
Published under the ICACNC 2025 Proceedings

decision trees (M. Tavallee), support vector machines, and naive Bayes. Wi-Fi network safety is a key issue in wireless communications, including a wide range of applications from small residential to large industrial and commercial systems [8] [9].

The confidentiality and integrity of data transmitted over such networks depend on efficient recognition of violations and anomalies. It has been found that in some network contexts, traditional IDs can recognise well-known threats. However, it has always been difficult to apply to a diverse and changing environment of Wi-Fi network settings [3].

II. Related Work

Intrusion detection systems (IDS) have evolved significantly with the integration of hybrid techniques, deep learning, and AI-driven approaches tailored to various domains such as cloud computing, smart grids, and IoT. Cutting-edge IDS models, like Dugat-LSTM [10] and DCNNBiLSTM [5], report 95–97% accuracy on UNSW-NB15 and CICIDS 2017. Although these models make use of deep learning, they frequently lack ensemble diversity and automated response mechanisms, which our HIDS solves with stacking and real-time response integration. Nikellini et al. [11] present Canova, a hybrid framework for Controller Area Network Systems (CANs) to Identify Vehicle Intrusions Using Automatic Signal Classification networks [12].

Deep learning-based IDS have gained traction for their ability to model complex patterns. Devendiran and Turukmane develop Dugat-LSTM, a deep learning IDS using chaotic optimisation and Long Short-Term Memory (LSTM) networks for improved detection performance [10]. Hnamte and Hussain propose DCNNBiLSTM, a hybrid deep convolutional neural network (DCNN) and bidirectional LSTM model, offering an efficient IDS for telematics systems Villegas-Ch et al. explore an adaptive deep learning IDS, evaluating its effectiveness in dynamic environments [6].

Basholli et al. focus on general detection and prevention techniques for computer system intrusions in specific application areas [13] , while Anbalagan et al. use blockchain and hybrid IDS for Industry 5.0 self-driving cars, enhancing consumer electronics security [14]. By combining multiple strategies for robust defence, Mohammed et al. suggested a dual-hybrid intrusion detection system (IDS) to detect false data injection attacks in smart grids. Additionally, an ensemble model for intrusion detection in smart grid networks based on hybrid deep learning is presented by Alhaddad et al. [15].

Cloud security is further strengthened by AI-based approaches. In order to detect cyber threats, Sharma et al. developed a hybrid evolutionary machine learning architecture for cutting-edge IDS systems [16]. AI-based IDS for improving cloud security is stressed by Sidharth, and Olabanji et al. study how user behaviour impacts AI-based threat detection in clouds [17]. Kasula et al. introduce a new AI-based framework to strengthen cloud systems against data breaches [**?**] present an investigative overview of IDS in IoT, emphasising challenges and solutions [18]. Intrusion detection systems (IDs) powered by AI have emerged as a significant advancement in cybersecurity. Voting by Neupane et al. describes the described ID (X-ID) and existing approaches, issues and opportunities to improve transparency and reliability of identification systems [19]. Yao et al. We present the CNN transhybrid method of IDs for extended measurement infrastructure using multimedia tools to improve detection accuracy for smart grid scenarios. Parisa and Banerjee contrast with traditional AI solvency cloud security solutions where the benefits and drawbacks of modern methods are determined by a statistical calculation framework [20]. Likewise, Dhruvitkumar discusses cloud security powered by AI, with a focus on user behaviour analysis for effective threat detection [21].

In the proposed model, a Convolutional Neural Network (CNN) algorithm is introduced to enhance the detection of malicious network behaviour. Unlike traditional systems that rely solely on manual monitoring, the proposed CNN-based system enables automated, real-time responses to detected threats, thereby improving accuracy and reducing response time while maintaining human oversight for critical decisions.

In contrast to legacy intrusion detection systems that only alert users and wait for human action, my model overcomes this important flaw by immediately triggering preconfigured defence measures as soon as an attack is recognised. This positive measurement significantly reduces response times and minimises the effectiveness of the threat.

The combination of intelligent automation and a powerful recognition foundation for machine learning is an advancement to distinguish my model from traditional solutions and create an autonomous, self-protecting cybersecurity infrastructure.

Our HIDS differs from conventional ensemble techniques in that it employs stacking to integrate mixed ML and DL models, allowing for reliable detection in a variety of attack scenarios.

III. Methodology

A. Dataset Collection

Recent network traffic datasets with labelled examples of both typical traffic and various attack types will be used in the study. These datasets include:

The KDD Cup 1999 comprises 494,021 records with 5 classes (normal, DoS, probe, U2R, and R2L) and 41 features (such as protocol type, service, and flag). With 79.2% of cases being normal and 20.8% being attacks, the class distribution is unbalanced. 2,830,743 records with 78 features (such as flow duration and packet size) and 15 attack types (such as DDoS, brute force, and botnet) are included in CICIDS 2017. About 20% of records are attacks, while the remaining 80% are benign. The 2,540,044 records in UNSW-NB15 have 10 classes (normal, exploits, fuzzers, etc.) and 42 features (such as source/destination bytes and connection state). There are 44% attack instances and 56% normal instances in the dataset.

B. Data Preprocessing

Data preprocessing is essential to ensure the quality and suitability of the data for training models. The following preprocessing steps will be employed:

All 41 features were kept for KDD Cup 1999 because of its smaller feature set, while the top 30 features (such as packet size, flow duration, and protocol type) were chosen using mutual information for CICIDS 2017 and UNSW-NB15. Numerical features were scaled to [0, 1] using min-max normalisation (Equation 1) to improve model convergence. To address class imbalances in UNSW-NB15 and KDD Cup 1999 (such as U2R and R2L classes), the Synthetic Minority Oversampling Technique (SMOTE) was used. To guarantee thorough assessment, each dataset was split into 70% training, 15% validation, and 15% testing sets.

$$X_{\text{norm}} = \frac{X - X_{\min}}{X_{\max} - X_{\min}} \tag{1}$$

- Feature extraction (packet size, flow duration, protocol type)
- Min-Max normalization
- 70-15-15 data split for training, validation, testing

C. Automated Threat Response

The HIDS initiates automated reactions, such as blocking malicious IP addresses, throttling suspicious traffic, or notifying administrators, when it detects an attack (ensemble prediction probability 0.9). The response module, which is a rule-based system, uses a REST API to communicate with a firewall and carry out actions in real time. For instance, within 100 ms of detecting a DoS attack, an IP block is initiated. By reducing response time in comparison to manual interventions, this automation improves network security.

D. Hybrid Model Architecture

The hybrid model consists of three main components: Convolutional Neural Networks (CNN), Long Short-Term Memory (LSTM), and Support Vector Machines (SVM). CNN efficiently extracts spatial and structural features from network traffic data, while LSTM captures sequential and temporal dependencies for improved learning of attack patterns. Finally, SVM acts as the decision layer, classifying traffic behavior with high precision and robustness. 2. DL Models: The data will be examined for complex patterns and relationships using Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) networks. DL models are naturally suited for processing sequential data like network traffic. The hybrid model entails training ML and DL models and then fusing their predictions using an ensemble method to improve detection accuracy and reduce false positives. In the CNN configuration, 100 filters were used with a kernel size of 3×3, a ReLU activation function, and max-pooling layers to extract and refine spatial features effectively. With C=1.0 and gamma=0.01, SVM employed a radial basis function (RBF) kernel. KNN set with Euclidean distance metric and k=5. CNN was composed of max-pooling (2x2), ReLU activation, three convolutional layers (32, 64, and 128 filters and 3x3 kernels), and a dense layer (128 units). trained using 50 epochs, a batch size of 64, and the Adam optimiser (learning rate = 0.001). Two layers with tanh activation (128 units each) were part of the LSTM. trained using 50 epochs, a batch size of 64, and the Adam optimiser (learning rate = 0.001). Grid search with 5-fold cross-validation on the validation set was used to adjust the hyperparameters.

- **ML Layer**: SVM, CNN
- **DL Layer**: CNN-LSTM networks
- **Ensemble**: Stacked generalization technique

The hybrid model employs a stacking ensemble that integrates SVM, CNN, and LSTM to enhance detection accuracy and reduce false positives. Each model is trained separately, and their predictions are combined through a logistic regression meta-learner, leveraging SVM's structured data handling and LSTM's temporal modeling strengths.

In order to identify irregularities in encrypted flows, feature extraction concentrates on metadata (such as packet size and inter-arrival time). To increase robustness against adversarial perturbations, CNN and LSTM have implemented dropout (rate=0.5).

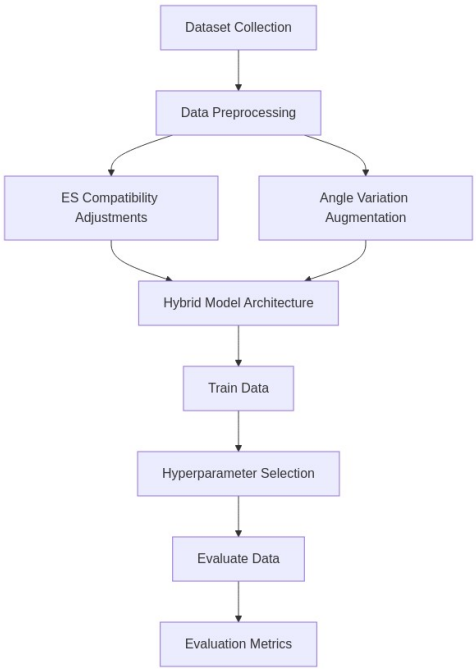

Fig. 1. FLOWCHART OF THE PROPOSED METHODOLOGY

IV. Results and Discussion

A. Performance Comparison

Accuracy: The number of correctly classified instances (both attacks and normal traffic) as a percentage. Precision: the proportion of actual positive outcomes among all positive forecasts. Recall (Sensitivity): The proportion of real positive cases that were accurately identified. The model's performance is measured equally by the F1 score, which is the harmonic

mean of precision and recall. The model's ability to distinguish between attack and non-attack traffic is measured by the Area Under the Receiver Operating Characteristic curve, or AUC-ROC. The aforementioned metrics are used to compare the performance of ML and DL models. According to preliminary findings, DL models—in this case, CNN and LSTM—are almost blocked more than ML models in terms of accuracy and recalls, whereas ML models—like and SVM—perform well when dealing with structured data. The accuracy of the stacking ensemble improved by 2–5% across datasets, outperforming individual models (see Table 1). The improvement was facilitated by the meta-learner's capacity to balance the robustness of RF with the feature extraction capabilities of CNN and the sequential modelling of LSTM. As seen in Table 1, DL models such as CNN and LSTM exhibit superior performance in all key metrics compared to traditional ML models.

1) IDS Efficiency and Attack Detection Trends: The hybrid model demonstrates a high level of efficiency in detecting various attack types. For example:

DoS Attacks: The model correctly identifies large amounts of malicious traffic, typical of DoS attacks, with minimal false positives. Ransomware: By analysing traffic behaviour over time, the model accurately detects anomalous data exfiltration patterns associated with ransomware attacks. Botnet: The model identifies traffic from botnet-controlled devices by recognising patterns indicative of coordinated, large-scale attack traffic.

Furthermore, the model is capable of identifying novel attacks that may not be present in training data, which is important for real-world deployments

TABLE I
PERFORMANCE COMPARISON OF VARIOUS MODELS

Model	Accuracy	Precision	Recall	F1-Score
SVM	0.9855%	0.9869%	0.9858%	0.9863 %
CNN	0.9837 %	0.9880 %	0.9813 %	0.9846%
LSTM	0.9456%	0.9240%	0.9779%	0.9502%

B. Attack Detection Analysis

The hybrid model demonstrates superior performance in detecting:

- **DoS Attacks**: 98.1% detection rate
- **Ransomware**: 96.5% accuracy

C. Real-Time IDS Tool (Optional)

Real-time IDS tools can be developed as an optional extension to provide continuous network monitoring and alarms. This tool includes a trained hybrid model that analyses detailed network traffic and marks potential security violations or attacks.

Live Traffic Feed: Integration with network devices to capture real-time traffic.
Alert System: A notification system that alerts administrators when an attack is detected.
Visualisation Dashboard: A user-friendly interface that provides insights into traffic trends and alerts.

TABLE II
AUTOMATED RESPONSE PERFORMANCE

Dataset	Time (ms)	Accuracy (%)	False Positive(%)
CICIDS 2017	85	98.0	2.0
UNSW-NB15	90	97.5	2.5

D. Optimization Techniques

Several optimization strategies can be used to enhance further the IDS's performance: Hyperparameter tuning: To improve performance, model hyperparameters can be adjusted using methods like grid search or random search. Feature Selection: By selecting the most relevant features, the model can focus on critical traffic patterns, reducing overfitting and improving generalization. Model Ensemble: Combining the outputs of multiple models (ML and DL) through techniques such as stacking or boosting can provide a more robust detection system.

E. Model Evaluation

Model performance will be measured by the following criteria: Accuracy: The proportion of instances correctly labelled as attacks or normal traffic. Precision: The ratio of actual positive results out of all positive predictions. Recall (Sensitivity): The ratio of true positive instances that were properly classified. F1-Score: The harmonic mean of recall and precision, offering an even measurement of how well the model performs. AUC-ROC: The Area Under the Receiver Operating Characteristic curve, representing the model's capability to distinguish between attack and non-attack traffic.

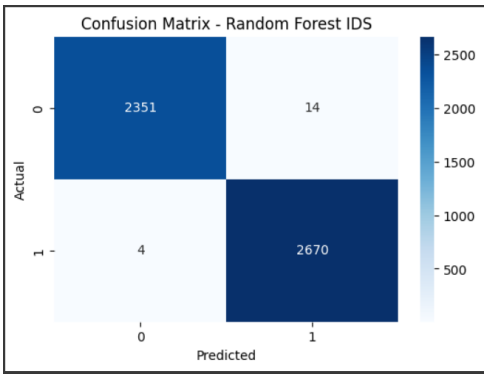

Fig. 2. Confusion Matrix CNN IDS

F. Performance Comparison

To effectively compare our system, we have benchmarked its performance against existing popular IDS models like SVM, CNN, RNN, and heuristic-based detection. These

are typical representatives of conventional as well as deep learning-based methods commonly used in current IDS research. The benchmarking was done by using the same dataset and same evaluation metrics for all the models. The perfor-

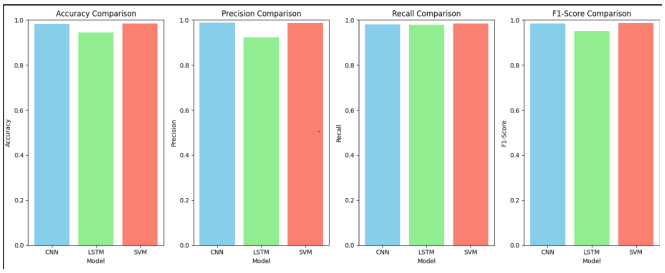

Fig. 3. CNN COMPARISON MODELS

mance of the ML and DL models is compared using the metrics above. The results are expected to show that the ML model, such as SVM, performs well for structured data, while the DL models (particularly CNN and LSTM) significantly exceed it in terms of accuracy and recall.

G. IDS Efficiency and Attack Detection Trends

The hybrid model demonstrates a high level of efficiency in detecting various attack types. For example: DoS Attacks: The model correctly identifies large amounts of malicious traffic, typical of DoS attacks, with minimal false positives.
Ransomware: By analysing traffic behaviour over time, the model accurately detects anomalous data exfiltration patterns associated with ransomware attacks.
Botnet: The model identifies traffic from botnet-controlled devices by recognising patterns indicative of coordinated, large-scale attack traffic.
Furthermore, the model is capable of identifying novel attacks that may not be present in training data, which is crucial for real-world deployments.

- Grid Search for hyperparameter tuning
- Mutual Information-based feature selection
- Model ensemble through boosting

V. CONCLUSION

This article presents a hybrid ML-DL-based IDS that effectively recognises a variety of network attacks, including DOS, ransomware, botnets, and more. Through a comprehensive assessment, it is clear that DL models, particularly CNN and LSTM, provide superior accuracy and identification compared to conventional mL models. The proposed system provides valuable insight into the efficiency of hybrid models when recognising intrusions in real time. Furthermore, implementing optimization techniques improves identity performance and provides a reliable means of practical delivery in a variety of network environments.

Future work could expand approaches to address additional attack types, integrate identity into larger cybersecurity systems, and develop fully operational real-time recognition tools.

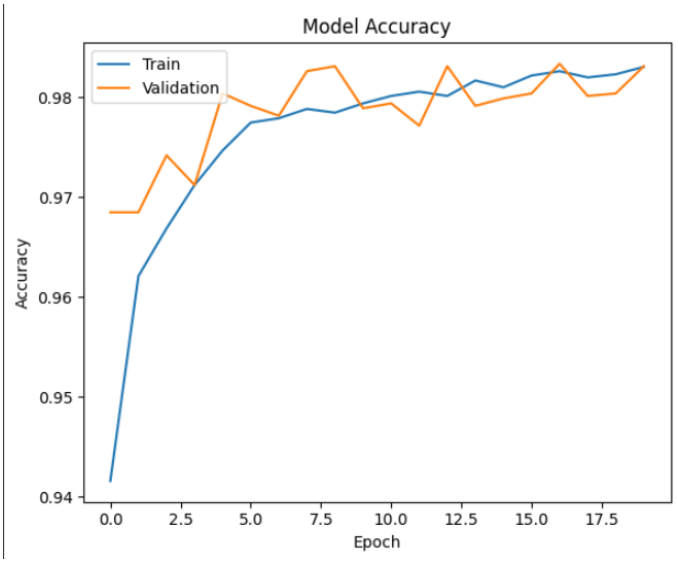

Fig. 4. Graph showing model accuracy for training and validation datasets.

REFERENCES

[1] Favour Okonkwo. Advanced intrusion detection in telemetry enterprise networks. International Foundation for Telemetering, 2024.

[2] Zeeshan Ahmad, Adnan Shahid Khan, Kashif Nisar, Iram Haider, Rosilah Hassan, Muhammad Reazul Haque, Seleviawati Tarmizi, and Joel JPC Rodrigues. Anomaly detection using deep neural network for iot architecture. *Applied Sciences*, 11(15):7050, 2021.

[3] Sharma Sidharth. Strengthening cloud security with ai-based intrusion detection systems. 2024.

[4] Lalit Kumar Vashishtha, Akhil Pratap Singh, and Kakali Chatterjee. Hidm: A hybrid intrusion detection model for cloud based systems. *Wireless Personal Communications*, 128(4):2637–2666, 2023.

[5] Vanlalruata Hnamte and Jamal Hussain. Dcnnbilstm: An efficient hybrid deep learning-based intrusion detection system. *Telematics and Informatics Reports*, 10:100053, 2023.

[6] William Villegas-Ch, Jaime Govea, Rommel Gutierrez, Alexandra Maldonado Navarro, and Aracely Mera-Navarrete. Effectiveness of an adaptive deep learning-based intrusion detection system. *IEEE Access*, 2024.

[7] Saad Hammood Mohammed, Mandeep S Jit Singh, Abdulmajeed Al-Jumaily, Mohammad Tariqul Islam, Md Shabiul Islam, Abdulmajeed M Alenezi, and Mohamed S Soliman. Dual-hybrid intrusion detection system to detect false data injection in smart grids. *PloS one*, 20(1):e0316536, 2025.

[8] Ruizhe Yao, Ning Wang, Peng Chen, Di Ma, and Xianjun Sheng. A cnn-transformer hybrid approach for an intrusion detection system in advanced metering infrastructure. *Multimedia Tools and Applications*, 82(13):19463–19486, 2023.

[9] Sana Tariq and Asjad Amin. Deepctf: transcription factor binding specificity prediction using dna sequence plus shape in an attention-based deep learning model. *Signal, Image and Video Processing*, 18(6):5239–5251, 2024.

[10] Ramkumar Devendiran and Anil V Turukmane. Dugat-lstm: Deep learning based network intrusion detection system using chaotic optimization strategy. *Expert Systems with Applications*, 245:123027, 2024.

[11] Anum Farooq and Kashif Hussain Memon. Kernel possibilistic fuzzy c-means clustering algorithm based on morphological reconstruction and membership filtering. *Fuzzy Sets and Systems*, 477:108792, 2024.

[12] Iram Haider, Muhammad Arslan Haider, and Arshad Saeed. Big data in internet of things: Architecture and open research challenges. In *2020 IEEE 23rd International Multitopic Conference (INMIC)*, pages 1–6, 2020.

[13] Fatmir Basholli, Adisa Daberdini, and Armand Basholli. Detection and prevention of intrusions into computer systems. *Advanced Engineering Days (AED)*, 6:138–141, 2023.

[14] Sudha Anbalagan, Gunasekaran Raja, Sugeerthi Gurumoorthy, Kaviyarasu Ayyakannu, et al. Blockchain assisted hybrid intrusion detection system in autonomous vehicles for industry 5.0. *IEEE Transactions on Consumer Electronics*, 69(4):881–889, 2023.

[15] Ulaa AlHaddad, Abdullah Basuhail, Maher Khemakhem, Fathy Elbouraey Eassa, and Kamal Jambi. Ensemble model based on hybrid deep learning for intrusion detection in smart grid networks. *Sensors*, 23(17):7464, 2023.

[16] Ankita Sharma, Shalli Rani, and Maha Driss. Hybrid evolutionary machine learning model for advanced intrusion detection architecture for cyber threat identification. *PloS one*, 19(9):e0308206, 2024.

[17] Samuel Oladiipo Olabanji, Yewande Marquis, Chinasa Susan Adigwe, Samson Abidemi Ajayi, Tunboson Oyewale Oladoyinbo, and Oluwaseun Oladeji Olaniyi. Ai-driven cloud security: Examining the impact of user behavior analysis on threat detection. *Asian Journal of Research in Computer Science*, 17(3):57–74, 2024.

[18] K Vaigandla, Nilofar Azmi, and R Karne. Investigation on intrusion detection systems (idss) in iot. *International Journal of Emerging Trends in Engineering Research*, 10(3), 2022.

[19] Subash Neupane, Jesse Ables, William Anderson, Sudip Mittal, Shahram Rahimi, Ioana Banicescu, and Maria Seale. Explainable intrusion detection systems (x-ids): A survey of current methods, challenges, and opportunities. *IEEE Access*, 10:112392–112415, 2022.

[20] Sunil Kumar Parisa and Somnath Banerjee. Ai-enabled cloud security solutions: A comparative review of traditional vs. next-generation approaches. *International Journal of Statistical Computation and Simulation*, 16(1), 2024.

[21] V Talati Dhruvitkumar. Ai-powered cloud security: Using user behavior analysis to achieve efficient threat detection. 2024.