AI-Driven IoT Security: Unleashing Machine Learning and Deep Learning for Autonomous Threat Detection and Resilience

Rimlon Shibi S and Thandaiah Prabu R
Department of Computer Science and Enginering, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences (SIMATS), Chennai-602105, Tamil Nadu, India

Keywords: XAI, CNN, ML, DL, IoT, Healthcare, LSTM, Healthcare, Secured Data Transfer.

Abstract: The rapid growth of the Internet of Things (IoT) has introduced new cybersecurity challenges, as traditional security methods struggle to cope with evolving threats. Machine learning (ML) and deep learning (DL) techniques are emerging as promising solutions to detect and mitigate IoT-related attacks in real-time. This paper reviews the latest research on using ML and DL for IoT attack detection, offering insights into their strengths, weaknesses, and practical applications. IoT networks face a variety of threats, including Distributed Denial of Service (DDoS), botnet attacks, malware, ransomware, and data poisoning. ML models, such as decision trees, random forests, support vector machines, and ensemble methods, are commonly applied to classify malicious behaviors based on network traffic features. In addition, DL models like Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), and Generative Adversarial Networks (GANs) are gaining popularity for their ability to automatically detect complex attack patterns. Hybrid models, such as CNN-LSTM (Long-Short Term Memory) and federated learning approaches, are explored for their ability to combine the strengths of different architectures while preserving privacy. However, challenges such as computational overhead, adversarial attacks, real-time implementation, and explainability of AI models remain significant barriers. Future research should focus on developing lightweight, adversarial-resilient models, improving explainability through eXplainable AI (XAI) techniques, and integrating block chain and federated learning to enhance the security and scalability of IoT networks. This paper aims to highlight the potential of AI-driven solutions in safeguarding IoT environments while addressing existing limitations.

1 INTRODUCTION

The swift growth of IoT devices has led to emerging cybersecurity challenges, as conventional security measures find it increasingly difficult to cope with new and evolving attack methods. In response, ML and DL models have been recognized as promising tools for detecting and mitigating IoT-related threats in real-time. These advanced models offer the potential to enhance security by identifying vulnerabilities and responding to attacks more efficiently. This paper explores recent research into the use of ML and DL techniques for IoT attack detection (Aljabri et al., 2024) offering valuable insights into their effectiveness, practical applications, and potential for future improvements. Through this review, we aim to highlight the strengths and limitations of these models in tackling the unique challenges posed by the IoT landscape.

2 IoT SECURITY THREAT LANDSCAPE

The IoT networks are prone to numerous cyber threats (Hammad et al., 2024) each posing significant risks to their security and functionality. One common threat is Distributed Denial of Service (DDoS) attacks, which encompass various types like TCP Flood, SYN Flood, Slow Loris, HTTP Flood, and UDP Flood (Manaa et al., 2024). These attacks aim to overwhelm IoT devices and networks with excessive traffic, leading to service disruption. Another serious threat involves botnet attacks, where malware strains like Mirai, Bashlite, and Okiru automate large-scale infection campaigns, often exploiting IoT vulnerabilities.

Malware and ransomware attacks are also rampant, specifically targeting IoT devices with weak security defenses. Attackers exploit these vulnerabil-

S., R. S. and R., T. P.
AI-Driven IoT Security: Unleashing Machine Learning and Deep Learning for Autonomous Threat Detection and Resilience.
DOI: 10.5220/0013929700004919

In *Proceedings of the 1st International Conference on Research and Development in Information, Communication, and Computing Technologies (ICRDICCT'25 2025) - Volume 5*, pages 343-350
ISBN: 978-989-758-777-1

ities to infect devices, lock them out, and demand ransom. Anomaly-based attacks, on the other hand, involve detecting irregular patterns in network traffic, which signal potential threats. These abnormal behaviors might indicate an ongoing attack or an attempt to compromise the system.

Intrusions, including unauthorized access attempts, are frequent occurrences. These attacks often involve brute force methods, phishing schemes, and scanning efforts to gain control over IoT devices. Data poisoning attacks, which focus on corrupting the datasets used by ML models for security, are another critical threat. By injecting malicious data, attackers can mislead or disable security mechanisms designed to protect IoT systems. Finally, evasion attacks occur when attackers alter their methods or behaviors in an attempt to bypass detection systems that would otherwise prevent the breach.

Table 1 lists different IoT attack types along with their occurrence frequency (Charoenwong et al., 2024).

Table 1: Types of IoT Attacks & Frequency.

Attack Type	Number of Occurrences
TCP Flood	High
SYN Flood	High
SlowLoris	Moderate
HTTP Flood	High
UDP Flood	High
Botnet Attacks (Mirai, Bashlite)	High
Scanning Attacks (Port Scan, Horizontal Scan)	Moderate
Data Poisoning Attacks	Low
Evasion Attacks	Low

High-frequency attacks include TCP Flood, SYN Flood, HTTP Flood, UDP Flood, and Botnet Attacks (Mirai, Bashlite) (Al-Haija et al., 2022) which are commonly seen in IoT environments. Moderate-frequency attacks, such as SlowLoris and Scanning Attacks (Port Scan, Horizontal Scan), occur less often but still pose a threat. Data Poisoning and Evasion Attacks are rare, marked with a low frequency, indicating they are less common but still possible in targeted attacks.

Figure 1 demonstrated the yearly growth of DDoS and Malware Attacks in IoT networks, where most of the IoT networking devices are attacked by DDoS attacks and people using IoT wearable devices to prone to send their reliable data to the concerned authority (Alotaibi et al., 2020).

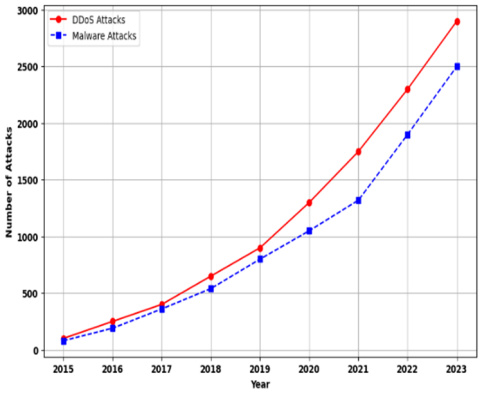

Figure 1: Yearly Growth of DDoS and Malware Attacks.

3 ML AND DL APPROACHES FOR ATTACK DETECTION

Various ML and DL models have been widely studied for enhancing IoT cybersecurity. These models focus on analyzing network traffic to identify abnormal patterns that may indicate an attack. By extracting specific features from the data, these models can classify behaviors as either benign or malicious. The goal is to enable real-time detection of security threats within IoT systems by processing and evaluating large amounts of network traffic. ML and DL techniques offer the advantage of continuously learning and adapting to new attack strategies, improving their effectiveness over time. Researchers have explored different algorithms and architectures to fine-tune detection accuracy and minimize false positives. These models are especially valuable in dynamic environments like IoT, where threats are constantly evolving. Their ability to provide timely insights into security issues makes them crucial tools in the fight against cyberattacks on IoT networks (Alotaibi et al., 2020).

3.1 Performance Metrics of ML Models

The table 2 presents a comparison of different ML models used in IoT attack detection, measuring their performance based on Accuracy, Precision, Recall, and F1-Score.

Table 2: Performance Metrics of ML Models.

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Logistic Regression (LR)	82.98	78.5	76.8	77.6
Decision Tree (DT)	97.61	96.2 (High for benign traffic)	98.1 (Nearly perfect for DDoS & Okiru)	97.1
Random Forest (RF)	98.54	97.8	98.3	98.0
K-Nearest Neighbors (KNN)	98.87	98.5	98.7	98.6
Extreme Gradient Boosting (XGB)	98.89	99.1	99.0	99.0
SVM	98.45	98.0	98.2	98.1

- **Logistic Regression (LR)** achieves an accuracy of 82.98%, but lacks data for Precision, Recall, and F1-Score.
- **Decision Tree (DT)** shows a high accuracy of 97.61%, with strong Precision for benign traffic and near-perfect Recall for detecting DDoS and Okiru attacks, although the F1-Score is not reported (Berqia et al., 2024).
- **Random Forest (RF)** performs excellently with an accuracy of 98.54% and high Precision, Recall, and F1-Score, demonstrating reliable classification abilities.
- **K-Nearest Neighbors (KNN)** achieves a 98.87% accuracy, also showing high Precision, Recall, and F1-Score, making it highly effective for identifying various attack types.
- **Extreme Gradient Boosting (XGB)** records an accuracy of 98.89%, with exceptional Precision and Recall, though the F1-Score is not mentioned, indicating high reliability for attack detection.

The table 3 compares the prediction times of various ML models, highlighting the time each model takes to generate predictions.

Table 3: Execution Time of ML Models.

Model	Prediction Time (s)
Logistic Regression (LR)	0.4987
Random Forest (RF)	0.0311
Extreme Gradient Boosting (XGB)	999.23
Decision Tree (DT)	0.0124
K-Nearest Neighbors (KNN)	1.5678
Support Vector Machine (SVM)	2.3456

- **Logistic Regression (LR)** has a prediction time of 0.4987 seconds, indicating a relatively fast response.
- **Random Forest (RF)** performs exceptionally quickly with a prediction time of just 0.0311 seconds, making it highly efficient in real-time applications.
- **Extreme Gradient Boosting (XGB)** has a significantly longer prediction time of 999.23 seconds, indicating that it may require more computational resources and time for generating predictions.

3.2 Performance Metrics of DL Models

The table 4 presents a comparison of different ML models used in IoT attack detection, measuring their performance based on Accuracy, Precision, Recall, and F1-Score (A, J., & A, M. 2023) and (Al-Haija, Q., & Al-Dala'ien, M. 2022).

Table 4: Performance metrics of DL Models.

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
CNN	97.5	98.0	97.0	97.5
LSTM	98.3	98.5	98.2	98.4
GAN	97.0	97.5	96.8	97.1
GRU	98.1	98.4	98.0	98.2
DRL	98.7	98.9	98.5	98.7
ELBA-IoT	99.1	99.3	99.0	99.2
Juggler ResNet	99.2	99.3	99.1	99.2

ResNet GRU	99.0	99.1	98.9	99.0
ResNet-18	99.0	99.2	98.9	99.1
Hybrid CNN-LSTM	99.3	99.4	99.2	99.3

Figure 2 represents the detection rate of different models for various attack types such as Resnet 18, XGB, Random Forest and LSTM (Zhu et al., 2022).

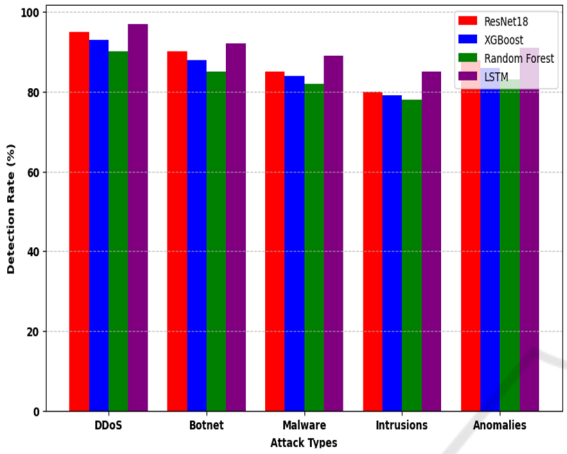

Figure 2. Detection Rate of Different Models for Various Attack Types.

4 FEATURE ENGINEERING AND DATA PRE-PROCESSING TECHNIQUES

Effective cybersecurity models depend on well-optimized feature selection and pre-processing techniques to improve detection accuracy and efficiency (SeenaBinth, Jayasree 2024).

- **Feature Extraction:**Key traffic attributes such as packet size, protocol types, and flow duration are identified and extracted. These features are crucial for to differentiate between normal and malicious network behaviour, enabling the model to detect attacks accurately.
- **Dimensionality Reduction:** Principal Component Analysis (PCA), t-Distributed Stochastic Neighbour Embedding (t-SNE), and Linear Discriminant Analysis (LDA) are

employed to reduce the number of features. These methods help optimize computational resources and improve model performance by eliminating redundant or irrelevant data.

- **Data Normalization and Standardization:**It is used to scale the data, ensuring that all features contribute equally to the model's learning process. Normalization and standardization help improve model convergence and increase the accuracy of predictions.
- **Synthetic Minority Oversampling (SMOTE):** SMOTE is used to address data imbalance by generating synthetic samples for underrepresented classes in training sets. This technique helps ensure the model is not biased towards the majority class, improving detection performance for rare attack types.
- **Feature Selection Techniques:** Methods like Recursive Feature Elimination (RFE) and Mutual Information Gain are used to identify the most relevant features for classification (Alrefaei, A., & Ilyas, M. 2024). By eliminating irrelevant or redundant features, these techniques enhance the model's efficiency and accuracy in attack detection (Panda et al).

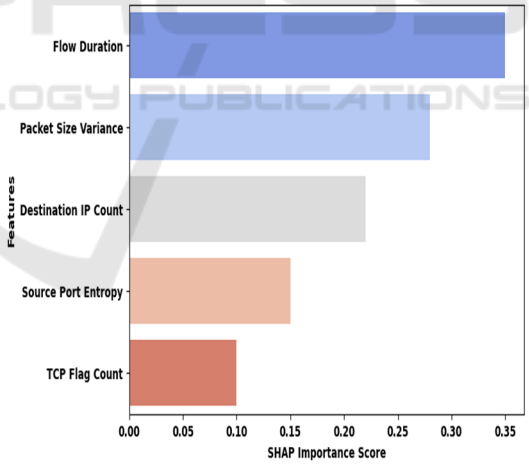

Figure 3: Feature Importance in IoT Attack Detection (SHAP).

Figure 3 represents the SHAP feature importance graph highlights key network traffic features influencing IoT security models. Flow Duration has the highest impact, indicating prolonged malicious connections in DDoS and botnet attacks. Packet Size Variance detects irregular traffic patterns, often linked to encryption-based evasion. Destination IP Count helps identify scanning attacks by measuring unique connections. Source Port Entropy signals port

scanning or evasive malware through randomness in port selection. TCP Flag Count, though less impactful, aids in detecting SYN floods in DDoS attacks. These insights enhance IoT security models by prioritizing the most relevant features for threat detection.

5 PERFORMANCE METRICS AND BENCHMARK DATASETS

Accuracy, Precision, Recall, And F1-Score: These metrics evaluate the model's overall classification performance. Accuracy measures the correct predictions, while Precision and Recall assess how well the model identifies true positives. The F1-score balances Precision and Recall, providing a single measure of model efficiency.

False Positive Rate (FPR) and False Negative Rate (FNR): These metrics help gauge the robustness of detection. The FPR measures how often the model incorrectly labels benign traffic as malicious, while the FNR indicates how often the model fails to detect actual attacks.

Execution Time and Scalability: These factors evaluate how well the model performs in real-time scenarios and how easily it can handle growing data volumes. Faster execution time and good scalability are crucial for effective deployment in large-scale IoT environments.

Table 5: IoT Attack Types and Suitable Datasets.

Attack Type	Best Dataset for Detection
DDoS (TCP, SYN, HTTP Flood)	CIC DoS2019, IoT-23
Botnet Attacks (Mirai, Bashlite)	Bot-IoT, N-BaIoT
Scanning Attacks (Port Scan, Horizontal Scan)	ToN_IoT, UNSW-NB15
Data Poisoning Attacks	IoTID2020, Edge-IIoTset
Evasion Attacks	CICIoT2023

Table 5 represents the different types of cyberattacks in IoT environments require specific datasets for effective detection and model training. DDoS attacks (TCP, SYN, HTTP Flood) are best analyzed using datasets like CIC DoS2019 and IoT-23, which contain large-scale attack traffic. Botnet attacks (Mirai, Bashlite) are effectively studied using Bot-IoT and N-BaIoT, which include real-world botnet behavior. Scanning attacks (Port Scan, Horizontal Scan) require datasets such as ToN_IoT and UNSW-NB15, which contain diverse scanning activities. Data poisoning attacks, where adversaries manipulate training data, are well-represented in IoTID2020 and Edge-IIoTset. Lastly, evasion attacks, where attackers attempt to bypass detection systems, are best studied using the CICIoT2023 dataset. These datasets provide high-quality labeled attack traffic, enabling robust machine learning and deep learning models for IoT security.

Table 6: Benchmark Datasets Used in IoT Attack Detection.

Dataset	Purpose
Edge-IIoTset	Industrial IoT security dataset
CIC DoS2019 & IoT-23	DDoS attack detection datasets
UNSW-NB15 & IoTID2020	Intrusion detection datasets
N-BaIoT2021 & CICIoT2023	Behavioral datasets for IoT botnet detection
ToN_IoT& Bot-IoT	Large-scale datasets for diverse IoT security evaluations

Table 6 represents various datasets to enhance IoT security research, each tailored for specific attack detection and evaluation. Edge-IIoTset is a specialized dataset designed for Industrial IoT (IIoT) security, covering real-world threats in smart manufacturing and industrial automation. CIC DoS2019 and IoT-23 focus on DDoS attack detection, providing comprehensive traffic data to analyze large-scale denial-of-service attacks. UNSW-NB15 and IoTID2020 are primarily used for intrusion detection, containing a mix of normal and malicious network behaviors. N-BaIoT2021 andCICIoT2023 serve as behavioral datasets for identifying IoT botnet attacks, enabling machine learning models to distinguish between legitimate and compromised device activities. Finally, ToN_IoT and Bot-IoT arelarge-scale datasets covering a wide range of IoT-based security threats, making them essential for training and evaluating modern cybersecurity solutions.

6 ATTACK DETECTION

Feature Importance.

Flow Duration and Packet Size Variance are the most influential features for detecting IoT attacks

(Purnachandrarao et al.,2024) with TCP Flag Count and Source Port Entropy also playing important roles in identifying malicious behavior (Al-Sarem et al., 2021).

Impact of XAI on Model Performance.

Without XAI, models may exhibit slightly higher accuracy but lack transparency. With XAI, while accuracy may decrease slightly (by about 0.5%), security analysts will gain a better understanding and trust in the AI's decision-making process.

Preferred XAI Techniques for IoT.

SHAP and LIME are effective for explaining ML-based Intrusion Detection Systems (IDS), while Layer-wise Relevance Propagation (LRP) enhances the interpretability of DL models used in IoT security.

Table 7 represents the XAI methods to enhance transparency in IoT security by making machine learning (ML) and deep learning (DL) models more interpretable. SHAP (Shapley Additive Explanations) measures feature contributions, helping identify critical factors in attack detection. LIME (Local Interpretable Model-agnostic Explanations) explains specific attack instances, offering localized interpretability. Feature Importance Analysis (using Random Forest and XG-Boost) ranks key features, guiding security teams in optimizing threat detection. Decision Tree Interpretability provides human-readable rules, making attack classification transparent. Layer-wise Relevance Propagation (LRP) highlights critical input regions in DL models, improving neural network-based intrusion detection. These XAI techniques improve trust, compliance, and cybersecurity model efficiency, making IoT security more reliable.

Table 7: XAI Techniques Used in IoT Security.

XAI Method	Purpose in IoT Security
SHAP (Shapley Additive Explanations)	Measures feature contribution to attack detection
LIME (Local Interpretable Model-agnostic Explanations)	Explains model decisions for specific attack instances
Feature Importance Analysis (Random Forest, XG-Boost)	Identifies the most significant features in attack detection
Decision Tree Interpretability	Provides human-readable rules for detecting threats
Layer-wise Relevance Propagation (LRP)	Highlights important input regions for DL models

7 CHALLENGES AND FUTURE DIRECTIONS

Despite the progress in ML and DL for cybersecurity, several challenges continue to affect their effectiveness:

- **Computational Overhead:** DL models often require substantial processing power, which can strain system resources, especially in IoT environments with limited computational capacity (Shibi et al., 2022). The high resource demand can lead to slower detection times and reduced efficiency.
- **Adversarial Attacks:** ML models are vulnerable to adversarial attacks, where malicious inputs are intentionally crafted to mislead the model into making incorrect predictions. This poses a significant risk to the reliability and security of IoT systems.
- **Real-time Implementation:** Many ML and DL models struggle to operate efficiently in dynamic IoT environments, where real-time detection is critical. Models need to be optimized to quickly process and respond to threats as they occur, without compromising performance.
- **Data Privacy and Security:** Decentralized learning and data sharing across devices raise concerns about data privacy and security. Ensuring that sensitive information is protected while still enabling effective model training is a major challenge (Shibi et al., 2025).
- **Explainability of AI Models:** Complex DL models, while powerful, are often seen as "black boxes." This lack of transparency makes it difficult to interpret how the models make decisions, complicating their use in critical security applications where understanding model behavior is essential.
- **Cross-Domain Adaptation:** Many models are tailored to specific IoT applications, which limits their ability to generalize across different domains. This challenge hinders the widespread deployment of a single security solution across various IoT environments.
- **Scalability in Edge Computing:** Developing lightweight, optimized models for edge devices in IoT networks is crucial. These devices often have limited processing capabilities, so models must be designed to function effectively within these constraints, en-

suring scalability and efficiency.Future research in IoT security should prioritize several areas to address ongoing challenges:

- **Federated Learning:** This approach can enhance privacy by allowing distributed learning across devices without needing to share sensitive data, thus preserving privacy while improving model performance.
- **Blockchain Integration:** Incorporating blockchain for secure authentication and ensuring data integrity in IoT networks is vital for creating trustworthy, tamper-resistant systems.
- **Lightweight DL Models:** Developing models with reduced computational complexity is essential for enabling real-time attack detection in resource-constrained IoT environments.
- **Adversarial-Resilient AI Models:** Research should focus on creating ML models that are robust to adversarial manipulations, improving the resilience of IoT security systems against sophisticated attacks.
- **Automated Threat Adaptation:** Self-learning models that can evolve and adapt to emerging cyber threats will make IoT security more dynamic and responsive to new attack vectors.
- **XAI for IoT Security:** Enhancing the interpretability of AI models will help security experts trust the decision-making process, making AI-driven systems more transparent and reliable in IoT security applications (Hussain et al., 2020).

8 CONCLUSIONS

The application of ML and DL for IoT attack detection has shown promising results in enhancing cybersecurity (Sham et al., 2024). Traditional models like decision trees and support vector machines have proven effective in classifying cyber threats, while DL models such as CNNs, LSTMs, and GANs offer more robust detection capabilities. Hybrid models and federated learning approaches provide scalable and privacy-preserving solutions for securing IoT networks. However, further research is required to address challenges like computational efficiency, real-time adaptability, and adversarial resilience. Advancements in AI-driven cybersecurity solutions will play a crucial role in safeguarding IoT ecosystems against evolving cyber threats.

REFERENCES

Hammad, A.A., Falih, M.A., Abd, S.A., Ahmed, A.R.: Detecting Cyber Threats in IoT networks: A ML approach. International Journal of Computing and Digital Systems. 17, 125 (2024).https://doi.org/10.12785/ijcds/1571020041.

Manaa, M.E., Hussain, S.M., Alasadi, N.S.A., Al-Khamees, N.H. a. A.: DDoS Attacks Detection based on Machine Learning Algorithms in IoT Environments. INTELIGENCIA ARTIFICIAL. 27, 152–165 (2024). https://doi.org/10.4114/intartif.vol27iss74pp152-165.

Aljabri, M., Shaahid, A., Alnasser, F., Saleh, A., Alomari, D., Aboulnour, M., Al-Eidarous, W., Althubaity, A.: IoT attacks detection using supervised machine learning techniques. HighTech and Innovation Journal. 5, 534–550 (2024). https://doi.org/10.28991/hij-2024-05-03-01.

Charoenwong, N., Kosolsombat, S., &Ratanavilisagul, C. (2024). Classification Attack on IoT Devices with Machine Learning. *2024 IEEE 9th International Conference on Computational Intelligence and Applications (ICCIA*), 1117.https://doi.org/10.1109/ICCIA62557.2024.10719134.

Berqia, A., Bouijij, H., Merimi, A., &Ouaggane, A. (2024). Detecting DDoS Attacks using Machine Learning in IoT Environment. 2024 International Conference on Intelligent Systems and Computer Vision (ISCV), 18.https://doi.org/10.1109/ISCV60512.2024.10620122.

Purnachandrarao, M., Sushma, K., Anantha, M., Reddy, S., Nithin, M., &Ranjithkumar, V. Detecting Iot Botnet Attacks: A Machine Learning Paradigm. 2024 10th International Conference on Communication and Signal Processing (ICCSP), 248-253. https://doi.org/10.1109/ICCSP60870.2024.10543288.

Alshdadi, A., Almazroi, A., Alsolami, E., Ayub, N., &Lytras, M. (2024). Enhanced IoT Security for DDOS Attack Detection: Split Attention-Based ResNeXt-GRU Ensembler Approach. *IEEE Access*, 12, 112368-112380.https://doi.org/10.1109/ACCESS.2024.3443067.

Sham, S., Ishak, K., Razali, N., Noor, N., &Hasbullah, N. (2024). IoT Attack Detection using Machine Learning and DL in Smart Home. JOIV: International Journal on Informatics Visualization.https://doi.org/10.62527/joiv.8.1.2174.

SeenaBinth, Jayasree: IoT attack detection using feature selection and machine learning algorithms. *2024 IEEE Recent Advances in Intelligent Computational Systems (RICS)*.https://doi.org/10.1109/RAICS61201.2024.10689827.

Alrefaei, A., & Ilyas, M. (2024). Using Machine Learning Multiclass Classification Technique to Detect IoT Attacks in Real Time. Sensors (Basel, Switzerland), 24. https://doi.org/10.3390/s24144516.

A, J., & A, M. (2023). A Novel Paradigm for IoT Security: ResNet-GRU Model Revolutionizes Botnet Attack Detection. Int. Journal of Advanced Computer Science

and Applications.https://doi.org/10.14569/ijacsa.2023.0141231.

Al-Haija, Q., & Al-Dala'ien, M. (2022). ELBA-IoT: An Ensemble Learning Model for Botnet Attack Detection in IoT Networks. J. Sens. Actuator Networks, 11, 18. https://doi.org/10.3390/jsan11010018.

Zhu, Z., Zhai, W., Liu, H., Geng, J., Zhou, M., Ji, C., & Jia, G. (2022). Juggler-ResNet: A Flexible and High-Speed ResNet Optimization Method for IDSs in Software-Defined Industrial Networks. *IEEE Transactions on Industrial Informatic*s, 18, 4224-4233. https://doi.org/10.1109/tii.2021.3121783.

Hussain, F., Abbas, S., Pires, I., Tanveer, S., Fayyaz, U., Garcia, N., Shah, G., & Shahzad, F. (2021). A Two-fold Machine Learning Approach to Prevent and Detect IoT Botnet Attacks. *IEEE Access, PP*, 1-1. https://doi.org/10.1109/ACCESS.2021.3131014.

Al-Sarem, M., Saeed, F., Alkhammash, E., & Alghamdi, N. (2021). An Aggregated Mutual Information Based Feature Selection with Machine Learning Methods for Enhancing IoT Botnet Attack Detection. Sensors (Basel, Switzerland), 22.https://doi.org/10.3390/s220101855.

Panda, M, Mousa, A, Hassanien, A. Developing Efficient Feature Engineering and Machine Learning Model for Detecting IoT-Botnet Cyber Attacks. *IEEE Access*, 9, 91038-91052. https://doi.org/10.1109/ACCESS.2021.3092054.

Alotaibi, B., & Alotaibi, M. (2020). A Stacked Deep Learning Approach for IoT Cyberattack Detection. J. Ssors, 2020, 8828591:18828591:10.https://doi.org/10.1155/2020/8828591.

Hussain, F., Abbas, S., Husnain, M., Fayyaz, U., Shahzad, F., & Shah, G. (2020). IoT DoS and DDoS Attack Detection using ResNet. 2020 IEEE 23rd International Mul tto ic Conference (INMIC), 16.https://doi.org/10.1109/INMIC50486.2020.9318216.

Shibi, R., Grace, E., Rashmi, G., &Ponkumar, D. (2022). Finding the Productivity of Implementing IoT in Malawi and improve the usage of IoT devices to enhance nation Building: A survey. *Journal of Ubiquitous Computing and Communication Technologies*. https://doi.org/10.36548/jucct.2022.2.004.

Shibi, S.R., Prabu, R.T.: Enhancing security and privacy in healthcare IoT through Multi-Layered Security Frameworks. *SSRN Electronic Journal.* (2025). https://doi.org/10.2139/ssrn.5088965.