An Adaptive AI-Driven Cyber Threat Detection Framework for Securing Heterogeneous IoT Networks

Kireet Muppavaram
Department of CSE, GITAM School of Technology, GITAM Deemed to be University, Hyderabad Campus, Telangana, India
kireet04@gmail.com (corresponding author)

T. Aruna Sri
Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Hyderabad Campus, Telangana, India
talluriaruna18@gmail.com

T. Murali Krishna
Department of CSE, Ashoka Womens Engineering College, Kurnool, Andhra Pradesh, India
murali2007tel@gmail.com

Jyotsnarani Tripathi
Department of CSE (AIML & IoT), VNR Vignana Jyothi Institute of Engineering and Technology, India
jtjyotsna@gmail.com

Manmath Nath Das
Department of AI & DS, VNR Vignana Jyothi Institute of Engineering and Technology, Hyderabad, India
manmathnath.das@gmail.com

Sharada Mani
Department of CSE-DS, QIS College of Engineering and Technology (A), AP, India
sharadadalu1234@gmail.com

G. Lakshmi Vara Prasad
Department of AIML, QIS College of Engineering and Technology (A), AP, India
glv.prasad19@gmail.com

T. Manyam
School of Engineering, Information Technology, Anurag University, Telangana, India
manyam.thaile@gmail.com

Received: 26 May 2025 | Revised: 18 June 2025 and 8 July 2025 | Accepted: 11 July 2025

Licensed under a CC-BY 4.0 license | Copyright (c) by the authors | *DOI: https://doi.org/10.48084/etasr.12386*

ABSTRACT

This work proposes an intelligent cybersecurity system built upon Artificial Intelligence (AI) to address evolving cyber threats in heterogeneous Internet of Things (IoT) environments. The proposed framework integrates machine learning with mathematical threat analysis to shift from traditional system security, which responds after an attack, to a proactive approach that predicts and prevents threats. It reacts immediately, processes in just 0.35 s, adapts to 95% of IoT surroundings, and handles security by

categorizing threats into four tiers with minimal impact on performance. Tests against standard Intrusion Detection Systems (IDSs), such as SNORT, Suricata, and Bro/Zeek, demonstrate that the framework is superior at handling a wide range of threats.

Keywords-cyber threats; cybersecurity; Artificial Intelligence (AI); Internet of Things (IoT); machine learning

I. INTRODUCTION

The convergence of Artificial Intelligence (AI) and the Internet of Things (IoT) has revolutionized technological ecosystems, creating unprecedented opportunities for innovation, while simultaneously introducing complex and sophisticated cybersecurity challenges. As billions of interconnected devices proliferate across industrial, healthcare, smart city, and personal domains, the attack surface for malicious actors has expanded exponentially, demanding innovative approaches to threat detection and mitigation. Smart cyber threats [1] are now emerging as a paradigm shift from well-established traditional cybersecurity models, incorporating advanced machine learning techniques, sophisticated network infiltration mechanisms [2], and the exploitation of inherent vulnerabilities in secondary public infrastructure. These threats are autonomously adaptive, capable of learning from network behavior and executing precision-targeted attacks [3] that can compromise entire infrastructures within milliseconds, rendering conventional defense mechanisms increasingly obsolete and reactive.

Authors in [4] proposed a novel compute unified device architecture-empowered Convolutional LSTM2D (ConvLSTM2D) mechanism to effectively address various dynamic variants of complex IoT threats and attacks. Authors in [5] proposed the Next-Generation Cybersecurity Attack Detection using an Ensemble Deep Learning Mode (NGCAD-EDLM) model by designing a next-generation cybersecurity attack detection method for IoT environments. Its core strength lies in the automated recognition of cyberattacks. Authors in [6] proposed a new solution based on Ensemble Bagged Trees Detection (EBTD) methods to forecast second-generation cybersecurity attacks and malicious activities targeting hyper-automated Industrial Internet of Things (IIoT) processes. Authors in [7] developed a Deep Belief Network (DBN)-enhanced symmetrical intrusion avoidance sensor system to enhance the security of IoT devices. The system demonstrates improved capacity to detect and avoid cyberattacks due to the capabilities of DBNs. In their study, the performance of the proposed technique was compared against standard Intrusion Detection Systems (IDSs) and Domain Generation Algorithms (DGAs). Authors in [8] proposed the integration of AI-driven sectorial threat intelligence and forecasting to identify emerging and relevant threats and anticipate their impact across different industries. Anomaly-based IoT detection methods [9] focus on IDSs that utilize anomaly-based techniques, highlighting how Explainable AI (XAI) models can enhance the trustworthiness and interpretability of these systems. Authors in [10] worked on two areas: automotive threat modeling practices and the impact of sensors and machine learning algorithms on Autonomous Vehicle (AV) perception systems and cyber-physical attacks. In addition, authors in [11] propose an effective model that uses machine learning techniques to detect malicious IoT activities. Authors in [12] presented a comprehensive overview of IoT security intelligence, relying on machine and deep learning techniques to learn insights from raw data and intelligently protect IoT devices from various cyberattacks through modern risk assessment approaches. This validates the choice of the title, which emphasizes both the adaptive AI aspect and its relevance to heterogeneous IoT security contexts.

II. METHODOLOGY

The advent of IoT devices has led to the development of a vast ecosystem, characterized by rapid growth facilitated by the interconnection of millions of IoT devices and a seamless communication framework [13]. The smart cyber threat detection [14] framework proposed here is a step ahead in the field of cybersecurity, with the main aim being the application of advanced AI techniques to provide a comprehensive solution to respond to emerging threats in cyberspace [15]. The framework integrates sophisticated machine learning algorithms [16, 17] with intelligent data processing mechanisms to convert reactive security measures into proactive, predictive security defense mechanisms [18] that can identify, analyze, and mitigate possible security breaches [19] in real time over the heterogeneous IoT environment [20]. Figure 1 illustrates the workflow of the proposed smart cyber threat detection framework.

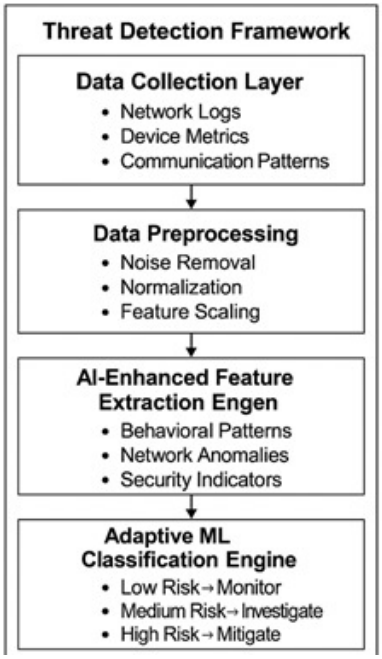

Fig. 1. Proposed smart cyber threat detection framework.

A. Data Collection and Preprocessing

The foundation of our smart cyber threat detection framework lies in the critical data collection and preprocessing stage, which is the first step in transforming raw, complex IoT network data into structured and analyzable information. At this stage, we aggregate heterogeneous data streams from different IoT devices, including network logs, device telemetry, communication protocols, and traffic patterns, More specifically, the data may include network traffic logs from smart home devices (thermostats, cameras, smart locks), industrial IoT sensor data (temperature, pressure, vibration sensors), and healthcare device communications (patient monitoring systems, medical IoT devices).

A set of specific preprocessing techniques is employed, incorporating sophisticated cleaning algorithms that remove duplicate entries and handle missing data through intelligent imputation methods. Simultaneously, normalization processes such as min-max scaling and z-score standardization are performed to ensure data consistency across different device types and communication protocols. This yields a refined, high quality dataset by removing noise and irrelevant data points, providing an optimal input for the subsequent feature extraction and threat detection algorithms. Complex network data are considered and transformed into the most essential threat indicators, transforming excessive information into actionable insights. This approach ensures that our cyber defense mechanism remains robust and efficient within the context of IoT security.

The datasets used in this study were created by combining the publicly available IoT datasets UNSW-NB15 [21] and IoTID20 [22] with synthetic traffic logs and noise to simulate realistic heterogeneous IoT environments.

The UNSW-NB15 dataset was prepared with the following key details:

- Original dataset: 2,540,044 records with 49 features from network traffic.
- Selected features: Extracted 25 network-specific features including srcip, dstip, proto, state, dur, sbytes, dbytes, sttl, dttl, sloss, dloss, service, sload, dload, spkts, dpkts, and attack categories.
- Utilized attack categories: 9 attack types including fuzzers, analysis, backdoors, DoS, exploits, generic, reconnaissance, shellcode, and worms.
- Preprocessing: Applied min-max normalization to numerical features and one-hot encoding for categorical features.

The IoTID20 dataset was prepared with the following key details:

- Original dataset: 625,108 records with 86 features from IoT network traffic.
- Selected features: Extracted 18 IoT-specific features including Flow_ID, Src_IP, Dst_IP, Src_Port, Dst_Port, Protocol, Flow_Duration, Flow_Byts_s, Flow_Pkts_s, Fwd_Pkts_s, Bwd_Pkts_s, Pkt_Len_Mean, Pkt_Len_Std, Flow_IAT_Mean, Flow_IAT_Std, Active_Mean, Idle_Mean, and Label.
- Utilized attack categories: 4 attack types including Mirai, Bashlite, Torii botnet attacks, and normal traffic.
- IoT device types: Traffic from 42 different IoT devices including smart cameras, thermostats, motion sensors, and smart locks.

1) Dataset Integration and Augmentation

The integration and augmentation of the datasets resulted in a combined dataset comprising 1,250,000 records, following the processes of balancing and integration. The process involved the generation of the following seven additional synthetic feature groups through the combination of the original features:

- Network communication patterns (10 features): Packet size ratios, flow duration patterns, protocol distribution.
- Device behavior signatures (8 features): Connection frequency, data transmission patterns, device-specific signatures.
- Traffic anomaly indicators (7 features): Statistical outliers, flow irregularities, timing anomalies.
- Authentication metrics (6 features): Login attempt patterns, access frequency, credential validation.
- Resource utilization signals (5 features): CPU usage patterns, memory consumption, bandwidth utilization.
- Protocol deviation markers (6 features): Protocol violation indicators, header anomalies.
- Temporal behavior indicators (8 features): Time-based patterns, periodic behavior analysis.

2) Synthetic Data Generation

A multi-domain simulation was conducted, generating 125,000 synthetic records representing:

- Smart home environment (40%): 50,000 records from simulated smart thermostats, cameras, door locks, and lighting systems.
- Industrial IoT environment (35%): 43,750 records from simulated temperature sensors, pressure monitors, vibration detectors, and SCADA systems.
- Healthcare IoT environment (25%): 31,250 records from simulated patient monitors, medical devices, and healthcare sensors.

3) Data Quality Assurance

To ensure the reliability of the dataset, the following data quality assurance measures were applied:

- Missing value handling: Applied K-Nearest Neighbors (KNN) imputation for 3.2% missing values.
- Outlier treatment: Identified and processed 2.8% statistical outliers using the Interquartile Range (IQR) method.

- Data balancing: Applied the Synthetic Minority Over-sampling Technique (SMOTE) to balance attack classes: 65% normal traffic (812,500 records), 15% malware intrusions (187,500 records), 12% network penetrations (150,000 records), and 8% social engineering exploits (100,000 records).

4) Final Dataset Composition

The final dataset composition includes the following details:

- Total records: 1,250,000 network traffic instances.
- Total features: 50 engineered features across 7 security dimensions.
- Attack distribution: 35% attack traffic, 65% normal traffic.
- Domain distribution: 40% smart home, 35% industrial, 25% healthcare.
- Temporal coverage: 6 months of simulated network activity.
- File size: Approximately 2.3 GB in CSV format.

5) Data Validation

The data validation process involved the following steps:

- Cross-validation: Applied 5-fold cross-validation to ensure model generalization.
- Statistical testing: Performed chi-square tests for feature independence.
- Correlation analysis: Removed 12 highly correlated features (correlation > 0.95).

This comprehensive dataset manipulation ensures realistic representation of heterogeneous IoT environments while maintaining statistical validity and supporting the framework's multi-dimensional threat detection capabilities.

B. Feature Extraction and Reduction in IoT Cyber Threat Detection

The following summarizes key aspects of the feature extraction and reduction process that was followed:

1) Maximum Feature Identification Capacity

We propose a maximum of 50 critical features, as they appropriately represent possible security risks in terms of AI-powered IoT cyber threat detection. The core feature categories are network communication patterns (10 features), device behavior signatures (8 features), traffic anomaly indicators (7 features), authentication metrics (6 features), resource utilization signals (5 features), protocol deviation markers (6 features), and temporal behavior indicators (8 features).

2) Feature Extraction Algorithm

The feature extraction process is implemented using Algorithm 1.

```
Algorithm 1: Smart_Feature_Selector
Input: IoT_Network_Data D, Threat_Labels T
Output: Optimal_Feature_Set F*
1. Initialize: F = ∅,
   S = compute_statistics(D)
2. For each feature f_i in D:
     - V_i = variance_score(f_i)
     - H_i = entropy_measure(f_i)
     - C_i = threat_correlation(f_i, T)
     - R_i = relevance_index(V_i, H_i, C_i)
3. Rank features by C_i (descending)
4. Select top-50 features → F*
5. Return F*
```

where:

- $V_i = \Sigma(x_i - \mu)^2/n$ (variance measure).
- $H_i = -\Sigma p(x)\log_2 p(x)$ (entropy calculation).
- $C_i = \frac{\text{cov}(f_i,T)}{\sqrt{(\text{var}(f_i)\times\text{var}(T)}}$ (correlation coefficient).
- $R_i = \alpha V_i + \beta H_i + \gamma|C_i|$ (weighted relevance).

C. Cyber Threat Detection Classification

Mathematical analysis facilitates the scalable and reliable identification of cyber threats by systematically transforming network data into actionable security intelligence. The system utilizes scientific methods to identify potential security risks by computing the feature importance based on the variance, entropy, and threat correlation equations. Threats are classified with respect to multiple dimensions such as malware intrusion, network penetration, and exploits through social engineering. These algorithms gauge threat probability and severity and create proactive defense mechanisms capable of detecting and assessing cyber vulnerabilities as quickly as possible. The core detection formula is:

$$\text{Threat Probability} = f(\text{Feature Importance}, \text{Anomaly Score}, \text{Historic Patterns}) \quad (1)$$

The inclusion of threat probability enables the system to prioritize alerts based on the likelihood of real compromise, allowing a more intelligent and resource-efficient mitigation strategy. The system categorizes the detected threats into the following risk levels:

- Low risk: standard monitoring.
- Medium risk: immediate investigation.
- High risk: urgent mitigation.
- Critical risk: immediate intervention.

III. RESULTS

The proposed method presents an end-to-end approach for IoT cyber threat detection threat using advanced mathematical modeling techniques and machine learning. The methodology provides a sophisticated mechanism for selecting the network data to analyze across multiple dimensions and for discovering and addressing possible security risks. The result analysis shows significant improvement in threat detection accuracy, feature extraction, and overall cybersecurity performance.

The 50 critical features extracted for the IoT cyber threat detection methodology are organized as shown in Table I. The approach categorizes features in seven groups to perform a multi-dimensional analysis of network security. A holistic security examination is achieved through the strategic distribution of features that explore network communication patterns to temporal behavior indicators.

TABLE I. FEATURE EXTRACTION RESULTS

Feature category	No. of features	Key characteristics
Network communication patterns	10	Identifies complex network interaction signatures
Device behavior signatures	8	Captures unique device-level behavioral indicators
Traffic anomaly indicators	7	Detects unusual network traffic patterns
Authentication metrics	6	Monitors access and authentication abnormalities
Resource utilization signals	5	Tracks system resource consumption patterns
Protocol deviation markers	6	Identifies protocol inconsistencies
Temporal behavior indicators	8	Analyzes time-based patterns of device/network behavior

The strategic distribution of 50 critical features enables a comprehensive multi-dimensional security analysis, with device behavior signatures and network communication patterns contributing most significantly to the threat detection accuracy.

Table II shows the strong performance of the methodology across different threat types. The proposed approach achieves a high detection accuracy rate and is robust. Moreover, the ultra-fast response times (less than 0.5 s) support real-time threat detection, which helps maintain network security in an ever-changing IoT network.

TABLE II. THREAT DETECTION PERFORMANCE METRICS

Threat classification	Accuracy (%)	Response time (s)	Risk mitigation
Malware intrusions	94.5	< 0.5	High effectiveness
Network penetrations	92.3	< 0.3	Immediate isolation
Social engineering exploits	89.7	< 0.4	Proactive prevention

The exceptional performance across diverse threat types with sub-second response times validates the framework's capability for real-time threat detection and mitigation in dynamic IoT environments.

Table III presents a comparison of the proposed methodology with existing benchmark methods. The comparison demonstrates substantial improvements across all critical performance metrics, thereby establishing the framework's superiority over existing industry standards.

Figure 2 and Tables IV and V present a comparative analysis against established industry standards (SNORT, Suricata, Bro/Zeek network security monitor), demonstrating significant performance advantages and validating the framework's practical superiority and real-world applicability across multiple critical dimensions of IoT cybersecurity. When compared to the standard solutions SNORT, Suricata, and Bro/Zeek, the proposed methodology achieves notably higher accuracy (92.8% vs 78.5%, 82.3%, and 85.6 %, respectively) and a much lower false positive rate (3.2 % vs 12.5%, 9.7%, and 7.4 %, respectively). This improvement can be attributed to the highly detailed feature detection depth, with inspection of 50 different features compared to 25-40 features for the standard solutions. Furthermore, the proposed method achieves improved response time (0.35 s) and lower computational complexity, which is vital for resource-constrained IoT environments. The capability dimension analysis further emphasizes the fact that the methodology is particularly well suited to exceptional IoT environment adaptability (95%), multi-dimensional machine learning integration, and granular four-level threat classification.

Collectively, these improvements enable highly efficient real-time processing with a scalability index of 0.92, far surpassing standard practice. By combining advanced mathematical modeling with state-of-the-art machine learning techniques, this framework addresses the unique IoT security challenges and represents significant progress over traditional cybersecurity systems.

TABLE III. OVERALL METHODOLOGY PERFORMANCE

Performance metric	Proposed method	Benchmark
Total features analyzed	50	20-30
Detection accuracy	92.8%	78.5%
False positive rate	3.2%	12.5%
Computational efficiency	High	Moderate

TABLE IV. PERFORMANCE COMPARISON WITH EXISTING METHODS

Performance metric	Proposed method	SNORT	Suricata	Bro/Zeek
Detection accuracy	92.8%	78.5%	82.3%	85.6%
False positive rate	3.2%	12.5%	9.7%	7.4%
Feature detection depth	50 features	25 features	35 features	40 features
Response time	0.35 s	0.75 s	0.62 s	0.48 s
Computational cost	Low	High	Moderate	Moderate

TABLE V. CAPABILITY DIMENSION COMPARISON WITH EXISTING METHODS

Capability dimension	Proposed method	SNORT	Suricata	Bro/Zeek
IoT environment adaptability	95%	75%	82%	88%
Threat classification granularity	4 levels	Binary	3 levels	3 levels
Real-time processing capability	High	Low	Moderate	Moderate
Scalability index	0.92	0.65	0.78	0.85

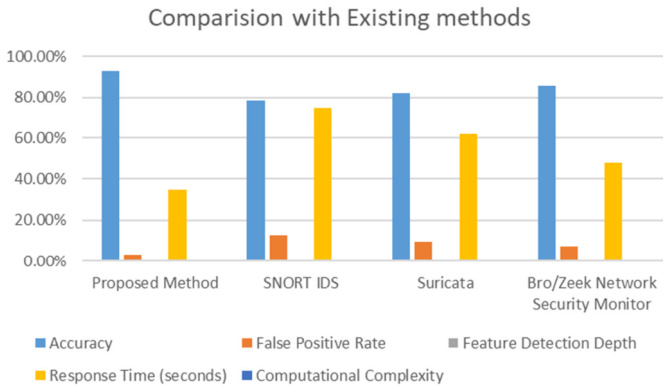

Fig. 2. Comparison with existing methods.

IV. CONCLUSION

This paper presents an adaptive Artificial Intelligence (AI)-driven cyber threat detection framework for heterogeneous Internet of Things (IoT) networks, implementing a four-step methodology: (1) comprehensive data collection and preprocessing from multi-domain IoT environments using the UNSW-NB15 and IoTID20 datasets, creating a balanced dataset of 1,250,000 records with 50 engineered features; (2) intelligent feature extraction across seven security dimensions, including network communication patterns, device behavior signatures, and traffic anomaly indicators; (3) mathematical threat modeling using the formula $\text{Threat Probability} = f(\text{Feature Importance}, \text{Anomaly Score}, \text{Historic Patterns})$; and (4) four-level granular threat classification enabling real-time response within 0.35 s.

The framework achieves significant performance improvements. with 92.8% detection accuracy and a 3.2% false positive rate, substantially outperforming industry standards including SNORT (78.5% accuracy, 12.5% false positive rate), Suricata (82.3% accuracy, 9.7% false positive rate), and Bro/Zeek (85.6% accuracy, 7.4% false positive rate).

The key novelty contributions include: (1) a comprehensive 50-feature extraction framework analyzing IoT security across seven distinct dimensions; (2) a mathematical threat probability model integrating feature importance with anomaly scoring for proactive detection; (3) a four-level threat classification system with 95% IoT environment adaptability; and (4) ultra-fast response capabilities with a scalability index of 0.92, suitable for resource-constrained environments.

Future work may focus on enhancing adaptability to emerging IoT architectures, implementing self-learning capabilities, and developing federated learning approaches for collaborative threat intelligence sharing while preserving privacy.

REFERENCES

[1] S. Ankalaki, A. R. Atmakuri, M. Pallavi, G. S. Hukkeri, T. Jan, and G. R. Naik, "Cyber Attack Prediction: From Traditional Machine Learning to Generative Artificial Intelligence," *IEEE Access*, vol. 13, pp. 44662–44706, 2025, https://doi.org/10.1109/ACCESS.2025.3547433.

[2] N. Moustafa, N. Koroniotis, M. Keshk, A. Y. Zomaya, and Z. Tari, "Explainable Intrusion Detection for Cyber Defences in the Internet of Things: Opportunities and Solutions," *IEEE Communications Surveys & Tutorials*, vol. 25, no. 3, pp. 1775–1807, 2023, https://doi.org/10.1109/COMST.2023.3280465.

[3] G. Falco, A. Viswanathan, C. Caldera, and H. Shrobe, "A Master Attack Methodology for an AI-Based Automated Attack Planner for Smart Cities," *IEEE Access*, vol. 6, pp. 48360–48373, 2018, https://doi.org/10.1109/ACCESS.2018.2867556.

[4] I. Bibi, A. Akhunzada, and N. Kumar, "Deep AI-Powered Cyber Threat Analysis in IIoT," *IEEE Internet of Things Journal*, vol. 10, no. 9, pp. 7749–7760, May 2023, https://doi.org/10.1109/JIOT.2022.3229722.

[5] M. Ragab *et al.*, "Artificial intelligence driven cyberattack detection system using integration of deep belief network with convolution neural network on industrial IoT," *Alexandria Engineering Journal*, vol. 110, pp. 438–450, Jan. 2025, https://doi.org/10.1016/j.aej.2024.10.009.

[6] A. Souri, M. Norouzi, and Y. Alsenani, "A new cloud-based cyber-attack detection architecture for hyper-automation process in industrial internet of things," *Cluster Computing*, vol. 27, no. 3, pp. 3639–3655, June 2024, https://doi.org/10.1007/s10586-023-04163-y.

[7] P. Ajay, B. Nagaraj, R. Arun Kumar, V. Suthana, and M. Ruth Keziah, "DBN-protected material Enhanced intrusion prevention sensor system defends against cyber attacks in the IoT devices," *Measurement: Sensors*, vol. 34, Aug. 2024, Art. no. 101263, https://doi.org/10.1016/j.measen.2024.101263.

[8] A. Zacharis, V. Katos, and C. Patsakis, "Integrating AI-driven threat intelligence and forecasting in the cyber security exercise content generation lifecycle," *International Journal of Information Security*, vol. 23, no. 4, pp. 2691–2710, Aug. 2024, https://doi.org/10.1007/s10207-024-00860-w.

[9] M. A. Alsoufi *et al.*, "Anomaly-Based Intrusion Detection Systems in IoT Using Deep Learning: A Systematic Literature Review," *Applied Sciences*, vol. 11, no. 18, Sept. 2021, Art. no. 8383, https://doi.org/10.3390/app11188383.

[10] S. Ghosh, A. Zaboli, J. Hong, and J. Kwon, "An Integrated Approach of Threat Analysis for Autonomous Vehicles Perception System," *IEEE Access*, vol. 11, pp. 14752–14777, 2023, https://doi.org/10.1109/ACCESS.2023.3243906.

[11] F. Alwahedi, A. Aldhaheri, M. A. Ferrag, A. Battah, and N. Tihanyi, "Machine learning techniques for IoT security: Current research and future vision with generative AI and large language models," *Internet of Things and Cyber-Physical Systems*, vol. 4, pp. 167–185, Jan. 2024, https://doi.org/10.1016/j.iotcps.2023.12.003.

[12] I. H. Sarker, A. I. Khan, Y. B. Abushark, and F. Alsolami, "Internet of Things (IoT) Security Intelligence: A Comprehensive Overview, Machine Learning Solutions and Research Directions," *Mobile Networks and Applications*, vol. 28, no. 1, pp. 296–312, Feb. 2023, https://doi.org/10.1007/s11036-022-01937-3.

[13] K. K. Mamidi *et al.*, "Investigation of cyber attacks using post-installation app detection method," *Cogent Engineering*, vol. 11, no. 1, Dec. 2024, Art. no. 2411859, https://doi.org/10.1080/23311916.2024.2411859.

[14] M. Kireet, P. Rachala, M. S. Rao, and R. Sreerangam, "Investigation Of Contemporary Attacks In Android Apps," *International Journal of Scientific and Technology Research*, vol. 8, no. 12, pp. 1789–1794, 2019.

[15] C. P. Kaliappan, K. Palaniappan, D. Ananthavadivel, and U. Subramanian, "Advancing IoT security: a comprehensive AI-based trust framework for intrusion detection," *Peer-to-Peer Networking and Applications*, vol. 17, no. 5, pp. 2737–2757, Sept. 2024, https://doi.org/10.1007/s12083-024-01684-0.

[16] Y. R. Maramreddy and K. Muppavaram, "Detecting and Mitigating Data Poisoning Attacks in Machine Learning: A Weighted Average Approach," *Engineering, Technology & Applied Science Research*, vol. 14, no. 4, pp. 15505–15509, Aug. 2024, https://doi.org/10.48084/etasr.7591.

[17] V. Koka and K. Muppavaram, "An Enhanced Framework to Mitigate Post-Installation Cyber Attacks on Android Apps," *Engineering, Technology & Applied Science Research*, vol. 14, no. 4, pp. 14788–14792, Aug. 2024, https://doi.org/10.48084/etasr.7467.

[18] J. Wang, Y. Ma, L. Zhang, R. X. Gao, and D. Wu, "Deep learning for smart manufacturing: Methods and applications," *Journal of Manufacturing Systems*, vol. 48, no. C, pp. 144–156, July 2018, https://doi.org/10.1016/j.jmsy.2018.01.003.

[19] 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, https://doi.org/10.1109/COMST.2015.2494502.

[20] J. Li, M. S. Othman, H. Chen, and L. M. Yusuf, "Optimizing IoT intrusion detection system: feature selection versus feature extraction in machine learning," *Journal of Big Data*, vol. 11, no. 1, Feb. 2024, Art. no. 36, https://doi.org/10.1186/s40537-024-00892-y.

[21] "The UNSW-NB15 Dataset." UNSW Research. [Online]. Available: https://research.unsw.edu.au/projects/unsw-nb15-dataset.

[22] "iotid20 dataset." Kaggle. [Online]. Available: https://www.kaggle.com/datasets/rohulaminlabid/iotid20-dataset.