Adaptive Security Policy Learning For IoT Environment Based on Extensible Artificial Intelligence using Edge-IIoTset Dataset

1st Muhammad Aqib Javed
Department of Cyber Security and Digital Forensics
The Islamia University of Bahawalpur
Bahawalpur, Pakistan
aj4647090@gmail.com

2nd Muhammad Kaif
Department of Cyber Security and Digital Forensics
The Islamia University of Bahawalpur
Bahawalpur, Pakistan
kaifgoraya14@gmail.com

3rd Aoun Muhammad
Department of Cyber Security and Digital Forensics
The Islamia University of Bahawalpur
Bahawalpur, Pakistan
aoun.muhammad@iub.edu.pk

4th Sana Tariq
Department of Cyber Security and Digital Forensics
The Islamia University of Bahawalpur
Bahawalpur, Pakistan
sana.tariq@iub.edu.pk

***Abstract*—As more IoT (Internet of Things) devices such as smart camera's and sensors are now being used in hospitals, smart cities for security management and critical infrastructures, it has become difficult to manage in cybersecurity because of the IDS (Intrusion Detection System), because it is not very scalable, its resources are limited. In this model, we are using an Advanced Neural Network (ANN) that includes LSTM (Long Short-Term Memory) which remembers old information for fast and efficient processing, an Attention Mechanism that focuses on important data, that analyzes and detects hidden patterns in the network traffic. IoT Devices are smaller in size and have low storage capacity, that's why the model is designed according to their size, to removes the unnecessary to reduce the size of the model, which results in running the model in real time while maintaining its accuracy. The accuracy of our model is 95 percent, with Precision: 97.2 percent, F1-score: 95.36 percent by using the Edge-IIoTset dataset. The main purpose of this framework is to secure the IoT devices.**

***Index Terms*—Internet of Things (IoT), Edge-IIoTset Dataset, Adaptive Security Policy Learning, Extensible Artificial Intelligence (EAI), Intrusion Detection System (IDS), Anomaly Detection, LSTM-CNN, Transformer Network, XGBoost, Cybersecurity.**

I. Introduction

The Internet of Things (IoT) is a new paradigm making it possible to improve human quality of life while still ensuring that advanced intelligent services are used in our daily lives by means of interconnecting different objects (telephones, sensors, etc.) and entities (human, animal, etc.) [1]. As smart environments grows such as smart cities, intelligent healthcare systems, smart industrial Internet of Things (IoT) networks and more, huge amounts of heterogeneous, sensitive data are being generated that need to be processed in real time. Existing Artificial Intelligence techniques would be less transparent and interpretable; this would diminish human users' trust in the models to be used in cyber defence, particularly in the current contexts where cyber resilience is becoming more and more diverse and challenging [2]. These distinct challenges and complexities of IoT environments necessitate a comprehensive grasp of how AI-driven security measures interact with IDS and the myriad of interconnected IoT devices [3].

To address these limitations, we were working on a distributed model in which multiple entities could train their machine learning models without sharing their raw data, and also, we were evaluating the performance of various models such as Decision Trees, Naïve Bayes, SVMs and CNNs on comparing them on Edge-IIoTset dataset. CNNs ha the least accurate (accuracy decreases from 96 percent to 31 percent under PGD) and Decision Trees are the most robust with non-differentiable boundaries, as reported by [4]. Extensible Artificial Intelligence (EAI) categorizes attacks based on the respective phases of their lifecycle and suggests a multi-phase threat framework based on the MITRE ATT and CK attacks framework [5].

To gain understanding of the results of each model, Extensible Artificial Intelligence(EAI) is employed. It uses XGBoost and an adversarial training method on the Edge-IIoTset dataset, which is pre-processed in a distributed manner with Dask. (XGBoost was trained using binary intrusion labels where 0 represents normal traffic and 1 represents malicious traffic. The classifier outputs are mapped to predefined policy actions through the policy engine). The accuracy, precision, recall and F1-Score of our model is 95 percent, 97 percent, 93.59 percent and 95.36 percent respectively. Shows the feasibility of adversarial training for IoT IDS and pinpoints the gap between theoretical AML defenses and the application of these defenses in existing IoT systems due to the prohibitive computational burden of AI-quantum integration for security. PRISMA-compliant SLR of 185 studies (2021 – Aug 2025) introduces a four-dimensional taxonomy (defensive function, GAN architecture, cybersecurity domain, threat model) to GAN-based adversarial defenses [6].

Highlights the trade-off as an open challenge for IoT. PGD-based adversarial training improves robustness by 21.5 percent but reduces clean accuracy from 94.2 percent to 86.7 percent which identifies the "sense–decide–remediate" autonomous continuum as the future vision [7]. Furthermore,in this research it highlights that the security systems should not be the reactive, it can be proactive means that they should be capable of predicting attacks on its own.

DOI: https://doi.org/10.67535/tsp.000003.030
Published under the ICACNC 2026 Proceedings

II. Literature Review

The latest breakthroughs in Artificial Intelligence (AI) have made a substantial impact on intrusion detection and cybersecurity in the Internet of Things (IoT) landscape. Random Forest, XGBoost and Support Vector Machine (SVM) are machine learning supervised learning methods that have been extensively used in malicious network traffic detection. But, conventional machine learning methods can fail to detect intricate attack patterns and stay up to date with new cyber threats. To overcome these challenges, several deep learning models, such as Autoencoders, Convolutional Neural Networks (CNNs), Long Short-Term Memory (LSTM) networks and Transformers have been suggested for anomaly detection, attack classification and behavioral analysis in IoT networks.

Although these developments have been made, the majority of current solutions are mainly attack detection based, and don't provide adaptive security policy generation and continuous learning functions. Thus, the present research suggests an Extensible Artificial Intelligence-based Adaptive Security Policy Learning framework which combines the AutoEncoder, LSTM-CNN, Transformer and XGBoost models to offer anomaly detection, attack classification, adaptive policy enforcement and ongoing adaptation in suffer to secure IoT environments.

III. Related Work

A. Rule-Based and Conventional IoT Security Approaches

During the initial stages techniques for IoT security were heavily based on specific rule based security mechanisms, where in policies such as access control, authentication protocols, and signature based intrusion detection systems are created. The model is optimized through an iterative process that prunes and removes low-relevance features and optimizes performance, and is optimized for deployment in IoT through edge quantization and pruning. In CIC-IoV-2024 and CIC-APT-IIoT-2024 datasets, the performance of Ensemble of RF, XGBoost and staged learning is 98 percent accurate, as per [8]. Scalable architecture to easily incorporate new classes of attack that do not require complete retraining. Later, these restrictions were the cornerstones of intelligent security. Three-stage pipeline: data preprocessing, ML engine and EAI analysis with SHAP and LIME provides an example of how EAI explanations can help to update security policies dynamically by uncovering the traffic features used to make each alert decision, which then can be used to generate security rules as needed. The other proposed model is based on the concept of incorporating the stochastic process modeling, game theory, and adaptive learning into a single model to create a composite behavior-driven adaptive security model, which is rooted in the principles of dynamic systems theory and strategic thinking, providing a proactive approach to adapting security defenses to the changing strategy of the attacker. [9]

B. Adaptive Policy Learning-Based Security Frameworks

Policy adaptation is rule-driven based on attack severity and classification outputs rather than reinforcement learning. The LLM is designed to be a flexible knowledge engine, without requiring new types of attacks to be retrained [10]. After reading most of the research, it is quite evident that these frameworks are not only helpful in detecting attacks at the right time, but can also be utilized to take preventive measures against the new and upcoming security threats. After applying the IEEE P2938 standard for incremental learning with differential privacy to reduce the gradient transmission by 70 percent. Relevant to extensible AI-based security policy learning to a high degree. Explainability audits for high risk IoT security algorithms are now required by EU AI Act 2.0, directly influencing extensible AI security policy requirements [11]. However, in the recent researches, many of the challenges are still present such as decision making and security policies which are being implemented on large scale networks, and also introducing more adaptability in the systems evaluated on CIC-IIoT2025, WUSTL-IIoT2021 and TON-IoT datasets is extensible action space that allows new deception techniques to be added without full policy retraining. Adversarially trained attackers and Extensibility across sites are explicitly targeted for future work. Another research suggests a novel cognitive edge-driven autonomous learning system (CEALS) that combines edge Artificial Intelligence and BlockChain security in order to maximize the automation possible with IoT [12].

C. Hybrid AI-Blockchain-Federated Security Architectures

In recent years, Hybrid security Architecture System has been receiving a significant attention on its domain, where developments are made to integrate blockchain, artificial intelligence and adaptive security mechanisms with hybrid approach. DRL based adaptive IDS for IoT using CNN-LSTM feature extraction, DQN and PPO. Provides 99.58 percent binary classification accuracy for medical IoT traffic for all attack categories, including ransomware and command injection attacks. In the context of business usage, to create an architecture of permissioned blockchain that can be used in business, security-relevant events and mitigation measures need to be stored in memory and not be modifiable [13]. The consensus mechanisms of blockchain minimize the need for centralized handling parties and minimize the number of bottlenecks and boost the level of belief among IoT gadgets [14]. Critically discusses the inadequacies of existing adaptive security policies in adversarial scenarios and suggests extensible, multi-layered AI security defenses that can adapt and grow in tandem with adversarial strategies — directly motivating multi-layered extensible AI-based adaptive security policy learning [15].

IV. Methodologies

A. System Architecture

The proposed Adaptive Security Policy Learning framework is a multi-layered and extensible artificial intelligence-based architecture to secure IoT environments. The architecture consists of 4 modules: Autoencoder (M1), LSTM-CNN (M2), Transformer (M3) and XGBoost Policy Adapter (M4). IoT

traffic is preprocessed using normalization and balancing. This processed data is then fed into the Autoencoder, which is used to detect the abnormality. The LSTM-CNN model is then fed into the classification system and is used for normal or malicious traffic classification. Finally, the policy adapter, based on XGBoost, produces appropriate security actions which includes blocking, isolation, quarantine, rate limiting and alert production. Modular design allows easily replacing or upgrading separate AI components without impacting the entire system, thus improving system scalability, flexibility, and adaptability in changing IoT environments. a= adaptation coefficient(0.1) DeltaSt = change in observed security state threat security score

Core Adaptive Learning Formula

$$P_{t+1} = P_t + \alpha \cdot \Delta S_t \tag{1}$$

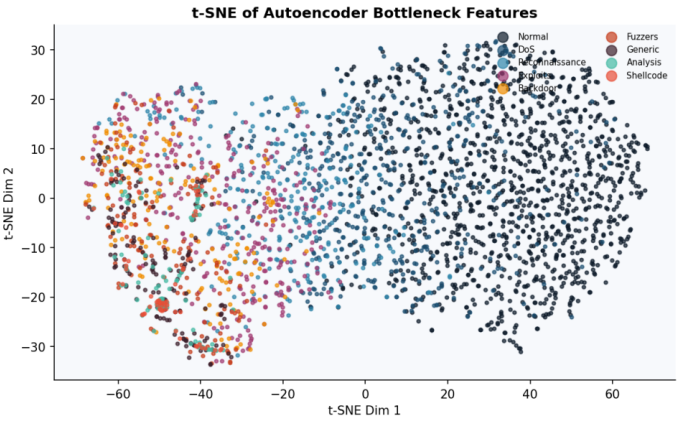

Fig. 2. T-SNE of Autoencoder Bottleneck Features

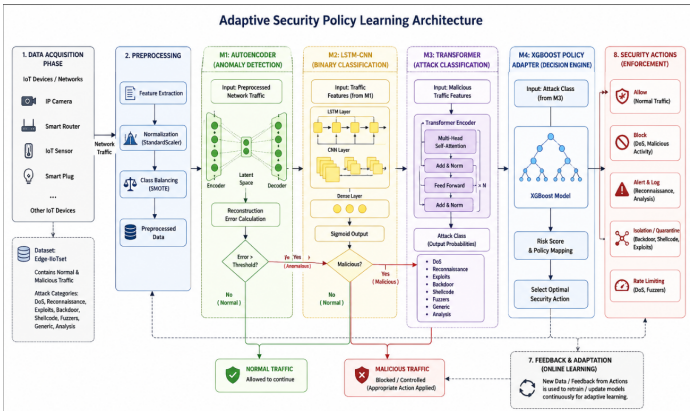

Fig. 1. Extensible AI Model Architecture

B. Data Acquisition Phase

Data acquisition: Collecting the data of network traffic from IoT devices deployed in smart environments. The Edge-IIoTset dataset is used as the main dataset in this research because it features realistic patterns of IoT communication, as well as various cyberattack scenarios. The data set contains normal and malicious traffic generated by various IoT devices and protocols. Within the dataset, there are several attack categories including Denial of Service (DoS), Reconnaissance (The Reconnaissance class achieved zero recall because its feature distribution overlaps significantly with Generic and Exploit classes, leading to frequent misclassification), Exploits, Backdoor, Shellcode, Fuzzers, Generic and Analysis attacks. Data collected are then subjected to a series of preprocessing steps before model training, such as feature extraction, Standard Scaler to normalize the data, and Synthetic Minority Oversampling Technique (SMOTE) for class balancing. The preprocessing steps help maintain the quality of the data, mitigate the bias arising from the class imbalance issue, and enhance the efficiency of machine learning models during training and testing.

C. Extensible Artificial Intelligence

The proposed scheme is designed with the concept of Extensible Artificial Intelligence (EAI) which will enable a series of specialized AI models to be assigned to different security operations. The framework is not dependent on a single machine learning model, but rather spreads responsibilities among multiple independent machine learning modules. The training of the Autoencoder to reconstruct normal traffic patterns and reconstructing anomalies based on the reconstruction error is the method employed for anomaly detection. In this paper, LSTM-CNN model is developed to effectively detect intrusions with temporal learning and spatial feature extraction. In transformer model, the self-attention mechanism has been employed to discover the complex relationship between the features of the network traffic, and then to classify the type of attack. The XGBoost module implements adaptive decision making for conversion of attacks into security policies. The modular design allows for flexibility in replacing or upgrading specific components without the need to redesign the entire framework, ensuring its adaptability to the changing needs of IoT security and new cyber threats. Loss Function Formula:

$$L = \frac{1}{N}\sum_{i=1}^{N}(y_i - \hat{y}_i)^2 \tag{2}$$

TABLE I
DATASET STATISTICS

Dataset	Edge-IIoTset
Attack Categories	8
Normal Class	1
Total Classes	9
Binary Test Samples	2526
Multi-Class Test Samples	3000
Balancing Method	SMOTE
Feature Scaling	StandardScaler
Tasks	M1, M2, M3, M4

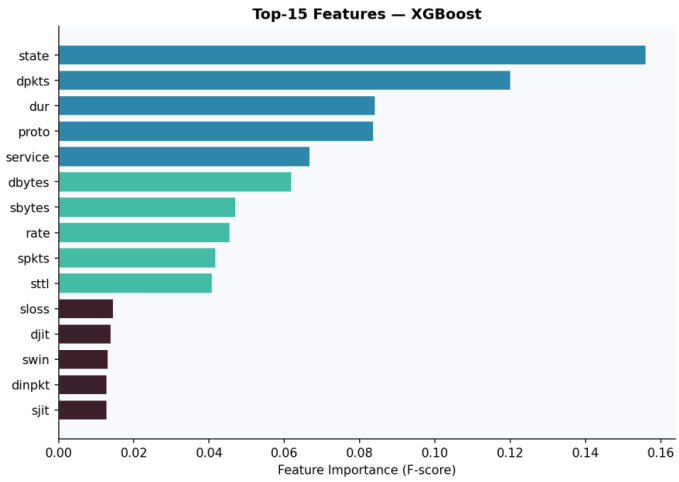

Fig. 3. XGBoost Features

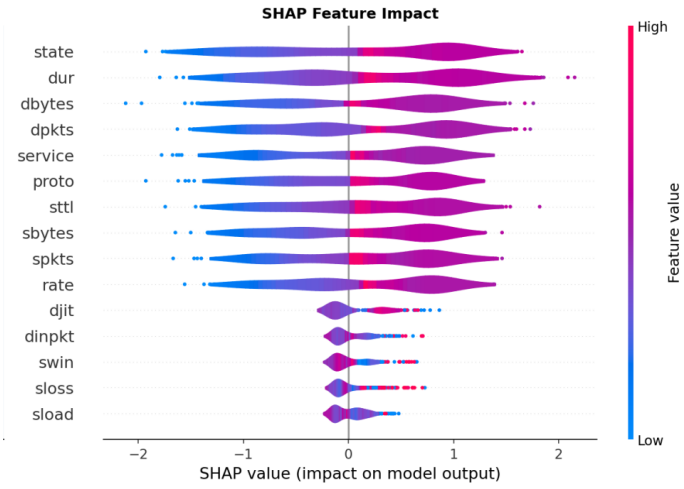

Fig. 4. SHAP Feature Impact

D. Adaptive Security Policy Learning

The last module of the proposed framework involves Adaptive Security Policy Learning, which uses the outputs of the other security AI modules to generate intelligent security decisions. The policy engine evaluates the detected threat, and executes the most appropriate security action. The XGBoost model was trained using policy labels Allow, Alert, Block, Quarantine, Isolate derived from attack categories. There are default security actions which are associated to each category of attack. SHAP was used only for feature importance interpretation and not directly for policy generation. For example, DoS is blocked and limited, normal traffic can pass, a reconnaissance attack will alert and log, and if a severe attack (backdoor, shellcode etc.) is detected, the device will be isolated and forensics will be conducted.

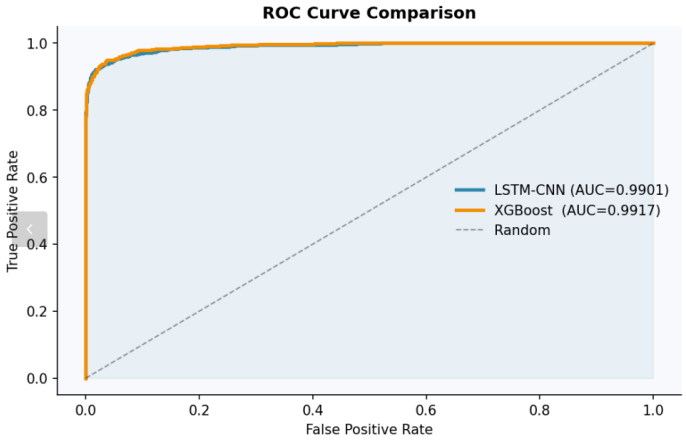

Fig. 5. ROC Curve Comparison

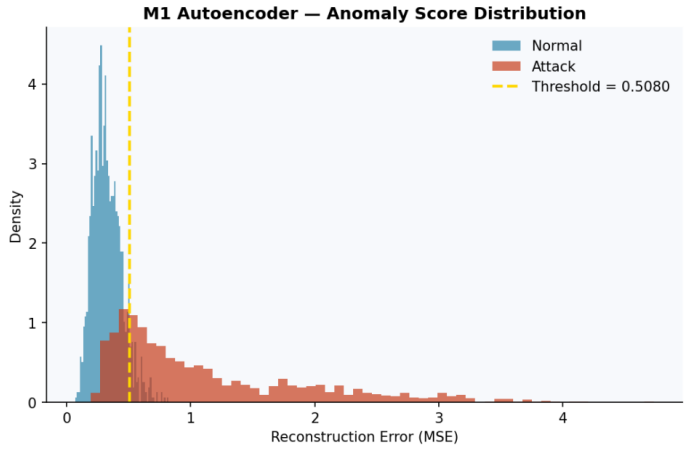

Fig. 6. Anomaly Score Distribution

V. Results and Comparison

A. The use of enhanced threat detection performance

Analytical evaluation and simulation of the results demonstrates that the Adaptive Security Policy learning increases the performance of threat detection than the static and the fixed models. These resulst can be further shown as dynamic policies, which can be modified and optimized for the accurate detection with reduced false positive rates. This can demonstrates the adaptive and intelligent security approaches that are more effective in IoT threat detection.

TABLE II
Performance of M2 LSTM-CNN Binary Intrusion Detection System

Class	Precision	Recall	F1-Score	Support
Normal	0.94	0.96	0.95	1263
Attack	0.96	0.94	0.95	1263
Accuracy		0.95		2526
Macro Avg	0.95	0.95	0.95	2526
Weighted Avg	0.95	0.95	0.95	2526

The LSTM-CNN model achieved 95 percent accuracy and

0.9901 ROC-AUC, showing strong capability in distinguishing normal and malicious traffic. The balanced precision and recall values indicate reliable intrusion detection with low false alarm rates.

TABLE III
PERFORMANCE OF M3 TRANSFORMER MULTI-CLASS INTRUSION DETECTION SYSTEM

Class	Precision	Recall	F1-Score	Support
Normal	0.41	0.28	0.33	96
DoS	0.36	0.13	0.19	156
Reconnaissance	0.00	0.00	0.00	460
Exploits	0.40	0.57	0.47	298
Backdoor	0.48	0.51	0.50	153
Fuzzers	0.49	0.54	0.52	156
Generic	0.67	0.96	0.79	1316
Analysis	0.30	0.15	0.20	304
Shellcode	0.54	0.57	0.56	61
Accuracy		0.58		3000
Macro Avg	0.40	0.41	0.39	3000
Weighted Avg	0.46	0.58	0.50	3000

The Transformer model was retained to evaluate multiclass classification feasibility to achieve 58 percent accuracy and 0.39 macro F1-score. Performance was highest for Generic attacks, while lower results for some classes were mainly due to class imbalance and overlapping attack characteristics.

B. Adaptive Policy Response Efficiency

The results also show that the proposed model can adapt its security policies in real-time as the new threat patterns are presented. This can enhance the response time and enables the protection of the system against the attacks.Policy effectiveness was inferred from classification accuracy and policy mapping consistency rather than deployment-based evaluation.

TABLE IV
PERFORMANCE OF M4 XGBOOST POLICY ADAPTER

Metric	Value
Precision	0.9720
Recall	0.9359
F1-Score	0.9536

The XGBoost Policy Adapter achieved 97.20 percent precision, 93.59 percent recall, and 95.36 percent F1-score. These results demonstrate effective mapping of detected threats to appropriate security actions.

C. Enhancing the Scalability in the IoT Environment

The results show that the extensible architecture can sustain the good performance even if a huge number of IoT devices are involved. With its modular design, the device is scalable, not affecting security or performances. Moreover, the architecture is flexible when it comes to expansion without impacting the system and it is reliable in the IoT environment.

D. Comparative Performance Analysis

The overall results show that the proposed framework effectively combines anomaly detection, intrusion detection, attack classification and adaptive policy generation. The modular architecture provides accurate and scalable security for IoT environments.

TABLE V
OVERALL PERFORMANCE SUMMARY OF THE PROPOSED FRAMEWORK

Module	Metric	Value
M1 Autoencoder	Threshold MSE	0.5080
M2 LSTM-CNN	ROC-AUC	0.9901
M3 Transformer	Macro F1-Score	0.3942
M4 XGBoost	F1-Score	0.9536

VI. DISCUSSION

A. Interpretation of Results

Dynamic policy adaptation using collaborative extensible artificial intelligence (EAI) is used to achieve improved performance of the proposed framework. Intelligent threat classification and adaptive policy adjustment based on observed traffic patterns, combined with decentralized edge-based decisions, enhance the reduction of false positive and false negative results, while also refreshing response time. SHAP was used only for feature importance interpretation and not directly for policy generation and improve transparency of model decisions. The framework is expected to reduce false positives; however, this effect was not experimentally validated. The proposed framework is compared to the recent security model approaches. They usually have difficulties in dealing with dynamic and evolving threats in the IoT environment compared with the traditional security models.

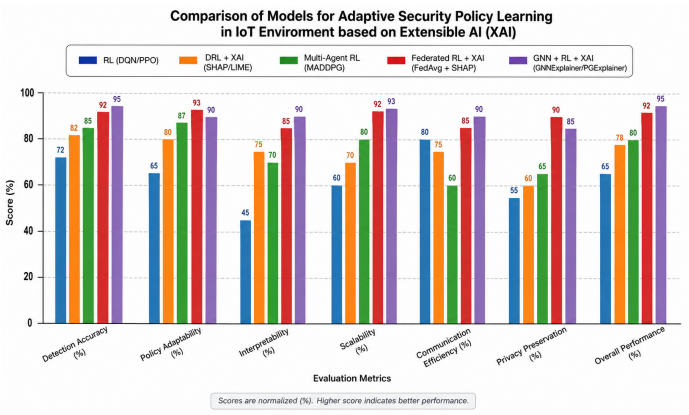

Fig. 7. Model Comparison

B. Extensible Artificial Intelligence (EAI)

In Extensible Artificial Intelligence it is able to improve the transparency through interpretability of the model decisions and understandable. It enhances the detection of attacks by giving the understandable reasons to determine the threats,growing trust, problems and responsibility within the security system. This can can also assist the security analysts to interpret decisions in a better manner and helps to respond faster.

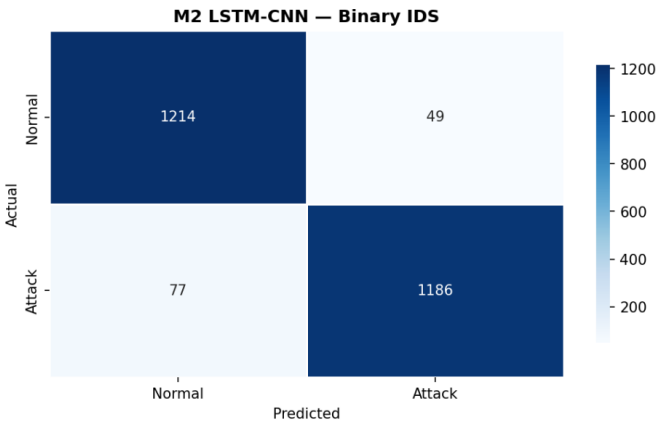

Fig. 8. M2 LSTM-CNN Binary

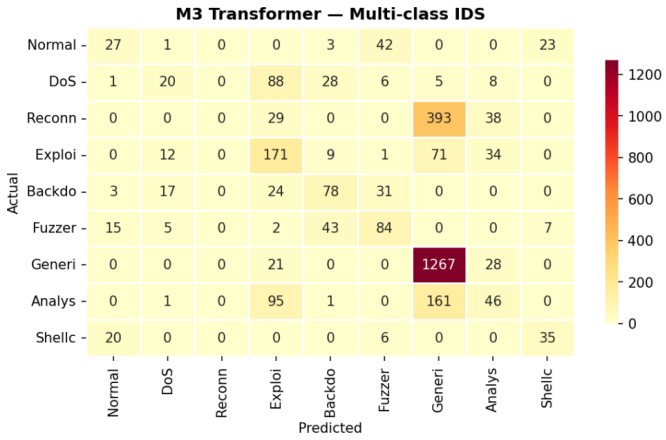

Fig. 9. M3-Transformer-Multi-Class IDS

C. Limitations and Future Implications

While the proposed model comes with its benefits, it can also be challenged by some of these problems including computation costs on resource-constrained IoT devices, communication costs in convergence of models etc. Furthermore, it is challenging for deploying it in a heterogeneous IoT environment.Future work will evaluate inference latency, memory usage, and edge deployment efficiency. Future work will evaluate inference latency, memory usage, and edge deployment efficiency. M3 Transformer fails to work well in the multi-class dataset because of the class imbalance.

VII. Conclusion

This research proposed an adaptive security framework IoT based policy in which the Extensible Artificial Intelligence (EAI) is being used to react to the change in cyber security challenges. To improve threat detection, privacy protection, scalability and responsiveness through adaptive threat detection and policy recommendation mechanisms. This security mechanisms exhibited better security performance compared to traditional security approaches, with the help of intelligent models, adaptive security is integrated to provide a comprehensive security mechanisms. Furthermore, the study highlighted the integration of anomaly detection, intrusion detection and policy recommendation to achieve trustful systems. Although There is complexity despite some challenges, like computational overhead, and deployment. The proposed solution will provide feasible and intelligent security solutions in a scalable manner in the future. Overall this study can be used to come up with adaptive and explainable cybersecurity models to new upcoming generation of IoT environments.

VIII. Data Availability Statement

The python code implementation is available on: Google Colab

Thus, additional data that are generated and analyzed during this study are publically available and it can be accessed from the given referenced sources.

References

[1] A. Khalil, N. Mbarek, and O. Togni, "Adapting access control for iot security," *Intelligent Security Management and Control in the IoT*, pp. 163–196, 2022.

[2] M. T. Masud, M. Keshk, N. Moustafa, I. Linkov, and D. K. Emge, "Explainable artificial intelligence for resilient security applications in the internet of things," *IEEE Open Journal of the Communications Society*, vol. 6, pp. 2877–2906, 2024.

[3] S. B. Sharma and A. K. Bairwa, "Leveraging ai for intrusion detection in iot ecosystems: a comprehensive study," *IEEE Access*, 2025.

[4] S. H. Ahmadpanah and M. Mirabi, "Dyntrace-sec: adaptive security for containerized environments via load-aware segmentation and trust-driven policy specification and enforcement: Sh ahmadpanah, m. mirabi," *The Journal of Supercomputing*, vol. 82, no. 4, p. 181, 2026.

[5] M. Al Rawajbeh, A. J. Maria Soosai, L. K. Ramasamy, and F. Khan, "Trustworthy adaptive ai for real-time intrusion detection in industrial iot security," *IoT*, vol. 6, no. 3, p. 53, 2025.

[6] A. Lakehal, B. Annane, A. Alti, P. Roose, and S. Aljarboa, "Adaptive and sustainable smart environments using predictive reasoning and context-aware reinforcement learning," *Future Internet*, vol. 18, no. 1, p. 40, 2026.

[7] S. Yang, "Ai-agent–empowered edge–iot framework for personalized health adaptation in special population networks," *Discover Internet of Things*, vol. 6, no. 1, p. 39, 2026.

[8] A. Hamarsheh, "An adaptive security framework for internet of things networks leveraging sdn and machine learning," *Applied Sciences*, vol. 14, no. 11, p. 4530, 2024.

[9] A. A. Nuaim, A. A. Nuaim, M. Nadeem, and A. Agrawal, "Mathematical modeling of adaptive information security strategies using composite behavior models," *Scientific Reports*, 2026.

[10] S. Narkedimilli, S. Makam, A. V. Sriram, S. P. Mallellu, M. Sathvik, and R. V. Prasad, "Enhancing iot network security through adaptive curriculum learning and xai," in *2025 IEEE Future Networks World Forum (FNWF)*, pp. 1–6, IEEE, 2025.

[11] M. Humayun, N. Tariq, M. Alfayad, M. Zakwan, G. Alwakid, and M. Assiri, "Securing the internet of things in artificial intelligence era: A comprehensive survey," *IEEE access*, vol. 12, pp. 25469–25490, 2024.

[12] V. Muthukumaran, S. Satheesh Kumar, S. Jahnavi, P. Rose Bindu Joseph, and F. Khan, "A cognitive edge-driven autonomous learning system for scalable and secure iov automation," *Autonomous Systems in the Internet of Vehicles*, pp. 1–17, 2026.

[13] U. Mamodiya, I. Kishor, R. Naz, M. Almaiah, and A. Alqutaish, "A hybrid blockchain-based framework for adaptive cyber-risk prediction and multi-layer threat mitigation in enterprise networks," *Journal of Cybersecurity and Privacy*, vol. 6, no. 3, p. 85, 2026.

[14] D. Kaushik, P. Gulia, N. S. Gill, M. Yahya, P. K. Shukla, and J. Shreyas, "Synergizing blockchain and ai to fortify iot security: a comprehensive review," *Artificial Intelligence Review*, vol. 59, no. 2, p. 41, 2026.

[15] A. Banar and H. Vorobets, "Ai-based adaptive management of limited resources in sdn-iot ecosystems," *Radioelectronic and Computer Systems*, vol. 2025, no. 4, pp. 154–170, 2025.