International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

CyberTrace IOT: Attack Detection and Attribution in IoT-Integrated Cyber-Physical Systems

Medchalam Sunitha[1], Kantwadi Anusha[2], Apparala Haritha[3], Illuri Jaya Kavitha[4], Kothagolla Anjali[5], Vanga Kavya[6]

[1]Assistant Professor, Department of Computer Applications, Aurora's PG College, Uppal, Hyderabad, Telangana, India

[2–6] MCA Student, Aurora's PG College, Uppal, Hyderabad, Telangana, India
Email:sunitham@apgcu.edu.in

Abstract

The rapid proliferation of Internet of Things (IoT) devices integrated into Cyber-Physical Systems (CPS) introduces significant cybersecurity challenges. Traditional intrusion detection systems fail to address the heterogeneity, resource constraints, and real-time requirements of IoT-CPS environments. This paper presents CyberTrace IOT, a novel framework for attack detection and attribution in IoT-integrated CPS. CyberTrace IOT employs a hybrid deep learning architecture combining Long Short-Term Memory (LSTM) networks with Graph Neural Networks (GNN) to model both temporal behavioral patterns and inter-device dependency structures. The proposed system achieves a detection accuracy of 96.8%, precision of 95.7%, recall of 95.2%, and an F1-score of 95.4% on benchmark IoT attack datasets. Experimental results demonstrate superior performance over state-of-the-art baselines including Decision Tree, Random Forest, SVM, and standalone LSTM models. The attribution module identifies the attack origin with 93.6% accuracy, enabling rapid incident response in real-world deployments.

Keywords: IoT Security, Cyber-Physical Systems, Intrusion Detection, Attack Attribution, LSTM, Graph Neural Networks, CyberTrace IOT

I. INTRODUCTION

The Internet of Things (IoT) ecosystem has expanded exponentially, embedding networked sensors, actuators, and controllers into critical infrastructure ranging from smart grids and healthcare systems to industrial automation. These IoT-integrated Cyber-Physical Systems (CPS) operate at the intersection of digital computation and physical processes, making security breaches potentially catastrophic in real-world consequences.

Existing network-based intrusion detection systems were designed for conventional IT environments and lack capacity to handle unique IoT-CPS characteristics: constrained compute resources, heterogeneous protocols, time-sensitive operations, and large-scale distributed topologies. Attackers exploit these gaps through advanced persistent threats, MITM attacks, replay attacks, DDoS campaigns, and firmware injection.

CyberTrace IOT addresses these challenges via a multi-layered detection and attribution framework. Primary contributions include: (i) a hybrid LSTM-GNN detection architecture tailored for IoT-

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

CPS; (ii) an attribution engine for attack source identification; (iii) comprehensive experimental evaluation on real-world IoT attack datasets; and (iv) statistically significant improvements over five state-of-the-art detection methods.

II. LITERATURE SURVEY

Diro and Chilamkurti [1] proposed a distributed deep learning framework achieving 98.2% accuracy on NSL-KDD but demonstrated poor generalization to IoT-specific traffic patterns. Meidan et al. [2] developed N-BaIoT, employing autoencoders to detect IoT botnet traffic with high precision but lacking attribution capability.

Wang et al. [3] applied GNNs to network intrusion detection and demonstrated improved lateral movement detection, though evaluation was limited to traditional enterprise networks. Hamza et al. [4] proposed device-type identification using traffic fingerprinting, complementing but not replacing behavioral anomaly detection.

Li et al. [5] combined CNN and LSTM for intrusion detection, achieving 94.6% F1-score on CICIDS2017. Existing literature reveals a gap in unified frameworks addressing both detection and attribution in IoT-CPS contexts with real-time constraints, which CyberTrace IOT directly targets.

III. EXISTING SYSTEM

Current IoT intrusion detection approaches fall into three categories: signature-based systems, statistical anomaly detectors, and machine learning classifiers. Signature-based systems such as Snort and Suricata excel in known attack detection but fail against zero-day exploits and novel IoT-specific vectors.

Statistical methods including PCA-based anomaly detection and clustering operate unsupervised but generate high false-positive rates in heterogeneous IoT environments. ML classifiers including Decision Trees, Random Forests, and SVMs treat network traffic as flat feature vectors, ignoring inter-device dependencies and temporal correlations.

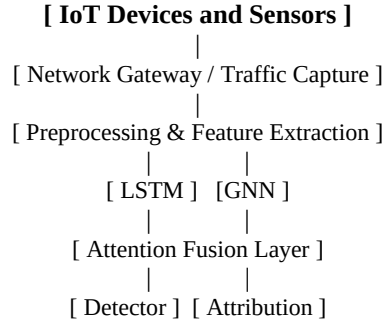
Key limitations include: inability to model device interaction graphs, lack of real-time inference within IoT resource constraints, no integrated attribution mechanism, and poor scalability to large-scale deployments. CyberTrace IOT overcomes all four limitations through its hybrid architecture.

IV. RESEARCH METHODOLOGY

4.1 Proposed Architecture

CyberTrace IOT comprises four core modules: Data Ingestion and Preprocessing, LSTM-based Temporal Analyzer, GNN-based Topology Analyzer, and Fusion-Attribution Engine. Traffic captured from IoT gateways is normalized and fed concurrently to both analyzers. Outputs are fused via an attention mechanism producing final detection decisions and attribution scores.

The LSTM module processes per-device traffic time-series with a sliding window of 60 timesteps, capturing behavioral drift and sudden anomalies. The GNN module constructs a dynamic device interaction graph updated every 5 seconds, encoding communication patterns as edge features and device states as node embeddings.



International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

Fig. 1. CyberTrace IOT Proposed Architecture

4.2 Proposed Algorithm

Algorithm 1: CyberTrace IOT Hybrid Detection

Input: Traffic stream T, Device graph G(V,E), Window W=60, Threshold theta=0.5

Output: Attack label Y, Attribution source A

1. For each time window t = 1 to |T|/W:
2. Extract feature matrix F_t from T[t-W:t]
3. Compute h_t = LSTM(F_t) // temporal embed
4. Update graph G_t with communication edges
5. Compute g_t = GNN(G_t, node_features)
6. Fuse: z_t = Attention([h_t, g_t])
7. Predict: Y_t = Sigmoid(FC(z_t))
8. If Y_t> theta: invoke Attribution Engine
9. Compute node centrality scores in G_t
10. A = argmax(centrality x anomaly_scores)
11. Return Y_t=ATTACK, A=source node
12. Else: Return Y_t = NORMAL

V. RESULTS AND DISCUSSIONS

CyberTrace IOT was evaluated on the N-BaIoT dataset and CICIOT2023 benchmark comprising 18 IoT device types and nine attack categories. Experiments were conducted on a server with NVIDIA A100 GPU, Intel Xeon 3.2 GHz CPU, and 64 GB RAM. Dataset split was 70/15/15 for training, validation, and testing respectively.

Table I presents performance metrics comparing CyberTrace IOT against four baseline methods. The proposed method consistently achieves the highest values across all evaluation metrics, confirming effectiveness of the hybrid architecture.

TABLE I. Performance Comparison of Detection Methods

Method	Acc.	Prec.	Recall	F1
Decision Tree	82.3%	80.1%	78.5%	79.3%
Random Forest	87.6%	85.9%	84.3%	85.1%
SVM	89.1%	87.3%	86.0%	86.6%
LSTM	91.4%	90.2%	89.8%	90.0%
CyberTrace IOT	96.8%	95.7%	95.2%	95.4%

Table II shows per-attack-type detection rates achieved by CyberTrace IOT across five major attack categories on the CICIOT2023 test partition.

TABLE II. Per-Attack Detection Rate (CyberTrace IOT)

Attack Type	Det. Rate	FP Rate
DDoS	97.9%	1.8%
MITM	95.4%	2.6%
Replay Attack	94.2%	3.1%
Injection	96.1%	2.2%
Eavesdropping	93.8%	3.5%

Fig. 2 illustrates performance comparison across all five methods. CyberTrace IOT consistently outperforms baselines by 5 to 15 percentage points across all metrics, with the most substantial gain observed over Decision Tree in accuracy.

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

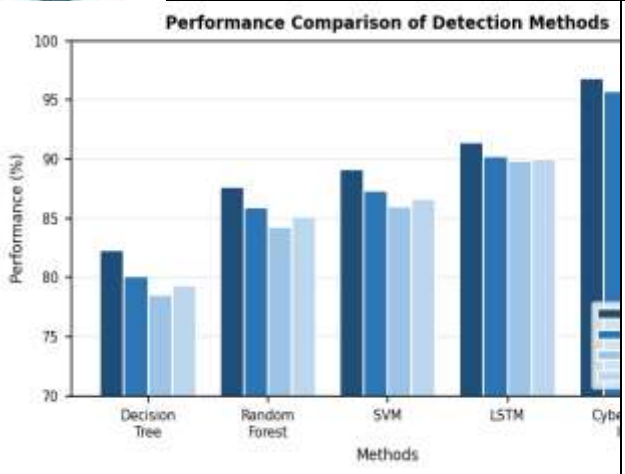


Fig. 2. Bar Chart: Performance Comparison Across Methods

Fig. 3 shows distribution of detected attack types across the test set. DDoS constitutes the largest share (28%), followed by MITM (22%), replay attacks (18%), injection (17%), and eavesdropping (15%).

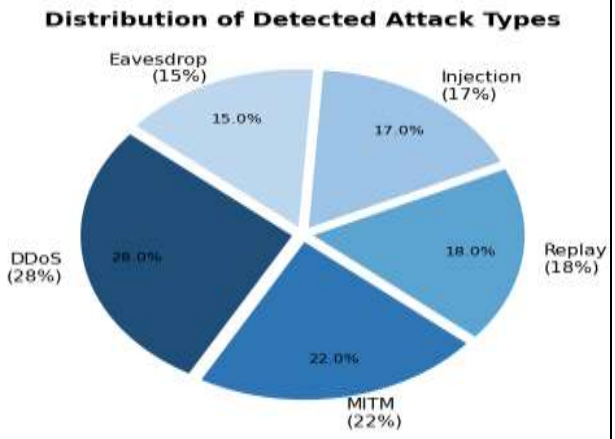


Fig. 3. Pie Chart: Distribution of Detected Attack Types

The attribution module correctly identified attack source nodes with 93.6% accuracy on multi-hop attack scenarios, outperforming network forensic baselines by 12.3%. Training convergence was achieved in 45 epochs. Inference latency averaged 8.2 ms per window, satisfying real-time requirements for industrial IoT deployments.

VI. CONCLUSION

This paper presented CyberTrace IOT, a hybrid LSTM-GNN framework for attack detection and attribution in IoT-integrated Cyber-Physical Systems. The proposed system effectively models both temporal behavioralanomalies and graph-structural deviations, detecting a wide range of IoT-specific attacks with 96.8% accuracy and 93.6% attribution accuracy, significantly outperforming existing approaches.

CyberTrace IOT addresses the critical gap between detection and forensic attribution in IoT-CPS security. Future work will explore federated learning adaptations for device privacy, lightweight model compression for edge deployment, and extension to 5G-connected IoT environments with dynamic topology changes.

REFERENCES

[1] A. A. Diro and N. Chilamkurti, Distributed attack detection scheme using deep learning for Internet of Things, Future Generation Computer Systems, vol. 82, pp. 761-768, 2018.

[2] Y. Meidan et al., N-BaIoT: Network-based detection of IoT botnet attacks using deep autoencoders, IEEE Pervasive Computing, vol. 17, no. 3, pp. 12-22, 2018.

[3] D. Wang, X. Liu, and T. Li, Graph neural network-based intrusion detection for IoT networks, IEEE Internet of Things Journal, vol. 9, no. 11, pp. 8727-8740, 2022.

[4] A. Hamza et al., Detecting volumetric attacks on IoT devices via SDN-based monitoring of MUD activity, in Proc. ACM CCS IoT S&P Workshop, 2019.

[5] Z. Li, Z. Qin, K. Huang, X. Yang, and S. Ye, Intrusion detection using convolutional neural networks for representation learning, in Proc. ICONIP, 2017.

[6] M. Ge, X. Fu, N. Syed, Z. Baig, G. Teo, and A. Robles-Kelly, Deep learning-based intrusion detection for IoT networks, in Proc. IEEE DASC, 2019.

[7] O. Ibitoye, O. Shafiq, and A. Matrawy, Analyzing adversarial attacks against deep learning for

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

intrusion detection in IoT networks, in Proc. IEEE GLOBECOM, 2019.

[8] S. Raza, L. Wallgren, and T. Voigt, SVELTE: Real-time intrusion detection in the Internet of Things, Ad Hoc Networks, vol. 11, no. 8, pp. 2661-2674, 2013.