Journal of Information & Optimization Sciences
ISSN 0252-2667 (Print), ISSN 2169-0103 (Online)
Vol. 47 (2026), No. 8, pp. 2931–2938
DOI : 10.47974/JIOS-2235

Hybrid-IDPS for IoT networks : A feature-augmented approach to anomaly detection

Sushama [§]
Department of Computer Science & Engineering
Manipal University Jaipur
Jaipur 303007
Rajasthan
India

Shuchita Vaidya [†]
School for Online and Digital Learning
Symbiosis International (Deemed University)
Pune 412115
Maharashtra
India

Surbhi Sharma *
Prashant Vats [‡]
Department of Computer Science & Engineering
Manipal University Jaipur
Jaipur 303007
Rajasthan
India

Anudeep Arora [@]
Department of Management
Symbiosis Institute of International Business
Symbiosis International (Deemed University)
Pune 412115
Maharashtra
India

[§] *E-mail:* sushama.tanwar@jaipur.manipal.edu
[†] *E-mail:* shuchitavaidya@gmail.com
* *E-mail:* surbhi.sharma@jaipur.manipal.edu (Corresponding Author)
[‡] *E-mail:* prashant.vats@jaipur.manipal.edu
[@] *E-mail:* anudeep.arora@siib.ac.in

© Taru Publications

Abstract

The rapid growth of IoT networks has expanded the attack surface, making conventional intrusion detection systems inadequate due to resource constraints and evolving threats. This paper proposes a Hybrid Intrusion Detection and Prevention System (Hybrid-IDPS) that integrates feature-augmented machine learning with lightweight cryptographic assurance for secure and adaptive anomaly detection. The framework employs a two-stage architecture combining discrete mathematical feature engineering with a hybrid shallow–deep learning engine. Elliptic-curve–based authentication and hash-chained alert logging ensure integrity, non-repudiation, and secure coordination. Experimental results on benchmark IoT datasets show improved detection accuracy, reduced false positives, and lower computational overhead. The proposed system offers a scalable and resource-efficient solution for next-generation IoT security.

Subject Classification: *Primary 68M10, Secondary 68M12.*

Keywords: *Hybrid-IDPS, IoT security, Anomaly detection, Feature engineering, Discrete mathematics, Cryptography, Elliptic curves, Machine learning, Intrusion detection, Prevention systems.*

1. Introduction

The Internet of Things (IoT) has emerged as a transformative paradigm, enabling seamless interconnection among billions of heterogeneous devices across domains such as smart cities, healthcare, industrial automation, transportation, and intelligent energy systems. By integrating sensing, communication, and computation capabilities into everyday objects, IoT infrastructures generate massive volumes of data and support real-time, mission-critical services. However, this rapid expansion has also introduced profound security challenges. IoT networks are inherently resource-constrained, highly distributed, and dynamically evolving, making them particularly vulnerable to a wide spectrum of cyber threats, including distributed denial-of-service (DDoS) attacks, botnet infiltration, data exfiltration, spoofing, and zero-day exploits. Traditional intrusion detection systems (IDS), which are largely designed for conventional enterprise networks, struggle to operate effectively in IoT environments due to their reliance on static signatures, high computational overhead, and limited adaptability to evolving attack patterns. Signature-based IDS techniques are incapable of detecting unknown or polymorphic attacks, while purely anomaly-based approaches often suffer from high false-positive rates caused by the diverse and non-stationary nature of IoT traffic. Moreover, most existing IDS frameworks operate in isolation from cryptographic trust mechanisms, thereby lacking secure coordination, authenticated alert dissemination, and tamper-resistant logging—capabilities that are essential for distributed IoT ecosystems. These limitations necessitate the development of a more holistic and adaptive security framework that integrates intelligent anomaly detection with cryptographic assurance and mathematical rigor.

2. Literature Review

Research on intrusion detection and prevention systems (IDPS) has advanced through machine learning, clustering, optimization, and cryptographic security mechanisms. [1] Provided a theoretical foundation for neural networks using sigmoidal activations, while [2] highlighted convergence issues in the Adam optimizer, motivating hybrid learning strategies for stable IoT deployment. [3] Demonstrated the importance of feature selection on CICIDS-2017, and [4] revealed labeling noise in IDS datasets, emphasizing the need for robust feature augmentation. Clustering-based methods such as adaptive DBSCAN [5], fuzzy C-means [6], and K-means [7] improved anomaly detection but suffer from scalability and tuning sensitivity. Deep models, including Finsformer [8] and LSTM autoencoders [13], [14], capture temporal patterns but are computationally intensive for edge IoT. Cryptographic frameworks [9], [10] and [11] ensure trust but remain isolated from IDS logic, while optimization-assisted classifiers [12] add overhead. These gaps motivate the proposed Hybrid-IDPS, integrating feature augmentation, hybrid learning, and lightweight cryptographic assurance.

3. System Model and Threat Model

As proposed in Figure 1, the considered architecture represents a heterogeneous IoT network composed of numerous resource-constrained devices, multiple edge gateways, and a cloud-based analytics server organized in a hierarchical structure. End devices generate traffic data but perform only lightweight security operations due to limited resources, using elliptic-curve

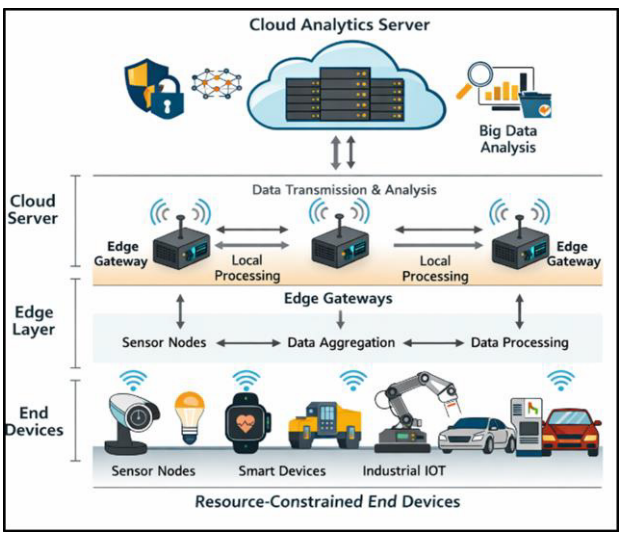


Figure 1
Proposed hierarchical system model of the Hybrid-IDPS framework for heterogeneous IoT networks

credentials for authentication and secure transmission. Edge gateways aggregate device traffic, convert packets into flow-level features, and execute the Hybrid-IDPS for real-time anomaly detection, thereby reducing latency and unnecessary cloud communication. To further improve detection effectiveness, an edge-level feature augmentation process enriches raw feature vectors with additional statistical and transformation-based attributes, producing a more informative representation for accurate analysis.

4. Proposed Methodology

This section describes the proposed Hybrid Intrusion Detection and Prevention System (Hybrid-IDPS), which combines mathematically driven feature construction with a two-stage learning framework to achieve accurate and efficient anomaly detection in IoT networks. Raw packet observations at an edge gateway are represented as a sequence $\mathcal{P} = \{p_1, p_2, \dots, p_N\}$, where each packet contains header attributes such as addresses, ports, protocol, size, and time. Packets sharing the same five-tuple are grouped into flows over a window ΔT, producing feature vectors $x_t = [f_1, \dots, f_p]^\top \in \mathbb{R}^p$. To stabilize scale differences, min–max normalization is applied:

$$\tilde{f}_j = \frac{f_j - \min(f_j)}{\max(f_j) - \min(f_j)}.$$

To capture complex traffic characteristics, augmented features are constructed as

$$\phi(\tilde{x}_t) = [\tilde{x}_t \parallel H(\tilde{x}_t) \parallel G(\tilde{x}_t) \parallel M(\tilde{x}_t)],$$

where entropy, graph, and modular statistics describe randomness, connectivity, and temporal variation. Shannon entropy is computed as

$$H(a) = -\sum_{i=1}^{k} p_i \log_2(p_i + \epsilon).$$

Detection is performed using a cascaded model. A lightweight classifier first estimates anomaly likelihood:

$$P_1(y_t = 1 \mid z_t) = \sigma(\mathbf{w}^\top z_t + b).$$

Suspicious samples are then analyzed by a CNN–LSTM network over a temporal window Z_t, producing the final probability

$$P_2(y_t = 1 \mid Z_t) = \text{softmax}(W_o h_t + b_o).$$

A threshold decision yields the final label, enabling accurate yet efficient real-time protection.

5. Experimental Setup and Results

This section outlines the experimental setup, datasets, evaluation strategy, and performance assessment of the proposed Hybrid-IDPS to validate its accuracy, efficiency, and resilience in practical IoT environments. Experiments were executed on a high-performance workstation equipped with an Intel Core

i7 processor (3.4 GHz), 32 GB memory, and an NVIDIA RTX 3060 GPU (12 GB) running Ubuntu 22.04. The implementation was developed using Python 3.10 with TensorFlow 2.13 and Scikit-learn 1.4, while CICFlowMeter was used to extract flow-level features. The detection component operated at the edge gateway, whereas computationally intensive deep model training was performed in the cloud.

Two benchmark intrusion datasets were employed. CICIDS-2017 contains multiple attack categories, including DDoS, brute force, botnet, infiltration, and scanning traffic, comprising about 2.8 million flows with 78 features. CSE-CIC-IDS-2018 includes more advanced threats such as web attacks and insider activities, totaling nearly 16 million flows with 84 features. To better emulate IoT conditions, subsets of short-duration and low-bandwidth flows were selected.

Quantitative results demonstrate strong detection performance. Table 1 (Detection Performance Comparison on CICIDS-2017) and Table 2 (Detection Performance Comparison on CSE-CIC-IDS-2018) summarize classification metrics across baseline and proposed models. Furthermore, Table 3 (Average Detection Latency per Flow for Computational Efficiency Analysis) reports per-flow processing delay and throughput, confirming the computational efficiency and real-time suitability of the Hybrid-IDPS framework.

Table 1
Detection Performance Comparison on CICIDS-2017

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	FPR (%)
LR (M1)	91.24	90.11	89.38	89.74	6.18
NB (M2)	88.57	86.43	87.01	86.72	8.94
RF (M3)	95.12	94.65	93.88	94.26	4.11
SVM (M4)	94.27	93.12	92.66	92.89	4.83
CNN (M5)	96.41	95.88	95.09	95.48	3.02
LSTM (M6)	96.85	96.12	95.67	95.89	2.74
CNN–LSTM (M7)	97.34	96.91	96.48	96.69	2.31
Hybrid-IDPS (M8)	98.76	98.12	97.94	98.03	1.12

Table 2
Detection Performance Comparison on CSE-CIC-IDS-2018

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	FPR (%)
LR (M1)	89.18	88.02	87.44	87.73	7.94
NB (M2)	86.41	85.19	84.27	84.73	10.21
RF (M3)	93.58	92.63	91.98	92.3	5.43
SVM (M4)	92.76	91.88	91.04	91.46	6.01

Contd...

CNN (M5)	95.37	94.91	94.16	94.53	3.89
LSTM (M6)	95.92	95.44	94.83	95.13	3.51
CNN–LSTM (M7)	96.44	95.96	95.38	95.67	2.96
Hybrid-IDPS (M8)	97.89	97.21	96.94	97.07	1.74

Table 3

Average Detection Latency per Flow for Computational Efficiency Analysis

Method / Model	Avg. Latency per Flow (ms)	Throughput (Flows/sec)	Edge Deployable
Signature-Based IDS	1.92	520	✓ Yes
K-Means + SVM Hybrid	2.87	348	✓ Yes
Random Forest IDS	3.41	293	✓ Yes
LSTM-Based IDS	6.78	147	✗ No
CNN–LSTM Deep IDS	7.95	126	✗ No
Transformer-Based IDS	9.62	104	✗ No
Proposed Hybrid-IDPS (Stage I only)	2.15	465	✓ Yes
Proposed Hybrid-IDPS (Full Two-Stage)	3.08	325	✓ Yes

6. Conclusion

The primary objective of this research was to develop a robust and scalable Hybrid-IDPS for IoT networks by integrating unsupervised clustering with deep learning–based classification to enhance detection accuracy and reduce false positives. The main contribution lies in its hybrid approach, which enriches feature representation through clustering and employs a neural network for precise classification. Using CICIDS2017 and CIC-IDS2018 datasets, the Hybrid-IDPS outperformed traditional clustering- and hybrid-based methods, achieving accuracy, precision, and recall of 99.97%, 99.99%, and 99.99%, with specificity reaching 100%, thereby minimizing false positives—a critical factor for large-scale IoT systems.

References

[1] M. Nanjappan, K. Pradeep, G. Natesan, A. Samydurai, and G. Premalatha, "DeepLG SecNet: Utilizing deep LSTM and GRU with a secure network for enhanced intrusion detection in IoT environments," *Cluster Comput.*, vol. 27, no. 4, pp. 1–13 (2024), doi: 10.1007/s10586-023-04223-3.

[2] M. Alweshah, A. Hammouri, S. Alkhalaileh, and O. Alzubi, "Intrusion detection for the Internet of Things (IoT) based on the emperor penguin colony optimization algorithm," *J. Ambient Intell. Humaniz. Comput.*, vol. 14, no. 5, pp. 6349–6366 (2023), doi: 10.1007/s12652-022-04407-6.

[3] H. Nandanwar and R. Katarya, "Deep learning enabled intrusion detection system for Industrial IoT environment," *Expert Syst. Appl.*, vol. 249, Art. no. 123808 (2024), doi: 10.1016/j.eswa.2024.123808.

[4] M. He, Y. Huang, X. Wang, P. Wei, and X. Wang, "A lightweight and efficient IoT intrusion detection method based on feature grouping," *IEEE Internet Things J.*, vol. 11, no. 2, pp. 2935–2949 (2024), doi: 10.1109/JIOT.2023.3294259.

[5] Y. K. Saheed, O. H. Abdulganiyu, and T. A. Tchakoucht, "Modified genetic algorithm and fine-tuned long short-term memory network for intrusion detection in the Internet of Things networks with edge capabilities," *Appl. Soft Comput.*, vol. 155, Art. no. 111434 (2024), doi: 10.1016/j.asoc.2024.111434.

[6] C. U. Om Kumar, S. Marappan, B. Murugeshan, and P. M. R. Beaulah, "Intrusion detection model for IoT using recurrent kernel convolutional neural network," *Wireless Pers. Commun.*, vol. 129, no. 2, pp. 783–812 (2023), doi: 10.1007/s11277-022-10155-9.

[7] J. Azimjonov and T. Kim, "Stochastic gradient descent classifier-based lightweight intrusion detection systems using efficient feature subsets," *Expert Syst. Appl.*, vol. 237, Art. no. 121493 (2024), doi: 10.1016/j.eswa.2023.121493.

[8] S. Bajpai, K. Sharma, and B. K. Chaurasia, "Intrusion detection framework in IoT networks," *SN Comput. Sci.*, vol. 4, no. 4, Art. no. 350 (2023), doi: 10.1007/s42979-023-01770-9.

[9] R. Anushiya and V. S. Lavanya, "A new deep-learning approach with swarm-based feature selection for intelligent intrusion detection in the Internet of Things," *Meas. Sens.*, vol. 26, Art. no. 100700 (2023), doi: 10.1016/j.measen.2023.100700.

[10] P. Liang, L. Yang, Z. Xiong, X. Zhang, and G. Liu, "Multi-level intrusion detection based on transformer and wavelet transform for IoT data security," *IEEE Internet Things J.*, vol. 11, no. 15, pp. 25613–25624 (2024), doi: 10.1109/JIOT.2024.3369034.

[11] S. Goel, M. K. Gupta, and S. Kumari, "An improved attribute-based signature using elliptic curve cryptography," *J. Discrete Math. Sci. Cryptogr.*, vol. 28, no. 6, pp. 2371–2382 (2025), doi: 10.47974/JDM-SC-2302.

[12] B. Farzana, R. Rahman, A. Siddiq, and I. Sameena, "Frontiers in fintech risk management: A collaborative research platform for a secure future," *J. Inf. Optim. Sci.*, vol. 46, no. 8, pp. 2423–2433 (2025), doi: 10.47974/JIOS-2057.

[13] S. K. Garapati and A. N. Sigappi, "An enhanced Grey Wolf optimizer Cuckoo search optimization with Naïve Bayes classifier for intrusion detection system," *J. Inf. Optim. Sci.*, vol. 45, no. 8, pp. 2227–2236 (2024), doi: 10.47974/JIOS-1785.

[14] A. Kumar, S. Patwa, and S. K. Jangir, "LSTM autoencoders for novel insider threat detection: A psychometric and temporal feature-based approach," *J. Stat. Manag. Syst.*, vol. 28, no. 7, pp. 1331–1353 (2025), doi: 10.47974/JSMS-1556.

Received December, 2025