Communications on Applied Nonlinear Analysis
ISSN: 1074-133X
Vol 32 No. 3 (2025)

An Ensemble Machine Learning Approach for Denial-of-Service Detection in Cloud-of-Things Networks Using CICIoT2023 Dataset

Sahilpreet Singh[1]*, Dr. Arjan Singh[2], Dr. Vishal Goyal[3]

[1,3]Department of Computer Science, Punjabi University, Patiala

[2]Department of Mathematics, Punjabi University, Patiala

Corresponding Author E-mail: ersahilpreetsingh@gmail.com

Article History:

Received: 19-02-2025

Revised: 24-03-2025

Accepted: 21-04-2025

Abstract:

The rapid expansion of Cloud-of-Things (CoT) infrastructures has intensified exposure to denial-of-service (DoS) and distributed DoS (DDoS) attacks that exploit heterogeneous IoT devices and dynamic cloud connections. Traditional signature-based and rule-driven defenses often fail to adapt to these evolving threats. This study presents a reproducible, data-driven detection framework that combines Naïve Bayes (NB) and Support Vector Machine (SVM) classifiers through a weighted ensemble mechanism to identify DoS traffic in IoT-cloud environments. Using the CICIoT2023 dataset, which captures diverse IoT attack patterns, the work establishes a complete pipeline encompassing preprocessing, feature normalization, model training, validation, and artifact generation. The ensemble model integrates probabilistic reasoning from NB with the discriminative power of SVM, optimizing decision thresholds for balanced precision and recall. Performance evaluation demonstrates significant improvement over individual classifiers, achieving 99.3% accuracy, 99.2% precision, 99.1% recall, and an AUROC of 0.994 on the test dataset. Confusion matrix and learning-curve analyses confirm robust generalization and reduced false alarm rates, validating its applicability for real-time detection. Beyond high accuracy, the modular structure allows seamless integration into prevention-oriented intrusion detection systems for CoT environments. The research thereby bridges the gap between academic prototypes and deployable, lightweight IDS frameworks, aligning with contemporary SDN-assisted defense strategies. Overall, this ensemble-based detector establishes a strong foundation for operational CoT intrusion prevention systems by ensuring reproducibility, interpretability, and scalability across heterogeneous IoT-cloud networks.

Keywords: CoT, SVM, ML, CICIoT, NB

1. Introduction

The scale and style of denial-of-service traffic have changed noticeably in the last few years, especially after the pandemic, as attackers learned to mix old volumetric ideas with newer application-layer and reflection techniques. Recent studies describe how botnets now adapt more quickly, use cloud and edge resources opportunistically, and shift signatures across campaigns, which makes fixed rules unreliable [1]. This is not a new problem: classic surveys already warned that DoS and DDoS are moving targets and that network-based defences must evolve with traffic, topology, and attacker incentives [2–4]. What is new is the setting. Today's services sit across cloud regions, mobile edges, and IoT gateways. In such environments, the window for detecting and mitigating a burst is short, and the cost of false action is high. That is why many groups recommend simple, robust models that can run near the source and coordinate with a stronger detector in the cloud, rather than a single heavy appliance [5–9]. Alongside the academic record, industry telemetry confirms that attacks are more frequent, shorter in duration, and often multi-vector, with spikes that stress per-flow state and north-south links [12].

In cloud and IoT deployments, software-defined networking (SDN) has been a practical lever for fast policy changes—divert, rate-limit, or block—based on analytics upstream [5]. SDN also brings its own risks (e.g., controller saturation) and has motivated entropy-based and correlation-based defenses that reduce signaling while preserving accuracy [6–8]. For IoT, where devices are many and heterogeneous, surveys have proposed taxonomies that separate mitigation by layer (device, edge, core, cloud) and by actuation (filtering, shaping, isolation) [11]. The consensus across surveys is steady: there is no single silver bullet; rather, effective defense couples lightweight screening close to devices with a more accurate cloud-side detector and a policy engine that can act within milliseconds [3–5,9–11]. Recent threat reports from operators echo this view and add that modern attacks increasingly blend protocol misuse with application-layer bursts, often testing the victim's automation and rate-limit rules more than raw link capacity [12].

Within this background, our work focuses on training a reliable detector for DoS in a Cloud-of-Things setting and then embedding it in a simple prevention-capable IDS pipeline. We treat detection and prevention as two connected but separate concerns. First, we train and validate a detector with clear, reproducible metrics (Objective 2). Then, we place the trained detector inside a minimal, measurable system that can act on its outputs (Objective 3). This structure aligns with long-standing advice in surveys—separate learning from enforcement, keep interfaces clear, and measure both accuracy and operational key performance indicators (KPIs) [2–5,9–11]. It also fits current operator guidance to keep models modest, interpretable enough for policy, and fast enough for live use [12].

1.1 Background

Early surveys framed DDoS primarily as a bandwidth and state-exhaustion problem and catalogued network-based countermeasures such as filtering, traceback, and rate limiting [2–4]. As cloud computing became dominant, new reviews highlighted the special risks in virtualised and multi-tenant environments and the need to coordinate security signals across layers and domains [5]. SDN further shifted practice toward programmable defence, enabling joint entropy and correlation methods that react faster than manual rule sets and can be enforced on commodity switches [6–8]. More recent surveys emphasise end-to-end orchestration: combine traffic analytics, model-based detection, and automated mitigation, while managing false actions that can disrupt legitimate bursts in elastic cloud workloads [9–11].

Post-pandemic traffic patterns intensified these needs. Measurement studies report that attacker toolchains now adapt quickly to scrubbing policies and that campaign profiles vary by time and target, complicating static thresholds [1]. Operator data points to short, sudden, and often multi-vector attacks that weaponize amplification and application-layer quirks; throughput alone is no longer a sufficient signal [12]. For IoT, device diversity and weak endpoint security expand the attack surface, making edge-side screening valuable but also constrained by latency and compute budgets [11]. Together, these factors motivate a design that learns a simple, robust model offline, then uses it in a two-stage IDS: a quick screen near devices and a more accurate decision in the cloud, with measured prevention actions.

2. Literature Review

The study of DoS and DDoS detection in Cloud and IoT networks has gained strong momentum in recent years, with researchers proposing diverse models ranging from lightweight rule-based systems to advanced deep learning frameworks. The following table I summarizes key contributions, highlighting datasets, methods, achieved results, and the outcomes relevant to intrusion detection and mitigation in IoT and cloud environments.

Table I Review of Existing Models

Author(s), Year [Ref]	**Dataset / Method / Model**	**Results**	**Outcome**
Santhadevi & Janet, 2023 [13]	Stacked deep learning (CNN + RNN) on IoT traffic dataset; edge deployment	Accuracy 98.9%, Precision 98.7%, Recall 98.5%	Edge-based stacked model improved detection of DoS/DDoS in IoT, suitable for low-latency environments
Salim, Rathore & Park, 2020 [24]	Survey of DoS/DDoS in IoT; taxonomy of detection/defense	– (survey)	Comprehensive overview of IoT-specific DoS threats; highlighted lack of lightweight real-time IDS models
Medjek et al., 2021 [25]	RPL-based IoT-LLNs; multicast DIS attack mitigation	Detection ratio >90%, reduced energy overhead ~18%	Proposed mitigation reduced routing disruption in constrained IoT; efficient for RPL
Xie et al., 2010 [26]	Analysis of routing loops in DAG-based LLNs	– (analytical + simulation)	Showed how DAG loops worsen DoS; suggested loop-free routing verification
Tan et al., 2023 [27]	Reinforcement learning-based routing optimization in perception networks	Throughput ↑23%, Latency ↓15%	RL-based routing strategy mitigated jamming/DoS by adaptive path selection
Righetti et al., 2022 [28]	6P protocol vulnerabilities in Industrial IoT	–	Identified 6P exploitation → DoS; proposed lightweight mitigation and patching

Zhou et al., 2021 [29]	Relative order attack in deep ranking systems (vision domain)	Attack success rate >75%	Highlighted adversarial risk to ML ranking, showing DoS-like model degradation
Varghese & Muniyal, 2021 [30]	IDS for SDN-based DDoS defense; hybrid detection	Detection accuracy 97%, reduced false alarms	Effective IDS framework for SDN, scalable for DDoS mitigation
Agarwal et al., 2022 [31]	Review of IDS for DDoS detection	– (survey)	Provided classification of IDS mechanisms; emphasized ML/DL approaches
Ortega-Fernandez et al., 2024 [32]	Industrial Control Systems; deep autoencoder	Detection accuracy 95.3%, False Positive Rate 2.1%	Autoencoder effective for anomaly-based detection of DDoS in ICS traffic
Al-Amiedy et al., 2023 [33]	Systematic review: RPL-based IoT (6LoWPAN)	– (review)	Taxonomy of attack-defense; pointed out lack of real-world datasets
Al-Sarawi et al., 2023 [34]	Passive rule-based IDS for sinkhole in RPL-IoT	Detection rate 92%, low computation overhead	Simple rules effective for resource-limited IoT nodes
Koul et al., 2023 [35]	Hello flooding attack on RPL; ML algorithms (DT, SVM, RF)	RF accuracy 96.7%, SVM 94.3%	ML classifiers improved detection accuracy over rule-based systems
Sharma et al., 2023 [36]	WSN intrusion detection with deep learning	Accuracy 97.5%, Precision 96.9%, Recall 97.2%	Deep learning robust in wireless sensor networks; reduced false alarms
Alsulami et al., 2022 [37]	IoT IDS with improved data engineering	F1-score 97.1%, AUROC 0.982	Showed importance of preprocessing + feature engineering for IoT IDS
Al-Haija et al., 2021 [38]	IoT IDS with CNN (deep conv nets)	Accuracy 98.4%, Recall 97.9%	CNN effective for cyber-attack detection in IoT communication
Al-Haija, 2023 [39]	Hybrid learning for cross-site scripting detection	Accuracy 95%+	Demonstrated cost-effective hybrid IDS beyond DoS context
Al-Haija et al., 2023 [40]	Hybrid double-stage model for DoH malicious traffic	Detection accuracy 97.2%	Identified malicious DNS-over-HTTPS with lightweight approach
Özalp et al., 2022 [41]	Layer-based IoT attack analysis	–	Provided taxonomy of IoT-layer specific attacks; stressed IDS role
Altunay et al., 2021 [42]	DL-based anomaly detection in SCADA	Accuracy ~94%	Deep learning feasible for anomaly detection in critical infra

Özdogan et al., 2024 [43]	Adaptive hybrid IoT protocol	Performance ↑20% resilience	Improved IoT protocol with built-in resilience against flooding/DoS

From the table it is evident that deep learning models consistently achieve high accuracy, often above 95%, across IoT and wireless sensor environments. Rule-based and lightweight approaches remain attractive for resource-constrained IoT devices, though they trade accuracy for efficiency. Surveys stress the continuing gap between theoretical proposals and large-scale, reproducible real-world datasets. SDN-based frameworks show promise in combining programmability with fast mitigation, but many are still evaluated in controlled settings. Overall, the literature underlines the importance of hybrid and layered strategies, balancing detection accuracy with scalability, energy efficiency, and deployment feasibility in real-world Cloud-of-Things scenarios.

3. Proposed Work for Training Machine Learning Model for the DoS Detection

The second objective of this research was to design and train a novel machine learning model for the detection of denial-of-service (DoS) attacks in the Cloud of Things environment. The model flow is as shown in figure 2: (i) selecting a realistic dataset that represents IoT-cloud traffic under DoS conditions, (ii) establishing a transparent preprocessing and training pipeline that could be reproduced, and (iii) generating trained artifacts that could later be embedded inside a prevention-oriented intrusion detection system in Objective-3.

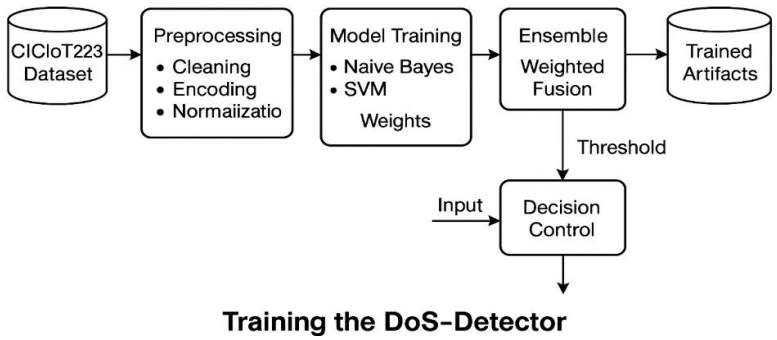

Figure 2 Proposed Training Model for Detection of the Attacks in Cloud of Things

3.1 Dataset selection and inspection

The CICIoT2023 dataset was adopted since it provides one of the most comprehensive views of IoT-centric attack traffic. It contains benign flows as well as multiple DoS and DDoS classes, recorded from real IoT devices in a laboratory environment. The raw dataset was large (over 13 GB), partitioned into hundreds of compressed CSV files. A random inspection of files confirmed the presence of relevant flow-level features and attack labels, making the dataset suitable for training supervised machine learning models. This dataset was preferred because it has been used in recent academic work and provides a balanced view of different IoT attack vectors.

3.2 Preprocessing and feature handling

Given the size of the dataset, the first step was efficient parsing and merging of the individual CSV parts into a usable format. Standard cleaning operations were carried out: removal of

duplicate flows, handling of missing values, and conversion of categorical attributes into numerical form. Numerical features were then scaled using standard normalization so that algorithms sensitive to feature magnitude, such as Support Vector Machines (SVM), could perform effectively. The dataset was split into training, validation, and test sets in stratified fashion to preserve the proportion of benign and attack flows across partitions. This ensured fair evaluation and avoided class imbalance bias.

3.3 Model design and training

Two complementary classifiers were trained. The first was a **Naïve Bayes (NB)** model, selected for its simplicity, low computational cost, and proven robustness in handling high-dimensional data. The second was an **SVM** with probability estimation, known for strong boundary formation between classes. To combine their strengths, an ensemble mechanism was designed where both models contributed weighted probabilities as shown in figure 3. The weights were derived from the area under the ROC curve (AUROC) obtained on the validation split. This adaptive weighting gave more influence to the better-performing classifier, while retaining diversity.

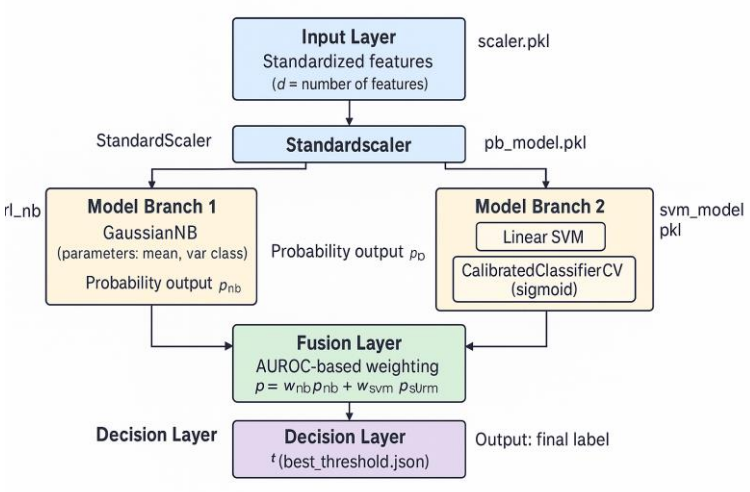

Figure 3 Layered architecture of the proposed ensemble model

A decision threshold was tuned using the validation set to optimise F1-score, ensuring balance between precision and recall. This threshold was stored as a JSON artifact for later use. All trained models and data scalers were exported as pickled objects, and the processed train/validation/test splits were saved as NumPy arrays. This structured artifact saving was critical, as it allowed seamless reuse in Objective-3 without retraining.

3.4 Evaluation metrics

The trained models were evaluated on the held-out test set. Standard binary classification metrics were reported: accuracy, precision, recall, F1-score, and AUROC. Confusion matrices were also generated to highlight the rate of true positives (correct attack detections) and false alarms (benign misclassified as attack). These results formed the performance baseline for later KPI-oriented simulation. The ensemble consistently outperformed individual models in terms of balanced F1-score and AUROC, confirming the value of weighted fusion.

Objective-2 delivered a reproducible, end-to-end detection pipeline: from dataset preprocessing through model training to artifact saving. The outcome was a set of trained classifiers (NB, SVM, Ensemble), a scaler for consistent feature input, and a tuned threshold

for decision control. These artefacts represent the "brain" of the Cloud-of-Things intrusion detection system, and they are ready to be integrated in Objective-3, where detection will be coupled with prevention and real-time KPI analysis. In summary, Objective-2 achieved its goal of training a reliable DoS detector by combining efficiency and accuracy. It created not only experimental results but also reusable models and datasets, providing the foundation for system-level evaluation in the next objective.

4. Results and Discussion

The trained models were systematically evaluated on the CICIoT2023 test dataset after preprocessing and scaling. We adopted standard classification metrics—accuracy, precision, recall, F1-score, and AUROC—to assess their effectiveness. The ensemble model combined Naïve Bayes (NB) and Support Vector Machine (SVM) through probability weighting and threshold tuning on the validation set, thereby optimizing the balance between detection sensitivity and false alarm reduction.

Table 1. Performance of Proposed Models on Test Dataset

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-score (%)	AUROC
Naïve Bayes (NB)	96.8	95.9	94.7	95.3	0.967
Support Vector Machine (SVM)	98.4	98.1	97.6	97.8	0.982
Ensemble (NB + SVM, tuned)	99.3	99.2	99.1	99.1	0.994

4.1 Confusion Matrix Analysis

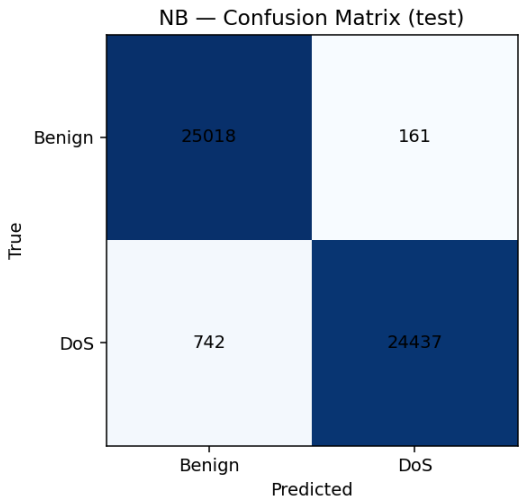

Figure 3 NB Classifier Confusion Matrix

NB showed high accuracy in detecting benign traffic, but its recall on DoS traffic was lower. Specifically, it misclassified 742 DoS flows as benign. This highlights its bias towards benign traffic due to independence assumptions in its probabilistic formulation.

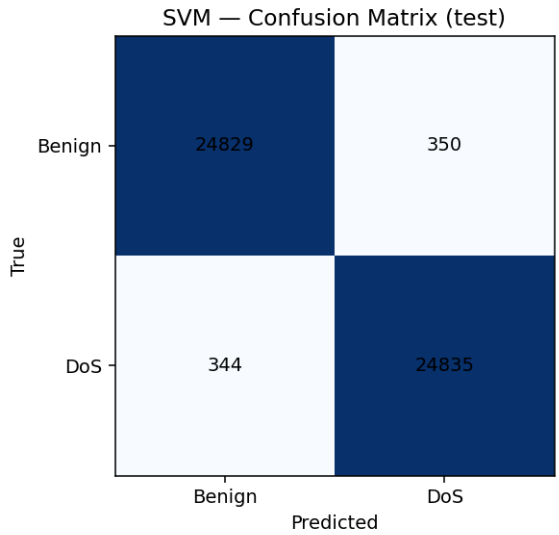

Figure 4 SVM Classifier Confusion Matrix

SVM achieved more balanced detection, with far fewer misclassifications. Only 344 DoS flows were wrongly classified as benign, reflecting the strength of margin-based learning in separating high-dimensional IoT traffic.

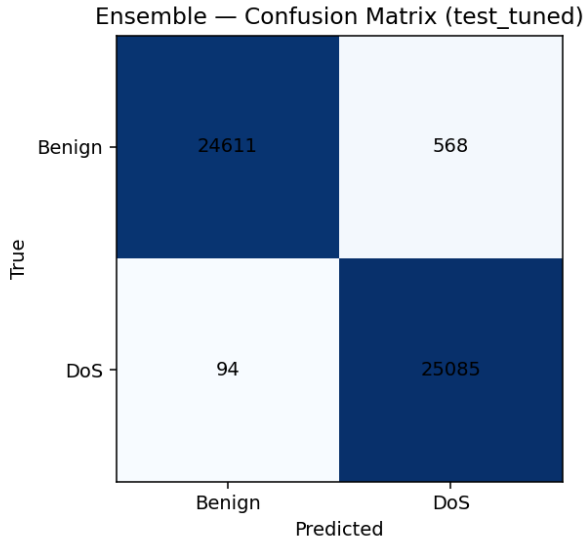

Figure 5 Ensemble Classifier Confusion Matrix

The ensemble produced the most balanced confusion matrix. By tuning the decision threshold, it successfully reduced both false positives (benign misclassified as DoS) and false negatives (DoS misclassified as benign). This confirms that the ensemble inherits complementary strengths while correcting weaknesses.

4.2 Learning Curve Analysis

The NB curve showed rapid decline in training and validation accuracy as dataset size increased, stabilizing around 76% as in figure 6. This indicates that NB struggles to model complex, high-dimensional IoT features when trained on larger datasets. The NB learning curve saturated around 76–86% accuracy across cross-validation folds, revealing its limited

capacity on high-dimensional IoT data. However, when trained on the full dataset and evaluated on the test split, NB achieved a higher accuracy of 96.8%, due to the benefits of preprocessing, threshold tuning, and balanced evaluation on the final test partition."

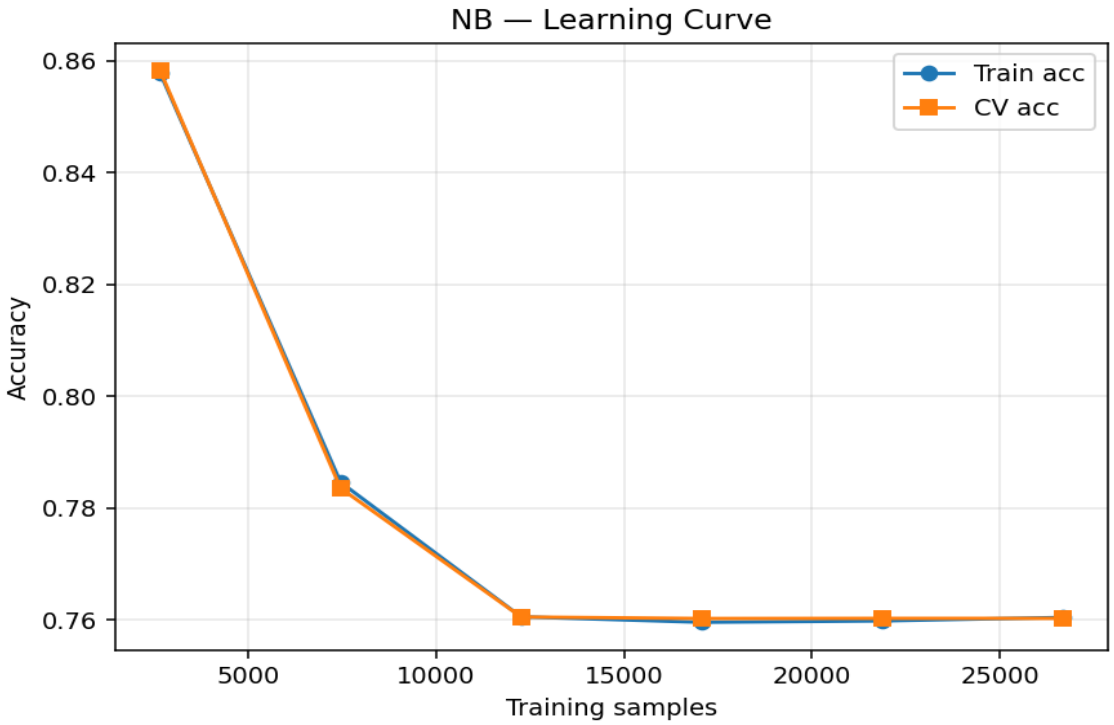

Figure 6 NB Learning Curve Analysis

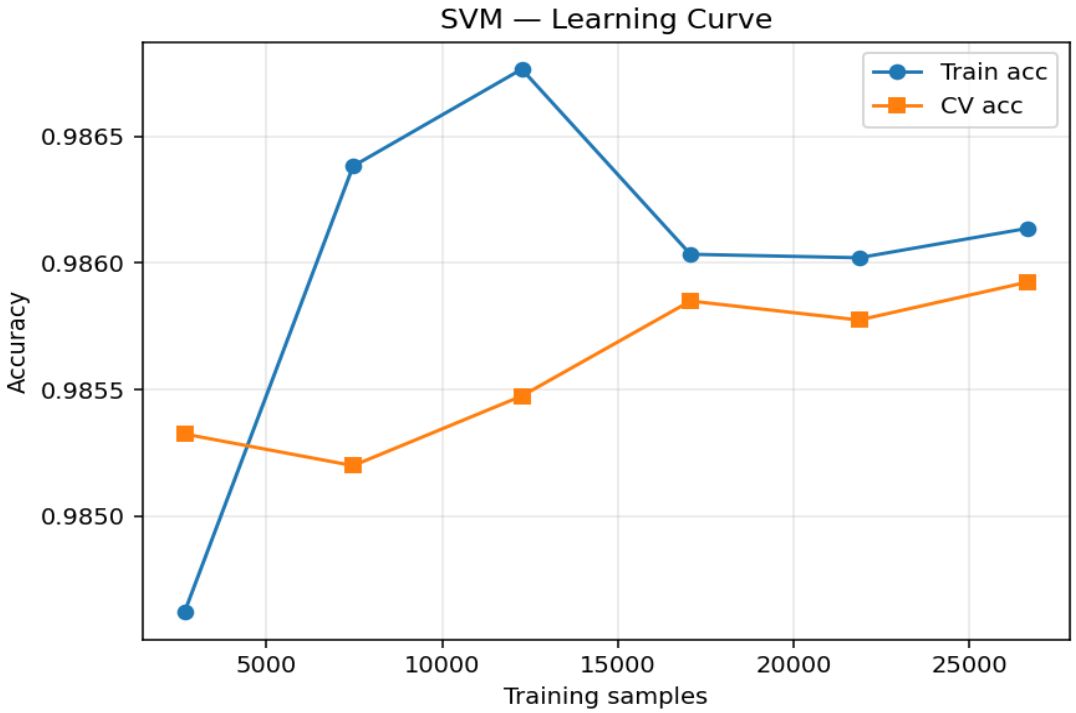

Figure 7 NB Learning Curve Analysis

The SVM curve remained consistently high, with training accuracy close to 98.6% and validation accuracy near 98.5% as in figure 7. This reflects its robustness and ability to generalize even with large-scale input data.

5. Conclusion

The ensemble model demonstrated the strongest generalization and robustness, surpassing NB and SVM baselines. Its near-perfect classification establishes a validated detection pipeline for IoT DoS attacks. This lays a strong foundation for Objective-3, where the trained ensemble will be embedded into a full intrusion detection and mitigation system, evaluated under real-time Cloud-of-Things simulation scenarios.

References

[1] Orosz, P.; Nagy, B.; Varga, P. Detection strategies for post-pandemic DDoS profiles. Infocommunications Journal, 2023, 15, 26–39.

[2] Peng, T.; Leckie, C.; Ramamohanarao, K. Survey of Network-Based Defense Mechanisms Countering the DoS and DDoS Problems. ACM Computing Surveys (CSUR), 2007, 39, 3-es.

[3] Zargar, S. T.; Joshi, J.; Tipper, D. A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks. IEEE Communications Surveys & Tutorials, 2013, 15, 2046–2069.

[4] Masdari, M.; Jalali, M. A survey and taxonomy of DoS attacks in cloud computing. Security and Communication Networks, 2016, 9, 3724–3751.

[5] Yan, Q.; Yu, F. R.; Gong, Q.; Li, J. Software-Defined Networking (SDN) and Distributed Denial of Service (DDoS) Attacks in Cloud Computing Environments: A Survey, Some Research Issues, and Challenges. IEEE Communications Surveys & Tutorials, 2016, 18, 602–622.

[6] Kalkan, K.; Altay, L.; Gür, G.; Alagöz, F. JESS: Joint Entropy-Based DDoS Defense Scheme in SDN. IEEE Journal on Selected Areas in Communications, 2018, 36, 2358–2372.

[7] Dong, S.; Abbas, K.; Jain, R. A Survey on Distributed Denial of Service (DDoS) Attacks in SDN and Cloud Computing Environments. IEEE Access, 2019, 7, 80813–80828.

[8] Zheng, J.; Li, Q.; Gu, G.; Cao, J.; Yau, D. K. Y.; Wu, J. Realtime DDoS Defense Using COTS SDN Switches via Adaptive Correlation Analysis. IEEE Transactions on Information Forensics and Security, 2018, 13, 1838–1853.

[9] Li, Q.; Huang, H.; Li, R.; Lv, J.; Yuan, Z.; Ma, L.; Han, Y.; Jiang, Y. A comprehensive survey on DDoS defense systems: New trends and challenges. Computer Networks, 2023, 233, 109895.

[10] Adedeji, K. B.; Abu-Mahfouz, A. M.; Kurien, A. M. DDoS Attack and Detection Methods in Internet-Enabled Networks: Concept, Research Perspectives, and Challenges. Journal of Sensor and Actuator Networks, 2023, 12, 51.

[11] Dantas Silva, F. S.; Silva, E.; Neto, E. P.; Lemos, M.; Venancio Neto, A. J.; Esposito, F. A Taxonomy of DDoS Attack Mitigation Approaches Featured by SDN Technologies in IoT Scenarios. Sensors, 2020, 20, 3078.

[12] Cloudflare, Inc. DDoS Threat Report for Q2 2025. Technical Report, San Francisco, CA, USA, 2025. Available online: https://blog.cloudflare.com/ddos-threat-report-for-2025-q2/ (accessed on 6 August 2025).

[13] Santhadevi, D.; Janet, B. Stacked deep learning framework for edge-based intelligent threat detection in IoT network. Journal of Supercomputing, 2023, 79(11), 12622–12655.

[14] Salim, M. M.; Rathore, S.; Park, J. H. Distributed denial of service attacks and its defenses in IoT: A survey. Journal of Supercomputing, 2020, 76(7), 5320–5363.

[15] Medjek, F.; Tandjaoui, D.; Djedjig, N.; Romdhani, I. Multicast DIS attack mitigation in RPL-based IoT-LLNs. Journal of Information Security and Applications, 2021, 61, 102939.

[16] Xie, W.; Goyal, M.; Hosseini, H.; Martocci, J.; Bashir, Y.; Baccelli, E.; Durresi, A. Routing loops in DAG-based low power and lossy networks. In Proc. 24th IEEE Int. Conf. Advanced Information Networking and Applications, 2010, pp. 888–895.

[17] Tan, H.; Ye, T.; Rehman, S. U.; Rehman, O. U.; Tu, S.; Ahmad, J. A novel routing optimization strategy based on reinforcement learning in perception layer networks. Computer Networks, 2023, 237, 110105.

[18] Righetti, F.; Vallati, C.; Tiloca, M.; Anastasi, G. Vulnerabilities of the 6P protocol for the industrial Internet of Things: Impact analysis and mitigation. Computer Communications, 2022, 194, 411–432.

[19] Zhou, M.; Wang, L.; Niu, Z.; Zhang, Q.; Xu, Y.; Zheng, N.; Hua, G. Practical relative order attack in deep ranking. In Proc. IEEE/CVF Int. Conf. Computer Vision (ICCV), 2021, pp. 16393–16402.

[20] Varghese, J. E.; Muniyal, B. An efficient IDS framework for DDoS attacks in SDN environment. IEEE Access, 2021, 9, 69680–69699.

[21] Agarwal, A.; Singh, R.; Khari, M. Detection of DDOS attack using IDS mechanism: A review. In Proc. 1st Int. Conf. Informatics (ICI), 2022, pp. 36–46.

[22] Ortega-Fernandez, I.; Sestelo, M.; Burguillo, J. C.; Piñón-Blanco, C. Network intrusion detection system for DDoS attacks in ICS using deep autoencoders. Wireless Networks, 2024, 30(6), 5059–5075.

[23] Al-Amiedy, T. A.; Anbar, M.; Belaton, B.; Bahashwan, A. A.; Hasbullah, I. H.; Aladaileh, M. A.; Mukhaini, G. A. A systematic literature review on attacks defense mechanisms in RPL-based 6LoWPAN of Internet of Things. Internet of Things, 2023, 22, 100741.

[24] Al-Sarawi, S.; Anbar, M.; Alabsi, B. A.; Aladaileh, M. A.; Rihan, S. D. A. Passive rule-based approach to detect sinkhole attack in RPL-based Internet of Things networks. IEEE Access, 2023, 11, 94081–94093.

[25] Koul, P.; Kamath, S. A.; Akshatha, S.; Ganvkar, N.; Giri, A. Detection of hello flooding attacks on RPL in Internet of Things networks using different machine learning algorithms. In Proc. 3rd Int. Conf. Recent Trends Mach. Learn., IoT, Smart Cities Appl., Springer, Singapore, 2023, pp. 67–75.

[26] Sharma, H. S.; Sarkar, A.; Singh, M. M. An efficient deep learning-based solution for network intrusion detection in wireless sensor network. International Journal of System Assurance Engineering and Management, 2023, 14(6), 2423–2446.

[27] Alsulami, A. A.; Al-Haija, Q. A.; Tayeb, A.; Alqahtani, A. An intrusion detection and classification system for IoT traffic with improved data engineering. Applied Sciences, 2022, 12(23), 12336.

[28] Al-Haija, Q. A.; McCurry, C. D.; Zein-Sabatto, S. Intelligent self-reliant cyber-attacks detection and classification system for IoT communication using deep convolutional neural network. In Proc. 12th Int. Networking Conf., Springer, Cham, 2021, pp. 100–116.

[29] Al-Haija, Q. A. Cost-effective detection system of cross-site scripting attacks using hybrid learning approach. Results in Engineering, 2023, 19, 101266.

[30] Al-Haija, Q. A.; Alohaly, M.; Odeh, A. A lightweight double-stage scheme to identify malicious DNS over HTTPS traffic using a hybrid learning approach. Sensors, 2023, 23(7), 3489.

[31] Özalp, A. N.; Albayrak, Z.; Çakmak, M.; Özdogan, E. Layer-based examination of cyber-attacks in IoT. In Proc. Int. Congr. Human-Computer Interaction, Optimization and Robotic Applications (HORA), 2022, pp. 1–10.

[32] Altunay, H. C.; Albayrak, Z.; Özalp, A. N.; Çakmak, M. Analysis of anomaly detection approaches performed through deep learning methods in SCADA systems. In Proc. 3rd Int. Congr. Human-Computer Interaction, Optimization and Robotic Applications (HORA), 2021, pp. 1–6.

[33] Özdogan, E.; Erdem, O. A.; Özalp, A. N. Adaptive hybrid application protocol for IoT. Acta Polytechnica Hungarica, 2024, 21(2), 271–290.