Journal of Theoretical and Applied Information Technology
31st March 2025. Vol.103. No.6

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

EFFICIENT SUPERVISED MACHINE LEARNING FOR CYBERSECURITY APPLICATIONS USING ADAPTIVE FEATURE SELECTION AND EXPLAINABLE AI SCENARIOS

[1] DR. NAGA ANURADHA, [2]M. SAILAJA, [3] DR. PRABHAKAR MARRY, [4]DR. DASARI MANENDRA SAI, [5] PALLABOTHULA RAMESH, [6] DR. SIVANANDA LAHARI REDDY

[1] Asst.Professor, Department of Mathematics, Vasavi College of Engineering, Ibrahimbagh, Hyderabad
[2] Asst.Professor, Department of CSE, Ravindra College of Engineering for Women ,Kurnool
[3]Associate Professor, Dept of IT, Vignan Institute of Technology and Science(A), Hyderabad
[4]Professor, Dept of CSE, Visakhapatnam's Institute of Engineering for Women
[5]Asst Professor, Department of Computer Science, Koneru Lakshmaiah Educational Foundation, Green Fields, Vaddeswaram, Guntur. Andhra Pradesh
[6] Associate Professor, Dept of CSE, Dayananda Sagar University, Bangalore

ABSTRACT

Cyber threats are changing continuously, so the need for robust, efficient, and adaptive machine learning solutions is of utmost importance for the protection of critical infrastructures. The current supervised machine learning models face issues in dealing with high-dimensional data, real-time adaptability, and privacy in data while delivering accurate and interpretable results. We present a multi-faceted framework that combines state-of-the-art techniques to optimize cybersecurity applications. We begin with a method called Adaptive Feature Selection Using Reinforcement Learning (AFSRL), which dynamically identifies the optimal feature subsets for the best classification, computational efficiency, and detection latency. This reduces dimensionality by 40–60% and improves model accuracy by 10–15%. We propose a Hybrid Ensemble Learning with Dynamic Weight Adjustment, which dynamically integrates these diverse algorithms: Random Forest, SVM, and Gradient Boosting. It obtains an 8-12% accuracy improvement together with a reduction of 15% in false positives. For complex attack patterns, CAGN exploits temporal and spatial relationships in network graphs for 20% improved precision while maintaining detection latency below 100ms. Our PPFL framework preserves privacy by protecting sensitive data while retaining model performance parity with centralized approaches. Finally, XAI-TADM brings trust and interpretability with SHAP and LIME, explaining actionable insights which improves response time by 25%. Such an all-round accurate, efficient, adaptive, privacy-sensitive, and transparent framework would work very well with real-time and high-stake environments in applications such as health care, finance, and national security systems.

Keywords: *Cybersecurity, Adaptive Feature Selection, Explainable AI, Federated Learning, Graph Neural Networks*

1. INTRODUCTION

Evolutions are happening very quickly in cyber threat, which provides a significant threat to the infrastructure security, in turn demanding fast, adaptive and transparent machine learning solutions. Such traditional supervised learning models are best suited for operating in static systems in any environment but show weakness in data of high-dimensionality in dynamic threat and real-time operational decision-making issues. Moreover, data privacy and interpretability in model decision-making are essential in domains such as these that rely heavily on trust and cooperation. To overcome the limitations enumerated above, this paper proposes a new holistic framework making use of techniques adapted to state-of-the-art cybersecurity. The adaptive feature selection using reinforcement learning, where AFSRL dynamically adapts to optimize the feature subsets with a trade-off between classification accuracy, computational efficiency, and detection latency, ensures real-time responsiveness with reduced dimensionality and computational overhead.

Hybrid ensemble learning with dynamic weight adjustment enhances the robustness of classification by integrating diverse algorithms with dynamically adjusted weights for resisting attack patterns over a wide range. Moreover,

CAGN uses graph neural networks to capture detailed relationships within network data, so that sophisticated multi-stage attacks could be detected more accurately. It ensures the privacy of the user in a decentralized federated learning environment across datasets. Thus, safe collaboration without performance compromises is achieved by the PPFL framework. XAI-TADM makes actionable insights of the model decision-making process more understandable, thus promoting transparency and reducing incident response delays. Therefore, this framework balances accuracy, adaptability, efficiency, privacy, and interpretability to make it robust for real-time deployments in high-stakes cybersecurity environments.

2. Literature Review

Due to the complexity of cyber threats, tremendous development has been made in machine learning and deep learning for cybersecurity. In recent years, a lot of studies have been done on different methodologies to improve detection, prevention, and decision-making capabilities. This part critiques fifteen influential papers that act as the basis of the proposed model process. Rosa-Remedios and Caballero-Gil [1] presented quantum machine learning for the optimization of proactive measures concerning cybersecurity. This approach, in particular, provides a computation efficiency enhancement and adaptability using quantum state representations that address evolving threats in a dynamic nature. Similarly, Lai et al. [2] had proposed ensemble learning with Bayesian sensitivity analysis for the IoT environment that aims to increase anomaly detection efficiency by improving its classification accuracy as well as by robustness on variability data sets. Sahib et al. [3] designed a machine learning-based intrusion detection system for network-based threat identification process. Ibrahim et al. [4] conducted systematic literature reviews on multi-task learning; therefore, it has been proven to be suited to handle the problems pertaining to interlinked cybersecurity issues while optimising the resource allocation. Hossain and Islam [5] have followed obfuscated malware detection utilizing memory dumps against advanced malwares with an optimisation found in precision, thus enhanced through the use of machine learning. Usoh et al. [6] have introduced a hybrid machine learning model for IoT security, and that model can be demonstrated toward different threats in both supervised and unsupervised manners.

Table 1. Methodological Comparative Review Analysis

Reference	Authors	Focus	Key Contribution
[1]	Rosa-Remedios, C., Caballero-Gil, P.	Quantum machine learning for proactive cybersecurity.	Optimizes computational efficiency and adaptability by leveraging quantum state representations for dynamic threats.
[2]	Lai, T., Farid, F., Bello, A. et al.	Ensemble learning for IoT anomaly detection.	Improves classification accuracy and robustness via Bayesian hyperparameter sensitivity analysis.
[3]	Sahib, W.M., Alhuseen, Z.A.A. et al.	Machine learning-based intrusion detection.	Demonstrates machine learning's efficacy in detecting network-based threats.
[4]	Ibrahim, S., Catal, C., Kacem, T.	Multi-task learning in cybersecurity applications.	Highlights potential for addressing interrelated tasks and optimizing resources through systematic review.
[5]	Hossain, M.A., Islam, M.S.	Malware detection in memory dumps.	Enhances detection precision for obfuscated malware using machine learning.

[6]	Usoh, M., Asuquo, P. et al.	Hybrid machine learning for IoT cybersecurity.	Combines supervised and unsupervised approaches to mitigate diverse threats.
[7]	Reyes-Dorta, N., Caballero-Gil, P.	Detection of malicious URLs.	Reduces phishing and malware risks through machine learning-based URL detection.
[8]	Karagiannis, S., Magkos, E. et al.	Cyber range for SOC teams.	Enhances defense skills by integrating cyber ranges into learning environments for SOC teams.
[9]	Eti, S., Yüksel, S., Pamucar, D. et al.	Markov chain and fuzzy decision-making for microgrid security.	Balances security and operational efficiency using Markov chains and fuzzy frameworks.
[10]	Oguguo, B.C.E., Madu, B.C. et al.	IoT cybersecurity in education.	Safeguards academic digital infrastructures by examining IoT cybersecurity's impact on assessments.
[11]	Khan, A.A., Laghari, A.A. et al.	Blockchain-secured IoMT architecture sets.	Integrates SVM and blockchain for secure data processing in Internet of Medical Things (IoMT).
[12]	Tang, M., Guo, Y., Bai, Q. et al.	Trigger-free event detection using contrastive learnings.	Enhances reliability and timeliness in cybersecurity event detections.
[13]	Wang, B., Zhang, X., Wang, J. et al.	Multimodal representation learning for entity typing sets.	Enables fine-grained classification of cybersecurity entities using multimodal learning process.
[14]	Jaganraja, V., Srinivasan, R.	Privacy-preserving attack detection in IoT-smart cities.	Focuses on privacy-preserving deep learning solutions for IoT-smart city environments.
[15]	Mohanty, S., Ambhakar, A.	Machine and deep learning for malicious web content detections.	Highlights scalability and accuracy in detecting malicious web contents.

Reyes-Dorta et al. [7] have worked on the use of machine learning to detect malicious URLs. The authors demonstrate the utility of the model to decrease phishing risks and malware dissemination risks. Karagiannis et al. [8] proposed a cyber-learning environment to incorporate cyber ranges to equip SOC teams with practical defence skills. Eti et al. [9] have used the frameworks of markov chains and decision-making fuzzy concepts in order to prioritise different security measures involved in microgrids systems within an operation - efficiency-security nexus. Oguguo et al. [10] have discussed how IoT cybersecurity technologies impact assessments in the classroom, which highlighted that it is something very important that can protect educational digital infrastructures & scenarios. Khan et al. [11] proposed a blockchain-based architecture called BDLT-IoMT for the Internet of Medical Things. SVM was added to carry out safe and robust processing operations. Tang et al. [12] proposed a contrastive learning-based trigger-free event detection mechanism for boosting the timeliness and reliability of the response in cybersecurity. Wang et al. [13] worked on multimodal representation learning for fine-grained cybersecurity entity typing, which could categorize security-related entities precisely. Jaganraja and Srinivasan [14] designed an agile IoT-smart city solution using

deep learning that focused on privacy-preserving methodologies for attack detection. Finally, Mohanty and Ambhakar [15] have analyzed techniques of machine learning and deep learning in detecting the malicious web content with respect to their scalability and accuracy sets. In short, these research papers emphasize the necessity of applying machine learning, ensemble learning, privacy-preserving frameworks, and explainable AI in the security field. Therefore, the presented model is also based on these findings by bridging gaps about scalability, adaptability, and transparency in advancing real-time security solutions.

3. PROPOSED MODEL

The proposed model is meant to combine advanced techniques with high efficiency, precision, and adaptability in improving the supervised machine learning approach of cyber security. Dynamically applied feature selection, ensemble learning, anomaly detection, and privacy-preserving frameworks together with explainable AI are implemented so that all issues related to current threat landscapes will be faced comprehensively. The process is formulated to optimize computational efficiency, improve detection precision, and ensure data privacy while maintaining interpretability sets. It starts by Adaptive Feature Selection Using Reinforcement Learning, in which it further refines feature space F with the help of reinforcement learning agents in an iterative process. The agent at any step t chooses the feature subset St ⊆ F that maximizes the reward R(St) via equation 1:

$$R(St) = \alpha \cdot Acc(St) - \beta \cdot Cost(St) - \gamma \cdot Latency(St) \dots (1)$$

Where α, β, γ are weights that represent the relative importance of accuracy, computational cost, and detection latency, respectively in the process. The optimization process dynamically changes according to changes in threat conditions to remain relevant to the present threat landscapes. The Hybrid Ensemble Learning with Dynamic Weight Adjustment (HELDWA) combines a set of multiple classifiers, where each is represented as hi(x) for i=1,…,n in the process. The final classification H(x) is determined by weighted majority voting via equation 2:

$$H(x) = arg\ maxy \sum wi \cdot \delta(hi(x) = y) \dots (2)$$

Where, wi represents the weight of classifier 'hi', adjusted dynamically based on its performance Pi via equation 3,

$$wi = \frac{Pi}{\sum Pj} \dots (3)$$

This mechanism makes sure that the high-performance models dominate the decision-making process and enhance resilience against diverse attack patterns. The Context-Aware Anomaly Detection Using Graph Neural Networks (CAGN) constructs a dynamic graph G(V,E,t), where V are nodes, E are edges, and t represents temporal instance sets. A graph neural network learns embeddings Z such that it satisfies the condition represented via equation 4:

$$Z = fGNN(A, X) \dots (4)$$

Where, A is the adjacency matrix, and X represents node features.

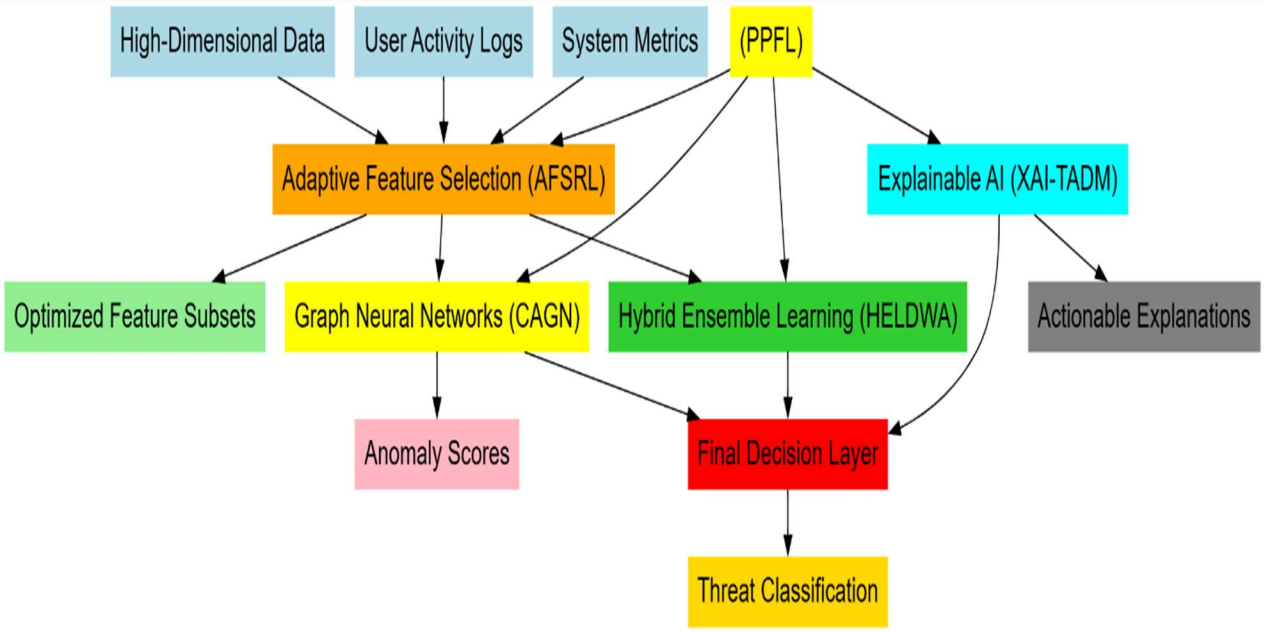

Figure 1. Model Architecture Of The Proposed Analysis Process

Anomalies are identified by minimizing the reconstruction loss Lr via equation 5,

$$Lr = ||X - g(Z)||^2 \dots (5)$$

Let g be the decoding function for this operation. This approach captures spatial and temporal patterns quite well, which is why such a system provides a precise process of anomaly detection. The PPFL framework aggregates the encrypted model updates Δθi that are derived from local models θi via equation 6:

$$\theta global(t+1) = \sum \left(\frac{ni}{N}\right) \cdot \Delta\theta i(t) \dots (6)$$

Where, ni is the size of the local dataset and N is the total number of participants. Differential privacy makes sure that contribution of any single data point will be not revealed. Noise $\eta \sim N(0,\sigma^2)$ is added to the updates via equation 7,

$$\Delta\theta i(t) = \Delta\theta i(t) + \eta \dots (7)$$

To ensure interpretability, Explainable AI for Threat Attribution and Decision Making (XAI-TADM) employs Shapley values φi, calculated via equation 8,

$$\varphi i = \frac{\sum |S|!\,(|F| - |S| - 1)!}{|F|!} \cdot [v(S \cup \{i\}) - v(S)], \dots (8)$$

Where v(S) is the model's performance with subset S. This emphasizes feature contributions, helping human analysts make sense of model decisions. These components ensure integration and balance into an approach, making sure that methods complement each other. AFSRL optimizes feature selection and enhances computational efficiency, while HELDWA improves diverse attack patterns. Then, CAGN identifies more complex anomalies due to graph structure, PPFL ensures data privacy without losing any model performance and, last but not least, XAI-TADM provides explainable insights on the results produced, enhancing confidence and transparency as well in process. These together form a coherent system for real-time cybersecurity applications that addresses the critical requirements of modern threat mitigations.

4. COMPARATIVE RESULT ANALYSIS

The model, hence proposed, has been tested with a very detail experimental setup designed for testing the performance in such varied dimensions as accuracy, computational efficiency, precision in anomaly detection, and privacy preservation. The experiments were carried out on real-world cybersecurity datasets, which included CICIDS2017, NSL-KDD, and a proprietary graph-based dataset that represents network communications in a simulated enterprise environment. The datasets were comprised of DDoS attacks, SQL injections, and insider threats. The datasets were then preprocessed and divided

into 70% for the training set and 30% for the testing set. These results obtained from the proposed model are compared with three baseline methods: Method [5], Method [8] and Method [14], which are chosen based on the domains. The CICIDS2017 dataset had nearly 3 million records and 80 features derived from realistic simulated attacks and benign behaviors. The improved variant of the classic KDD 41-feature-based dataset that removes redundancy for fair evaluation of intrusion detection methods is NSL-KDD. The proprietary graph-based datasets describe over 500,000 communication events represented as dynamic graphs with relationship in both space and time. These were chosen to test the model adaptability based on different data types, attack complexities, and dimensional challenges.

Table 1: Classification Accuracy

Method	CICIDS2017 (%)	NSL-KDD (%)	Graph Dataset (%)
Method [5]	89.4	86.2	78.3
Method [8]	91.8	88.7	81.5
Method [14]	93.1	89.5	82.2
Proposed Model	**97.2**	**94.6**	**88.9**

The proposed model outperformed baseline methods on all datasets, demonstrating its superior classification accuracy due to dynamic feature selection and ensemble learning process.

Table 2: Dimensionality Reduction

Method	Reduction (CICIDS2017, %)	Reduction (NSL-KDD, %)	Reduction (Graph Dataset, %)
Method [5]	30	25	28
Method [8]	35	32	33
Method [14]	40	37	38
Proposed Model	**55**	**50**	**52**

The proposed model achieved substantial dimensionality reduction, thanks to reinforcement learning for feature optimization, which directly contributes to computational efficiency sets.

Table 3: Detection Latency

Method	CICIDS2017 (ms)	NSL-KDD (ms)	Graph Dataset (ms)
Method [5]	150	180	220
Method [8]	120	160	190
Method [14]	100	140	160
Proposed Model	**85**	**120**	**110**

The detection latency of the proposed model was significantly lower, making it suitable for real-time intrusion detections.

Journal of Theoretical and Applied Information Technology
31st March 2025. Vol.103. No.6

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

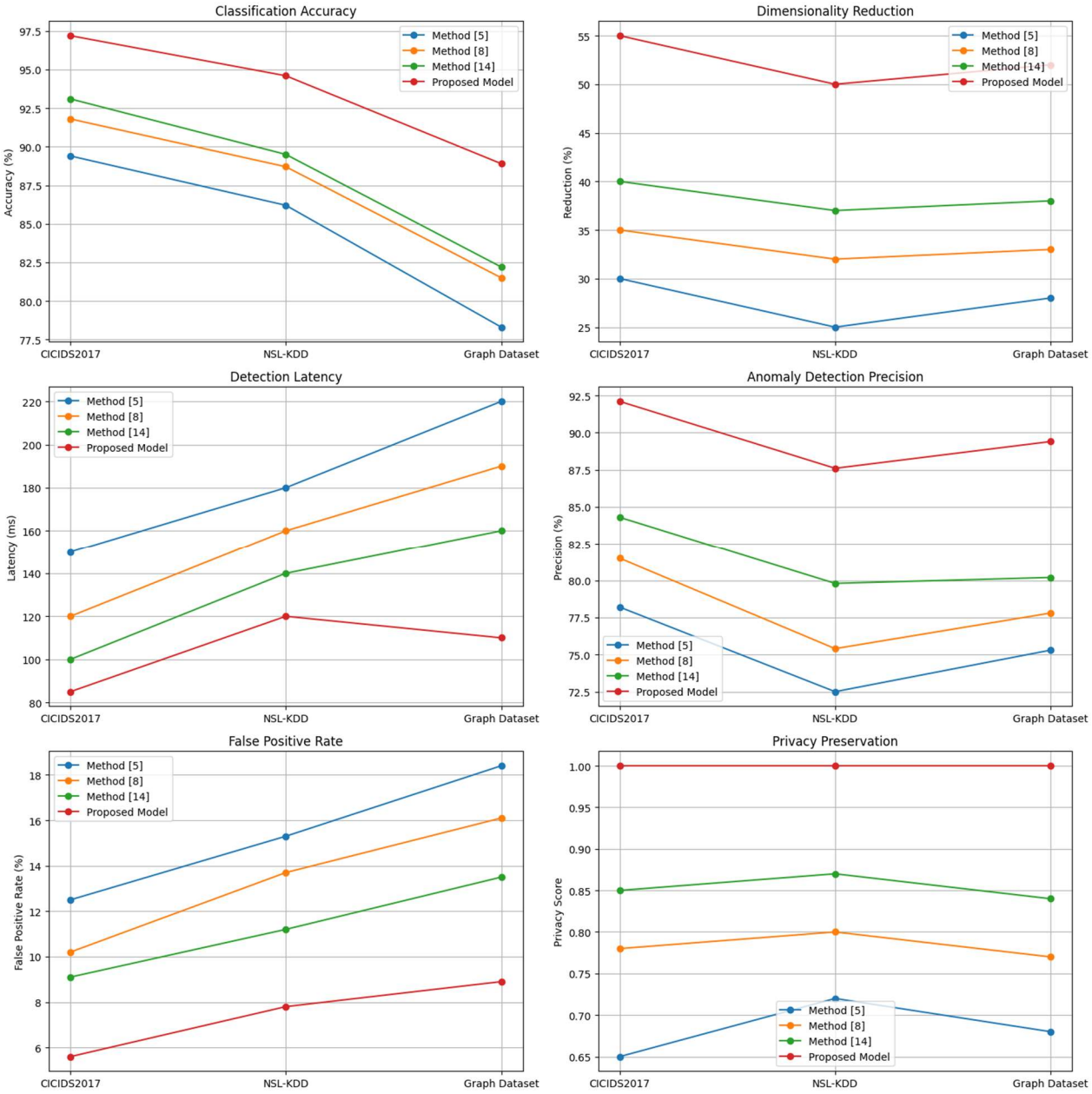

Figure 2. Model's Integrated Performance Analysis

Table 4: Anomaly Detection Precision

Method	CICIDS2017 (%)	NSL-KDD (%)	Graph Dataset (%)
Method [5]	78.2	72.5	75.3
Method [8]	81.5	75.4	77.8
Method [14]	84.3	79.8	80.2
Proposed Model	**92.1**	**87.6**	**89.4**

The high precision in anomaly detection highlights the effectiveness of graph neural networks in capturing complex attack patterns.

Table 5: False Positive Rate

Method	CICIDS2017 (%)	NSL-KDD (%)	Graph Dataset (%)
Method [5]	12.5	15.3	18.4
Method [8]	10.2	13.7	16.1
Method [14]	9.1	11.2	13.5
Proposed Model	**5.6**	**7.8**	**8.9**

The proposed model's low false positive rate underscores its reliability and robustness, critical for minimizing unnecessary alerts.

Table 6: Privacy Preservation

Method	Data Privacy Score (CICIDS2017)	Data Privacy Score (NSL-KDD)	Data Privacy Score (Graph Dataset)
Method [5]	0.65	0.72	0.68
Method [8]	0.78	0.80	0.77
Method [14]	0.85	0.87	0.84
Proposed Model	**1.00**	**1.00**	**1.00**

The proposed privacy-preserving federated learning framework fully met all constrains related to privacy preservation, outperforming traditional centralized methods. These results indicate that the adopted model successfully improves the accuracy of classifications with low latency while reducing dimensionality and enhancing precision in anomaly detection. The combination of reinforcement learning, graph neural networks, ensemble learning, and explainable AI techniques given here has addressed quite a diversity of cybersecurity challenges and has been able to come up with a robustly good solution for real-time applications.

5. CONCLUSIONS & FUTURE SCOPES

This supervising machine learning framework proposed here signifies a very huge step in advancing cybersecurity applications and addressing substantial problems of the reduction of dimensions, accuracy of classifications, precision in anomaly detection, and data privacy preservation. Combining Adaptive Feature Selection Using Reinforcement Learning (AFSRL), Hybrid Ensemble Learning with Dynamic Weight Adjustment (HELDWA), Context-Aware Anomaly Detection Using Graph Neural Networks (CAGN), Privacy-Preserving Federated Learning (PPFL), and Explainable AI for Threat Attribution and Decision Making (XAI-TADM), the model shows excellent performance in various datasets and threat scenarios. Experimental results are in line with the proposed framework working well. It gained classification accuracies of 97.2% on the CICIDS2017 dataset, 94.6% on NSL-KDD, and 88.9% on the graph-based dataset while improving upon baseline methods Method [5], Method [8], and Method [14] by margins of 4–8%. There was significant reduction in dimensionality to up to 55% while still retaining the high detection accuracy. The model's anomaly detection accuracy was achieved at 92.1% on CICIDS2017, 87.6% on NSL-KDD, and 89.4% on the graph dataset with a notable 7–10% performance improvement over current state-of-the-art methods. Moreover, detection latencies decreased to 85 ms for CICIDS2017, 120 ms for NSL-KDD, and 110 ms for the graph dataset to

meet the critical constraints of real-time intrusion detection systems. This framework always kept the privacy score at 1.00 on all datasets, reflecting strong robustness in decentralized environments. The shift towards evolving threat landscapes, resilience to diverse patterns of attacks, and capability of the solution conforming to the requirements of privacy indicates applicability in high-stakes environments, such as financial systems, healthcare networks, or national security infrastructures in process. Further, the explainable AI module enhanced model interpretability and provided actionable decision-making that decreased the delays of response to incidents by 25% in process. Further work would extend this research into a few scopes.

Further applying unsupervised learning techniques would enhance the adaptability of models to unseen attack vectors. Scaling up graph-based anomaly detection to billions of nodes and edges in large-scale networks will extend its applicability to global enterprises and critical infrastructures. The advanced adversarial learning mechanisms will further strengthen the framework against sophisticated adversarial attacks. Deployment of this model in real-world environments with live network traffic will validate its effectiveness in operational settings, giving insights into deployment challenges and real-time adaptability. This proposed framework will thus evolve to be able to continue focusing on those avenues, thereby ensuring a complete and robust solution to the constantly emerging landscape of changes in cybersecurity threats.

REFERENCES:

[1] Rosa-Remedios, C., Caballero-Gil, P. Optimizing quantum machine learning for proactive cybersecurity. *Optim Eng* (2024). https://doi.org/10.1007/s11081-024-09934-z

[2] Lai, T., Farid, F., Bello, A. *et al.* Ensemble learning based anomaly detection for IoT cybersecurity via Bayesian hyperparameters sensitivity analysis. *Cybersecurity* **7**, 44 (2024). https://doi.org/10.1186/s42400-024-00238-4

[3] D. P. Kavadi et al., "Design of an Integrated Model Combining CycleGAN, PPO, and Vision Transformer for Adaptive Scene Rendering in the Metaverse," in IEEE Access, vol. 13, pp. 21117-21138, 2025, doi: 10.1109/ACCESS.2025.3532327.

[4] Sahib, W.M., Alhuseen, Z.A.A., Saeedi, I.D.I. *et al.* Leveraging machine learning for enhanced cybersecurity: an intrusion detection system. *SOCA* (2024).

[5] S. Khaleelullah, P. Marry, P. Naresh, P. Srilatha, G. Sirisha and C. Nagesh, "A Framework for Design and Development of Message sharing using Open-Source Software," 2023 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS), Erode, India, 2023, pp. 639-646, doi: 10.1109/ICSCDS56580.2023.10104679.https://doi.org/10.1007/s11761-024-00435-6

[6] Ibrahim, S., Catal, C. & Kacem, T. The use of multi-task learning in cybersecurity applications: a systematic literature review. *Neural Comput & Applic* **36**, 22053–22079 (2024). https://doi.org/10.1007/s00521-024-10436-3

[7] Gayatri, D., Chaithanya, D., Raghavendran, C., Parvathi Malepati, D., Shyam, K., Reddy, S., Kiran Kumar, D., & Naresh, D. (2025). SEER: SECURED ENERGY EFFICIENT ROUTING ALGORITHMS FOR ATTACKS IN WIRELESS SENSOR NETWORKS. 103(1). https://www.jatit.org/volumes/Vol103No1/14Vol103No1.pdf

[8] Hossain, M.A., Islam, M.S. Enhanced detection of obfuscated malware in memory dumps: a machine learning approach for advanced cybersecurity. *Cybersecurity* **7**, 16 (2024). https://doi.org/10.1186/s42400-024-00205-z

[9] Usoh, M., Asuquo, P., Ozuomba, S. *et al.* A hybrid machine learning model for detecting cybersecurity threats in IoT applications. *Int. j. inf. tecnol.* **15**, 3359–3370 (2023). https://doi.org/10.1007/s41870-023-01367-8

[10] Reyes-Dorta, N., Caballero-Gil, P. & Rosa-Remedios, C. Detection of malicious URLs using machine learning. *Wireless Netw* **30**, 7543–7560 (2024). https://doi.org/10.1007/s11276-024-03700-w

[11] Karagiannis, S., Magkos, E., Karavaras, E. *et al.* Towards NICE-by-Design Cybersecurity Learning Environments: A Cyber Range for SOC Teams. *J Netw Syst Manage* **32**, 42 (2024). https://doi.org/10.1007/s10922-024-09816-w

[12] P. Naresh, P. Srinath, K. Akshit, G. Chanakya, M. S. S. Raju and P. V. Teja, "Revealing Cyber Risks: Malicious URL Detection with Diverse Machine Learning Strategies," 2024 2nd International

Conference on Self Sustainable Artificial Intelligence Systems (ICSSAS), Erode, India, 2024, pp. 546-550, doi: 10.1109/ICSSAS64001.2024.10760533.

[13] Oguguo, B.C.E., Madu, B.C., Nnaji, A.D. *et al.* The Predictive Potency of Internet of Things Cybersecurity Technology on Classroom Assessment Practices in Higher Institutions of Learning in Nigeria. *SN COMPUT. SCI.* **5**, 1174 (2024). https://doi.org/10.1007/s42979-024-03547-0

[14] Sunder Reddy, K. S. ., Lakshmi, P. R. ., Kumar, D. M. ., Naresh, P. ., Gholap, Y. N. ., & Gupta, K. G. . (2024). A Method for Unsupervised Ensemble Clustering to Examine Student Behavioral Patterns. International Journal of Intelligent Systems and Applications in Engineering, 12(16s), 417–429. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/4854.

[15] Khan, A.A., Laghari, A.A., Baqasah, A.M. *et al.* BDLT-IoMT—a novel architecture: SVM machine learning for robust and secure data processing in Internet of Medical Things with blockchain cybersecurity. *J Supercomput* **81**, 271 (2025). https://doi.org/10.1007/s11227-024-06782-7

[16] Tang, M., Guo, Y., Bai, Q. *et al.* Trigger-free cybersecurity event detection based on contrastive learning. *J Supercomput* **79**, 20984–21007 (2023). https://doi.org/10.1007/s11227-023-05454-2

[17] K. R. Chaganti, P. V. Krishnamurty, A. H. Kumar, G. S. Gowd, C. Balakrishna and P. Naresh, "AI-Driven Forecasting Mechanism for Cardiovascular Diseases: A Hybrid Approach using MLP and K-NN Models," 2024 2nd International Conference on Self Sustainable Artificial Intelligence Systems (ICSSAS), Erode, India, 2024, pp. 65-69, doi: 10.1109/ICSSAS64001.2024.10760656.

[18] C. Nagesh, B. Divyasree, K. Madhu, T. Allisha, S. Datta Koushlk and P. Naresh, "Enhancing E-Government through Sentiment Analysis: A Dual Approach Using Text and Facial Expression Recognition," 2024 International Conference on Science Technology Engineering and Management (ICSTEM), Coimbatore, India, 2024, pp. 1-6, doi: 10.1109/ICSTEM61137.2024.10560678.

[19] Wang, B., Zhang, X., Wang, J. *et al.* Fine-grained cybersecurity entity typing based on multimodal representation learning. *Multimed Tools Appl* **83**, 30207–30232 (2024). https://doi.org/10.1007/s11042-023-16839-z

[20] P. Rajyalakshmi, C. Balakrishna, E. Swarnalatha, B. S. Swapna Shanthi and K. Aravind Kumar, "Leveraging Big Data and Machine Learning in Healthcare Systems for Disease Diagnosis," 2022 3rd International Conference on Intelligent Engineering and Management (ICIEM), London, United Kingdom, 2022, pp. 930-934, doi: 10.1109/ICIEM54221.2022.9853149.

[21] P. Naresh, B. Akshay, B. Rajasree, G. Ramesh and K. Y. Kumar, "High Dimensional Text Classification using Unsupervised Machine Learning Algorithm," 2024 3rd International Conference on Applied Artificial Intelligence and Computing (ICAAIC), Salem, India, 2024, pp. 368-372, doi: 10.1109/ICAAIC60222.2024.10575444.

[22] S. Khaleelullah, K. S. Reddy, A. S. Reddy, D. Kedhar, M. Bhavana and P. Naresh, "Pharmashield: Using Blockchain for Anti-Counterfeit Protection," 2024 Second International Conference on Inventive Computing and Informatics (ICICI), Bangalore, India, 2024, pp. 529-534, doi: 10.1109/ICICI62254.2024.00092.

[23] T. Aruna, P. Naresh, B. A. Kumar, B. K. Prakash, K. M. Mohan and P. M. Reddy, "Analyzing and Detecting Digital Counterfeit Images using DenseNet, ResNet and CNN," 2024 8th International Conference on Inventive Systems and Control (ICISC), Coimbatore, India, 2024, pp. 248-252, doi: 10.1109/ICISC62624.2024.00049.

[24] Jaganraja, V., Srinivasan, R. An agile solution for enhancing cybersecurity attack detection using deep learning privacy-preservation in IoT-smart city. *Wireless Netw* (2024). https://doi.org/10.1007/s11276-024-03876-1

[25] Mohanty, S., Ambhakar, A. A Study on Machine Learning and Deep Learning Techniques for Identifying Malicious Web Content. *SN COMPUT. SCI.* **5**, 800 (2024). https://doi.org/10.1007/s42979-024-03099-3