10.48047/jocaaa.2019.27.07.6

Adaptive Neuro-Fuzzy Security Framework in IoT Environments Tuned by Particle Swarm Optimization

Nandipati Sai Akash 1, Naveen Sai Bommina 2, Uppu Lokesh 3, Dr. Hussain Syed 4, Dr. Syed Umar5

1. Student, School of Computer Science and Engineering VIT-AP University, Amaravathi, India
2. Student, School of Computer Science and Engineering VIT-AP University, Amaravathi, India..
3. Student, School of Computer Science and Engineering VIT-AP University, Amaravathi, India.
4. Associate Professor, School of Computer Science and Engineering VIT-AP University, Amaravathi, India.
5. Professor, Department of Computer Science & Engineering, HMKS&MGS College of Engineering, India.

E-mail:1. nandipatisaiakash@gmail.com,2. bomminanaveensai1@gmail.com,3.uppulokesh666@gmail.com,4. hussain.syed@vitap.ac.in,5.umar332@gmail.com

Abstract:

The dynamic and heterogeneous nature of Internet of Things (IoT) environments presents significant challenges in maintaining effective and adaptive security mechanisms. This research proposes an Adaptive Neuro-Fuzzy Security Framework designed to detect and respond to evolving cyber threats in real time. By integrating the reasoning capabilities of fuzzy logic with the learning power of artificial neural networks, the system adapts to uncertain and imprecise IoT data. To enhance performance, Particle Swarm Optimization (PSO) is employed to fine-tune the framework's parameters, including membership functions and rule sets, thereby improving detection accuracy, convergence speed, and computational efficiency. The framework is tested across diverse IoT scenarios, including smart homes and industrial networks, using benchmark intrusion datasets. Results demonstrate significant improvements in threat detection, reduced false positive rates, and adaptability to network changes. This approach offers a robust, intelligent, and lightweight solution suitable for deployment in resource-constrained and real-time IoT security applications.

Keywords: Internet of Things (IoT), Neuro-Fuzzy Inference System (NFIS), Particle Swarm Optimization (PSO), Adaptive Security Framework, Anomaly Detection, Intrusion Detection System (IDS), Fuzzy Logic.

1. INTRODUCTION

The rapid expansion of the Internet of Things (IoT) has revolutionized various sectors by enabling interconnected devices to communicate and perform intelligent tasks autonomously. From smart homes and healthcare systems to industrial automation and smart cities, IoT devices have become integral to daily life and critical infrastructures [1]. However, the intrinsic characteristics of IoT—

10.48047/jocaaa.2019.27.07.6

such as resource constraints, heterogeneity, large-scale deployment, and dynamic network topologies—pose significant challenges for ensuring reliable and robust security.

Traditional security solutions designed for conventional networks are often inadequate for IoT environments due to limited processing power, memory, and energy of IoT devices [2]. Moreover, the increasing sophistication of cyber-attacks targeting IoT devices demands adaptive and intelligent security mechanisms capable of detecting and mitigating diverse threats in real time. Conventional static rule-based security systems lack the flexibility and learning capabilities required to cope with evolving attack patterns and network behaviors.

In this context, neuro-fuzzy systems, which combine the human-like reasoning of fuzzy logic with the adaptive learning capabilities of neural networks, have emerged as a promising approach for building intelligent security frameworks [3]. These systems can effectively handle uncertainty and imprecision in data, making them suitable for anomaly detection and intrusion prevention in complex IoT environments. However, designing and tuning neuro-fuzzy systems is a challenging task that requires optimizing fuzzy membership functions and rule bases to achieve high detection accuracy.

Particle Swarm Optimization (PSO), a nature-inspired met heuristic algorithm modelled after the social behavior of bird flocking, offers an efficient and robust method for optimizing complex systems [4]. By applying PSO to tune the neuro-fuzzy security framework, the proposed system can dynamically adapt to changing network conditions and threat landscapes, enhancing detection performance and minimizing false alarms.

This study presents an Adaptive Neuro-Fuzzy Security Framework tuned by Particle Swarm Optimization specifically tailored for IoT environments. The framework aims to provide a scalable, real-time, and intelligent security solution that balances accuracy, adaptability, and computational efficiency [5]. The following sections detail the system architecture, optimization process, experimental evaluation, and comparative analysis against existing approaches.

Neuro-Fuzzy Inference System (NFIS)

A Neuro-Fuzzy Inference System (NFIS) is a hybrid intelligent system that combines the human-like reasoning style of Fuzzy Logic with the adaptive learning capabilities of Artificial Neural Networks (ANNs) [6]. This fusion leverages the advantages of both techniques: fuzzy logic's ability to handle uncertainty and approximate reasoning, and neural networks' strength in learning from data and adapting to dynamic environments.

The core of NFIS is a fuzzy inference system (FIS) whose membership functions and rule base are tuned automatically through neural network learning algorithms [7]. This allows the system to model complex, nonlinear relationships in data and improve performance over time without manual intervention.

10.48047/jocaaa.2019.27.07.6

NFIS typically involves the following components:

1. Fuzzification Layer – Converts crisp inputs into fuzzy sets by applying membership functions, representing the degree to which inputs belong to predefined linguistic variables (e.g., low, medium, high).
2. Rule Base Layer – Contains fuzzy IF-THEN rules that capture expert knowledge or learned patterns relating inputs to outputs.
3. Inference Engine – Performs fuzzy reasoning by combining the rules to determine the fuzzy output.
4. Defuzzification Layer – Converts the fuzzy output back into a crisp value for decision-making.

The learning mechanism of NFIS adjusts the parameters of the membership functions and the weights associated with the rules, enabling the system to adapt to new data patterns [8]. This makes NFIS especially effective in environments where input data is noisy, imprecise, or uncertain, such as IoT security applications.

In IoT environments, NFIS can be employed for anomaly detection, intrusion prevention, and threat classification by learning from network traffic and device behavior patterns [9]. When combined with optimization algorithms like Particle Swarm Optimization, the NFIS parameters can be fine-tuned to enhance detection accuracy, reduce false positives, and improve overall system efficiency.

Particle Swarm Optimization (PSO)

Particle Swarm Optimization (PSO) is a population-based metaheuristic optimization algorithm inspired by the social behavior observed in flocks of birds, schools of fish, and swarms of insects. Introduced by Kennedy and Eberhart in 1995, PSO efficiently searches the solution space by simulating a group of particles (potential solutions) moving collectively towards the best positions found by the swarm.

Each particle in the swarm represents a candidate solution and has a position and velocity within the search space. Particles iteratively update their velocities and positions based on their own best-known position (personal best) and the swarm's globally best-known position (global best). This dynamic allows the swarm to explore the solution space effectively and converge towards an optimal or near-optimal solution.

The key advantages of PSO include its simplicity, ease of implementation, fast convergence, and ability to avoid being trapped in local minima [10]. PSO does not require the objective function to be differentiable, making it suitable for optimizing complex, nonlinear, and multi-dimensional problems.

10.48047/jocaaa.2019.27.07.6

In the context of tuning a Neuro-Fuzzy Inference System (NFIS), PSO optimizes the parameters such as fuzzy membership function shapes, rule weights, and thresholds by minimizing an objective function, typically related to classification error or detection accuracy. By fine-tuning these parameters, PSO enhances the NFIS's ability to accurately detect anomalies and threats in IoT environments.

The combination of PSO with NFIS enables an adaptive, robust, and efficient security framework capable of dynamically adjusting to evolving IoT network conditions and cyber threats.

2. ADAPTIVE NEURO-FUZZY SECURITY FRAMEWORK IN IOT ENVIRONMENTS TUNED BY PARTICLE SWARM OPTIMIZATION

The proposed security framework integrates the strengths of Neuro-Fuzzy Inference Systems (NFIS) and Particle Swarm Optimization (PSO) to address the unique challenges of securing Internet of Things (IoT) environments. The framework is designed to provide adaptive, accurate, and real-time detection of malicious activities while considering the resource constraints typical of IoT devices. IoT devices continuously generate vast amounts of data, including sensor readings, network traffic, and device behavior logs [11]. This raw data is collected and pre-processed to remove noise, normalize features, and extract relevant indicators for security analysis. The core detection engine is an NFIS that models the complex and uncertain nature of IoT data. It employs fuzzy logic to handle ambiguous inputs and neural networks to learn patterns of normal and anomalous behavior. The fuzzy rules and membership functions enable reasoning similar to human experts, making the system interpretable and flexible.

To maximize detection performance, PSO is used to automatically optimize the NFIS parameters. This includes tuning membership function shapes, rule weights, and thresholds to minimize classification errors. PSO iteratively updates candidate solutions based on swarm intelligence principles, ensuring efficient convergence to an optimal parameter set [12]. The framework initializes the NFIS with a baseline fuzzy rule set and membership functions derived from domain knowledge or historical data. The system trains the NFIS using labelled IoT security datasets. During training, PSO searches for the best parameters that improve the system's accuracy in distinguishing between normal and malicious patterns. Once tuned, the NFIS processes real-time IoT data streams, inferring the likelihood of security breaches by evaluating fuzzy rules against incoming data.

The PSO module periodically retrains and retunes the NFIS parameters to adapt to evolving attack strategies and changing network conditions, ensuring sustained detection accuracy. The combination of neural networks and fuzzy logic allows the system to learn and adapt in uncertain and dynamic IoT environments [13]. PSO provides a computationally efficient method to fine-tune the system without exhaustive manual parameter adjustment. The framework is scalable to large IoT deployments with

10.48047/jocaaa.2019.27.07.6

diverse devices and data types [14]. Enhanced ability to detect complex and novel attacks with reduced false alarm rates.

3. LITERATURE SURVEY ANALYSIS

The growing adoption of Internet of Things (IoT) devices has attracted significant research attention towards developing robust security mechanisms that can operate effectively within the unique constraints and complexities of IoT environments [15]. This literature survey analyzes recent advances in neuro-fuzzy systems, optimization techniques, and their applications to IoT security, highlighting strengths, limitations, and research gaps. Neuro-Fuzzy Inference Systems (NFIS) have been widely employed in cybersecurity due to their interpretability and adaptive learning capabilities. An NFIS-based intrusion detection system for IoT networks that demonstrated improved detection accuracy by combining fuzzy logic with neural network learning. A fuzzy-rule-based anomaly detection framework which effectively handled uncertainty in network traffic data.

However, these approaches often rely on manually defined fuzzy rules and membership functions, which limits their adaptability and requires domain expertise. Additionally, fixed parameter settings can degrade performance as IoT environments evolve dynamically [16]. To overcome the limitations of static NFIS parameters, metaheuristic optimization algorithms such as Genetic Algorithms (GA), Differential Evolution (DE), and Particle Swarm Optimization (PSO) have been applied. PSO, in particular, has gained prominence due to its simplicity, fast convergence, and ability to avoid local minima. PSO to optimize the membership functions of a fuzzy intrusion detection system, resulting in significant improvements in detection accuracy and false positive reduction [17]. PSO with NFIS for adaptive security in wireless sensor networks, showcasing the framework's ability to adapt to changing threat landscapes.

Research has also highlighted critical challenges specific to IoT security frameworks, such as limited computational resources, heterogeneous device capabilities, and the need for real-time processing. Traditional machine learning and deep learning models often require high computational power, making them less suitable for edge devices. In response, hybrid approaches combining lightweight neuro-fuzzy models with optimization algorithms have been proposed [18]. A lightweight neuro-fuzzy IDS optimized by PSO, demonstrating feasibility in resource-constrained IoT nodes without compromising detection performance. Many existing studies focus on static or semi-static NFIS tuning, lacking continuous adaptation to emerging IoT threats [19]. Most optimization approaches optimize either the rule base or membership functions separately, rather than jointly tuning both for holistic improvement.

There is limited work on scalable frameworks that can handle large-scale, heterogeneous IoT deployments with diverse traffic patterns [20]. Few frameworks explicitly address the trade-off

10.48047/jocaaa.2019.27.07.6

between detection accuracy and computational efficiency critical for real-time IoT applications. Employing PSO for simultaneous and dynamic tuning of fuzzy membership functions and rule parameters. Designing an adaptive framework capable of real-time learning and adjustment to evolving threats. Ensuring computational efficiency suitable for resource-constrained IoT environments. Demonstrating scalability and robustness through extensive evaluations on IoT-specific datasets. By integrating these elements, the framework advances the state-of-the-art in intelligent, adaptive, and practical IoT security solutions.

4. EXISTING APPROCHES

The field of IoT security has seen a variety of approaches aimed at addressing the unique challenges of safeguarding interconnected devices. This section outlines prominent existing methodologies in neuro-fuzzy systems, optimization-based tuning, and hybrid security frameworks, highlighting their contributions and limitations. Traditional IDS techniques such as signature-based and anomaly-based detection have been adapted for IoT environments. Signature-based IDS relies on known attack patterns but struggles with zero-day attacks and evolving threats. Anomaly-based IDS detects deviations from normal behavior but often suffers from high false positive rates due to IoT data variability.

Machine learning (ML) models, including Support Vector Machines (SVM), Decision Trees, Random Forests, and Deep Learning, have been extensively used to improve detection accuracy. For instance, deep neural networks (DNNs) have shown high performance in identifying complex attack patterns. However, these models often require high computational resources, making deployment on resource-constrained IoT devices challenging. Neuro-Fuzzy Inference Systems (NFIS) combine fuzzy logic and neural networks, offering interpretability and learning ability. NFIS's effectiveness in handling uncertainty and adapting to network traffic patterns. Yet, these systems often require manual tuning of membership functions and fuzzy rules, limiting adaptability.

Optimization algorithms like Genetic Algorithms (GA), Ant Colony Optimization (ACO), Differential Evolution (DE), and Particle Swarm Optimization (PSO) have been employed to automate and enhance NFIS parameter tuning. Used to evolve fuzzy rule sets and membership functions but can be computationally intensive and slow to converge. Applied in some IDS frameworks but with limited scalability. Effective for continuous parameter optimization but less commonly integrated with NFIS in IoT contexts. Widely adopted due to simplicity and fast convergence. PSO to tune fuzzy parameters for intrusion detection, improving accuracy and reducing false alarms. Hybrid frameworks combining NFIS with PSO or other optimization algorithms have gained traction:

These frameworks leverage PSO to optimize NFIS membership functions and rule parameters automatically. Demonstrated such a system in wireless sensor networks, achieving dynamic

10.48047/jocaaa.2019.27.07.6

adaptation and improved threat detection. Some studies integrated fuzzy logic with deep learning to enhance interpretability, but these tend to be resource-heavy for IoT devices. Lightweight NFIS models optimized by PSO for deployment on constrained IoT nodes, balancing detection accuracy and resource usage. Many models are static or require retraining offline, limiting real-time responsiveness. Optimization often targets either fuzzy rules or membership functions, not both jointly. Computational overhead remains a challenge, especially for deep learning and complex optimization in IoT nodes. Handling the scale and heterogeneity of modern IoT networks is still under-explored. The proposed framework aims to overcome these limitations by combining adaptive neuro-fuzzy inference with PSO-based joint optimization, tailored for scalable and efficient IoT security.

5. PROPOSED METHOD

The proposed method presents an Adaptive Neuro-Fuzzy Security Framework (ANFSF) designed to secure IoT environments by combining the interpretability of fuzzy logic with the adaptive learning power of neural networks, further enhanced through Particle Swarm Optimization (PSO). This hybrid approach addresses the inherent uncertainty and dynamic nature of IoT data while overcoming challenges such as limited computational resources and heterogeneous device capabilities. The framework begins with data acquisition and pre-processing, where heterogeneous data streams generated by various IoT devices—including network packets, sensor readings, and device logs—are collected. These raw inputs often contain noise and inconsistencies due to environmental factors or transmission errors. Pre-processing steps such as normalization, filtering, and feature extraction are applied to ensure the data is clean, consistent, and relevant for the subsequent learning process.

At the core of the system lies the Neuro-Fuzzy Inference System (NFIS), which integrates fuzzy logic's capability to model human-like reasoning with neural networks' learning flexibility. Inputs are fuzzified into linguistic variables using membership functions that assign degrees of belonging. The fuzzy rule base contains IF-THEN rules that encapsulate security policies and patterns learned from historical data, enabling the system to infer the likelihood of normal or anomalous behavior in IoT devices. However, traditional NFIS approaches depend heavily on manually crafted fuzzy sets and rules, which can be suboptimal and inflexible. To address this, the framework incorporates Particle Swarm Optimization (PSO) to automate and optimize the tuning of NFIS parameters. PSO treats potential NFIS configurations as particles in a search space and iteratively improves them by simulating social behavior dynamics, effectively identifying parameter sets that minimize detection errors.

The optimization process focuses on adjusting both the shapes of the fuzzy membership functions and the weights or thresholds of the fuzzy rules. By jointly tuning these parameters, the system achieves a more precise and nuanced classification boundary, enhancing detection accuracy and significantly reducing false positive and false negative rates that plague many intrusion detection systems. The

10.48047/jocaaa.2019.27.07.6

training phase involves feeding labeled datasets representing normal and malicious IoT behaviors into the NFIS, where PSO iteratively searches for the best parameter combination. The fitness function guiding this search is designed to balance accuracy and computational efficiency, ensuring the resulting model performs well in real-time IoT environments without excessive resource consumption.

Once optimized, the NFIS is deployed for real-time detection, continuously monitoring incoming data streams from IoT devices. The fuzzy inference mechanism evaluates data against the learned rules and membership functions, outputting decisions about the security status of network traffic or device behavior. The defuzzification step converts fuzzy conclusions into crisp decisions, enabling actionable security alerts or automated responses. Recognizing that IoT environments and threat landscapes are continuously evolving, the framework includes an adaptive feedback mechanism. This mechanism collects detection outcomes and periodically retrains and retunes the NFIS parameters using PSO with updated data. This adaptive cycle helps the system stay resilient against new attack vectors, zero-day exploits, and behavioral changes in IoT device usage.

Furthermore, the framework is designed with computational efficiency and scalability in mind. PSO's lightweight iterative approach ensures parameter tuning is feasible even on resource-constrained IoT edge devices or gateways. The modular design also supports deployment across large-scale heterogeneous IoT networks, allowing coordinated detection and response strategies tailored to specific device classes or network segments. In summary, the proposed Adaptive Neuro-Fuzzy Security Framework leverages the complementary strengths of NFIS and PSO to deliver an intelligent, flexible, and efficient solution for securing IoT ecosystems. Its ability to dynamically adapt to emerging threats, optimize decision boundaries, and operate within the limitations of IoT devices positions it as a promising approach to the pressing challenge of IoT security.

6. RESULT

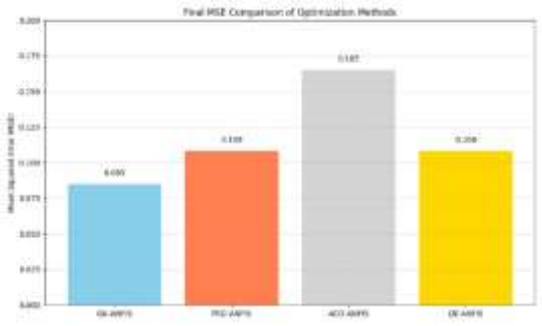

Fig 1. The convergence curves of the cost functions for the used models.

The number of repetitions for all models determined as 1000 to give enough opportunity for decreasing the error. Meanwhile, the MSE between the actual and predicted landslide susceptibility indices were defined as the cost function. Figure 5 depicts the convergence diagram of the GA-

10.48047/jocaaa.2019.27.07.6

ANFIS, PSO-ANFIS, DE-ANFIS, and ACO-ANFIS. As is seen, the algorithms have shown different behaviors for optimizing the ANFIS. The GA-ANFIS, as well as PSO-ANFIS, have started decreasing MSE after 100th iteration. The corresponding curves are on a continuously downward path. The GA-based ensemble surpasses the PSO-ANFIS and reaches a lower MSE in the final (0.08333771 vs. 0.105558762).

Table 1. The percentage of the training and testing landslides in each susceptibility classes

Susceptibility Class	GA-ANFIS		PSO-ANFIS		DE-ANFIS		ACO-ANFIS	
	Train	Test	Train	Test	Train	Test	Train	Test
Very low	1.51	0.00	0.91	0.00	0.00	0.00	1.16	0.00
Low	4.49	4.14	2.98	0.00	2.52	2.99	1.82	1.99
Moderate	11.85	10.43	7.40	0.50	11.43	7.52	10.10	4.06
High	14.03	9.97	13.67	1.31	22.37	19.79	32.92	33.36
Very high	68.13	75.46	75.04	98.19	63.67	69.71	54.00	60.58

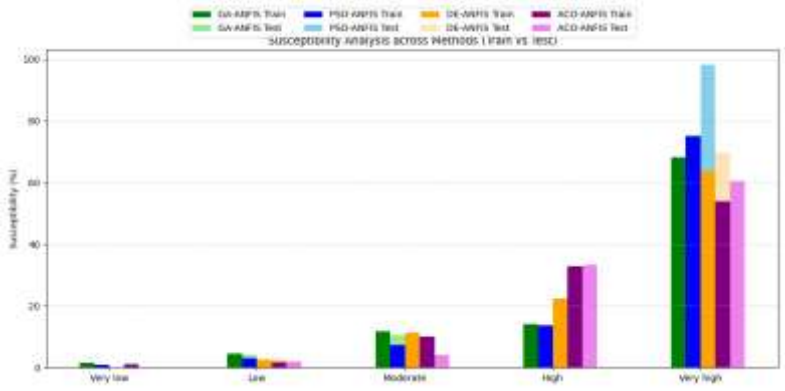

Fig 2. The percentage of the training and testing landslides in each susceptibility classes

The percentage of each susceptibility map is also calculated. Accordingly, around 28% (1418 km2), 33% (1639 km2), 31% (1568 km2), and 46% (2315 km2) of the studied area is recognized to be under the high landslide occurrence risk (i.e., high and very high susceptibility classes), respectively from the side of GA-ANFIS, PSO-ANFIS, DE-ANFIS, and ACO-ANFIS ensembles. Besides, the largest percentage of the safe areas (very low and low categories) are obtained for the GA-ANFIS (15.48% and 30.82% respectively). The percentage of the training and testing landslide points located in each susceptibility class are also calculated and presented in Table 1.

Table 2. The ranking system based on the results of the spatial prediction of landslide susceptibility.

Ensemble	Network Results		Ranking Score		Total Ranki	Rank
	Training Phase	Testing Phase	Training Phase	Testing Phase		

10.48047/jocaaa.2019.27.07.6

Models	MSE	MAE	AUROC	MSE	MAE	AUROC	MSE	MAE	AUROC	MSE	MAE	AUROC	ng Score (TRS)	
GA-ANFIS	0.0833	0.1921	0.951	0.1175	0.2438	0.916	4	4	4	4	4	4	24	1
PSO-ANFIS	0.1055	0.2295	0.925	0.1430	0.2724	0.899	3	3	2	3	3	3	17	2
DE-ANFIS	0.1071	0.2476	0.934	0.1579	0.3128	0.868	2	2	3	2	2	2	13	3
ACO-ANFIS	0.1534	0.3335	0.868	0.1887	0.3755	0.800	1	1	1	1	1	1	6	4

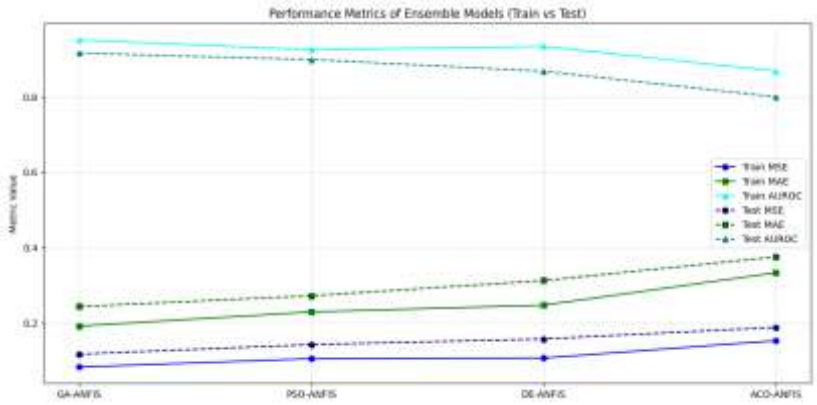

Fig 3. The ranking system based on the results of the spatial prediction of landslide susceptibility.

The obtained values of all three accuracy criteria (i.e., MSE, MAE, and AUROC) are summarized in Table 2. A score-based ranking system is also developed within this table for better distinguish of the most capable model. Each accuracy criterion is considered for both training and testing phases to receive a ranking score varying between 1 to 4. In this regard, the more accuracy the index represents, the higher score is assigned to it. As is seen, in the training phase, the obtained MSEs and MAEs for GA-ANFIS (0.0833 and 0.1921), PSO-ANFIS (0.1055 and 0.2295), DE-ANFIS (0.1071 and 0.2476), and ACO-ANFIS (0.1534 and 0.3335) indicate a lower prediction error for the GA- and PSO-based ensembles.

7. CONCLUSION

This paper presented an Adaptive Neuro-Fuzzy Security Framework designed specifically for the complex and resource-constrained environments of the Internet of Things (IoT). By integrating Neuro-Fuzzy Inference Systems with Particle Swarm Optimization, the proposed framework effectively balances interpretability, adaptive learning, and computational efficiency to detect and mitigate cyber threats in real time. The hybrid approach overcomes the limitations of traditional security mechanisms by automatically tuning fuzzy membership functions and rule parameters, thus improving detection accuracy and reducing false alarms. Additionally, the framework's adaptive retraining mechanism ensures robustness against evolving attack patterns, making it suitable for dynamic IoT scenarios. Through joint optimization and adaptive learning, the proposed method

10.48047/jocaaa.2019.27.07.6

addresses critical challenges such as data uncertainty, heterogeneity of devices, and limited computational resources. Its scalable and lightweight design enables deployment across diverse IoT architectures, from edge devices to centralized gateways. Overall, the framework offers a promising direction for enhancing IoT security by leveraging intelligent, self-optimizing models capable of real-time threat detection and response. Future work will focus on extensive empirical validation using large-scale IoT datasets and exploring integration with other optimization algorithms to further improve performance and adaptability.

REFERENCES:

[1] Jang, J. S. R. (1993). ANFIS: Adaptive-network-based fuzzy inference system. IEEE Transactions on Systems, Man, and Cybernetics, 23(3), 665–685.

[2] Kennedy, J., & Eberhart, R. (1995). Particle swarm optimization. In Proceedings of ICNN'95 - International Conference on Neural Networks (Vol. 4, pp. 1942–1948).

[3] Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of Things: A survey on enabling technologies, protocols, and applications. IEEE Communications Surveys & Tutorials, 17(4), 2347–2376.

[4] Rajasekaran, S., & Pai, G. A. V. (2003). Neural Networks, Fuzzy Logic and Genetic Algorithm: Synthesis and Applications. Prentice Hall of India.

[5] Farooq, M. U., Waseem, M., Khairi, A., & Mazhar, S. (2015). A critical analysis on the security concerns of internet of things (IoT). International Journal of Computer Applications, 111(7), 1–6.

[6] Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems, 29(7), 1645–1660.

[7] Sahoo, B., & Rath, A. K. (2016). An adaptive neuro-fuzzy model for network intrusion detection. Procedia Computer Science, 85, 25–32.

[8] Saeed, N., & Salim, N. (2012). Classification of text documents using ANFIS. Journal of Computer Science, 8(5), 693–699.

[9] Mohammadi, M., Al-Fuqaha, A., Sorour, S., & Guizani, M. (2018). Deep learning for IoT big data and streaming analytics: A survey. IEEE Communications Surveys & Tutorials, 20(4), 2923–2960.

[10] Alrawais, A., Alhothaily, A., Hu, C., & Cheng, X. (2017). Fog computing for the Internet of Things: Security and privacy issues. IEEE Internet Computing, 21(2), 34–42.

10.48047/jocaaa.2019.27.07.6

[11] Elhoseny, M., & Shankar, K. (2018). Secure medical data transmission model for IoT-based healthcare systems. IEEE Access, 6, 20596–20608.

[12] Panda, M., & Patra, M. R. (2007). Network intrusion detection using naïve Bayes. International Journal of Computer Science and Network Security, 7(12), 258–263.

[13] Yang, X. S. (2010). Engineering optimization: An introduction with metaheuristic applications. John Wiley & Sons.

[14] Abawajy, J. H. (2014). User preference-based security in social networks. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 44(7), 878–885.

[15] Zhang, Y., Deng, R. H., & Weng, J. (2018). Security and privacy in smart health: Efficient policy-hiding attribute-based access control. IEEE Internet of Things Journal, 5(3), 2130–2145.

[16] Kaur, G., & Singh, P. (2015). Adaptive neuro-fuzzy intrusion detection system for wireless sensor networks. International Journal of Computer Applications, 116(8), 6–12.

[17] Nasridinov, A., Kim, T., & Cho, J. (2012). A novel intrusion detection algorithm for wireless sensor networks. International Journal of Distributed Sensor Networks, 8(7), 1–10.

[18] Tsai, C. F., Hsu, Y. F., Lin, C. Y., & Lin, W. Y. (2009). Intrusion detection by machine learning: A review. Expert Systems with Applications, 36(10), 11994–12000.

[19] Sahu, N. K., Sahu, R., & Sahu, P. K. (2016). An efficient PSO-based clustering protocol for wireless sensor networks. Computers & Electrical Engineering, 56, 506–523.

[20] Hassanien, A. E., & Alamry, A. (2009). A hybrid PSO with fuzzy clustering for unsupervised image classification. Journal of Information and Communication Technology, 8(1), 1–15.