An IDS-based Adaptive Neural Fuzzy Inference System (ANFIS) for IoBT Security Utilizing Particle Swarm Optimization

Basmh Alkanjr
Department of Computer Science, College of Computer and Information Science, Jouf University, Sakaka, Saudi Arabia
bikhinjar@ju.edu.sa (corresponding author)

Thamer Alshammari
Department of Computer Engineering and Networks, College of Computer and Information Science, Jouf University, Sakaka, Saudi Arabia
tsshammari@ju.edu.sa

Afrah Alanazi
Department of Information System, College of Computer and Information Science, Jouf University, Sakaka, Saudi Arabia
aoalenzy@ju.edu.sa

Easa Alalwany
Department of Computer Science, College of Computer Science and Engineering, Taibah University, Yanbu, Saudi Arabia
ealwani@taibahu.edu.sa

Received: 9 March 2025 | Revised: 5 April 2025 | Accepted: 23 April 2025

 DOI: https://doi.org/10.48084/etasr.10852

ABSTRACT

Within the domain of cybersecurity, Intrusion Detection Systems (IDSs) are crucial to protecting network infrastructures from hostile actions. This paper presents a novel approach that leverages Particle Swarm Optimization (PSO) for feature selection to enhance the performance of an Adaptive Neuro-Fuzzy Inference System (ANFIS)-based IDS. The PSO algorithm identifies the most significant features of a dataset, reducing dimensionality and computational complexity. Subsequently, the selected features are utilized by the ANFIS model to detect and classify intrusions with greater accuracy and efficiency. The proposed PSO-ANFIS framework outperforms traditional methods in terms of detection accuracy and false positive rate, as evidenced by experimental results. The combination of PSO for feature selection with ANFIS for intrusion detection offers a solution to cybersecurity issues, especially in dynamic and intricate systems such as the Internet of Battlefield Things (IoBT).

Keywords-fuzzy logic; machine learning; neural fuzzy inference system; particle swarm optimization; intrusion detection system; internet of battlefield things

I. INTRODUCTION

The rapid advancement of IoT technology has revolutionized various sectors, including healthcare, transportation, and military operations. In particular, the Internet of Battlefield Things (IoBT) is critical to applying IoT to military environments. Connecting devices and sensors improves understanding of the current situation on the battlefield, helps to make decisions, and makes operations more productive. However, the growth of IoBT also brings security risks, as these networks are highly susceptible to cyberattacks, including Distributed Denial of Service (DDoS) [1], data leaks, and malicious intrusions. Therefore, ensuring the security and integrity of IoBT networks is crucial to keep operations running effectively and protect sensitive military data [2].

IDS systems are essential to protect IoBT networks, as they monitor network traffic and detect suspicious activities that might indicate cyberattacks. Traditional IDS methods often need help dealing with the dynamic and heterogeneous nature

of IoBT environments. To address these challenges, adaptive and intelligent IDS solutions are required. An approach that shows promise is ANFIS, as it combines the learning ability of neural networks with fuzzy logic's ability to handle uncertainty and imprecision. ANFIS combines the strength of neural networks and fuzzy logic to build a solid and flexible IDS. Neural networks are great at learning from data and identifying complex patterns. Fuzzy logic offers a structured approach to making decisions in situations of ambiguity. By combining these two methods, ANFIS can analyze network traffic data and accurately detect anomalies. Moreover, it allows it to continuously update its knowledge base, making it well-suited for the ever-evolving threat landscape of IoBT [3, 4].

Feature selection, which determines the crucial dataset features required for accurate detection, is a crucial step in building an efficient IDS. This study uses Particle Swarm Optimization (PSO) for feature selection, which is inspired by nature, mimicking the social behavior of bird flocks or schools of fish. Using the movement and intelligence of individual particles within the swarm iteratively improves a potential solution. PSO's capacity to effectively search the search space and identify optimal feature subsets that improve detection accuracy makes it a good fit for feature selection [5]. Combining ANFIS with PSO for feature selection forms a powerful and adaptable IDS framework for IoBT security. ANFIS utilizes its neural-fuzzy architecture to analyze network traffic and detect anomalies. PSO enhances the feature selection process, ensuring the utilization of the most essential features for detection and improving the overall performance and accuracy of the system. Several studies have shown the efficacy of ANFIS and related methods in diverse security applications. ANFIS has been effectively used to detect Distributed Denial of Service (DDoS) attacks, detect and identify malicious network intrusions, and monitor abnormal activity in IoT networks [6-8]. These studies emphasize the ability of ANFIS to offer a solid and flexible IDS solution for the IoBT environment. Moreover, the application of PSO for feature selection has been shown to improve the effectiveness of IDSs by increasing detection accuracy and decreasing the occurrence of false positives [5, 9].

In [6], ANFIS was used in an IDS for the MQTT protocol, achieving a 93% F1-score with a False Positive Rate (FPR) of 0.1-0.3%, successfully detecting and preventing DoS attacks. This IDS was suitable for resource-constrained IoBT environments due to its high True Positive Rate (TPR), which showed considerable gains in detection rates and computational efficiency using InfoGain for feature selection to improve the model's performance by lowering complexity and enhancing detection accuracy. In [10], a combination of fuzzy logic and game theory was used to develop a hybrid IDS for IoT devices with low resources. Combining classic and hybrid IDS techniques decreased FPR and increased accuracy. By balancing detection performance and resource utilization, this system successfully identified abnormal activity in low-constrained IoBT devices. Combining fuzzy logic with game theory demonstrated the advantages of both fields, leading to improved accuracy and recall rates. Although the feature selection method was not described, the overall improvement in IDS performance was due to the mix of techniques.

In [7], an anomaly-based IDS utilizing ANFIS obtained a TPR of 91.1% and an FPR of 0.006%. By using the InfoGain feature selection technique, this system improved the fuzzy inference process, resulting in a substantial increase in its efficacy in identifying DDoS attacks. This study highlighted the ability of ANFIS to generate intrusion detection results that are more easily comprehensible and readable. The high F1-score indicates that ANFIS has well-balanced precision and recall capabilities [7]. Researchers have increasingly turned to hybrid approaches to make IDSs more adaptive and accurate. For instance, in [11], ANFIS was shown to be able to effectively detect malicious network behavior by learning complex, nonlinear patterns. Researchers have also explored smarter ways to select the most relevant features from large datasets. A notable example is the use of a hybrid technique that combined Cuckoo Search with PSO, which was applied to the CICIoT2023 dataset and significantly improved detection performance [12]. All these studies reflect a growing interest in blending optimization techniques with machine learning to build IDS frameworks that are not only powerful but also lightweight and flexible, traits especially valuable in dynamic and resource-constrained environments such as the IoBT.

Collectively, these studies emphasize the efficacy of applying ANFIS in IDSs to improve detection accuracy, precision, and recall while reducing false positives. Incorporating ANFIS with other methods, such as game theory and signature-based detection, has offered robust and adaptable IDS solutions. These solutions can effectively address the current limitations of IoBT networks, ensuring robust and effective security measures to protect IoBT infrastructures against ever more complex cyber threats. Continuous progress in this domain is essential to develop more robust and effective security systems that protect IoBT networks. Table I shows a comparison between the results of this study and relevant ones. Combining ANFIS with PSO for feature selection is a promising method to improve IoBT security. This adaptive and intelligent IDS framework offers reliable and accurate anomaly detection using neural networks, fuzzy logic, and nature-inspired optimization. The proposed method employs a continuous learning and adaptation process to successfully protect IoBT networks from various cyberattacks, ensuring the security and integrity of critical military operations.

A. Motivation

The absence of a lightweight, secure system makes defense organizations vulnerable to adversaries. Therefore, there is an urgent need in this area to provide a strong defense mechanism, which should, in particular, focus on the confidentiality, availability, and integrity of sensitive data transmitted between the military equipment essential to complete the mission and make decisions accordingly. To our knowledge, developing an IDS for the IoBT environment has yet to be fully investigated. In addition, the fact that none of the proposed systems in other environments are entirely ideal offered an inspiration to build a secure and effective IDS based on neural fuzzy logic to detect abnormal traffic in such a sensitive environment. This work aimed to address these issues and integrate these methods into the IoBT framework.

TABLE I. COMPARISON OF THIS AND RELATED WORKS

Metric	[6]	[10]	[7]	This work
Accuracy	95%	Improved	91.1%	98%
F10score	93%	-	-	98.8%
Precision	94%	Improved	-	1
Recall	92%	Enhanced	91.1%	97.6%
FPR	0.1-0.37%	Reduced	0.006%	0.004%
TPR	High	Improved	91.1%	97.8%
FSM	InfoGain	-	InfoGain	PSO

II. COMPARISON OF FEATURE SELECTION METHODS IN IDS

The process of selecting the most relevant features is a very crucial step for an IDS. This process helps improve performance and enhance detection accuracy since it reduces the dimensionality. A comparison of three common feature selection methods is presented below.

A. InfoGain

InfoGain is a method to calculate the entropy reduction from the transformation of a dataset. It also evaluates the gain of each feature in relation to the target. This allows this method to extract the most relevant features that can be used for classification tasks [13].

1) Advantages

- Relevance: Effectively identifies the most relevant features, improving model interpretability and performance.
- Efficiency: It is suitable for large datasets since it is computationally efficient.
- Ease of Use: It is easy to implement.

2) Disadvantages

- Bias: Could be biased towards features with more categories or higher variability, potentially overlooking important features with lower variance.
- Redundancy: It does not account for feature redundancy, which might result in selecting multiple correlated features.

B. Principal Component Analysis (PCA)

PCA is a statistical method that transforms the original features into orthogonal ones. The orthogonal features are structured in a way to get the largest amount of variation present in the dataset [14].

1) Advantages

- Dimensionality Reduction: Decreases the dimensionality of the features while preserving the majority of the variability present in the data.
- Noise Reduction: By focusing on the principal components, PCA can help reduce noise in the data.
- Uncorrelated Features: The resulting principal components are uncorrelated, which can improve the performance of some machine learning algorithms.

2) Disadvantages

- Interpretability: The interpretation of new features could be a challenge since principal components are formed by linearly combining the original characteristics.
- Linear Assumption: Relies on the assumption of linear correlations between features, which may not adequately reflect intricate interactions within the data.

3) Impact on IDS

The dimensionality and noise reduction provided by this method improve the effectiveness of IDSs, leading to faster training and better detection performance.

C. Nature-Inspired Algorithms (NIAs)

NIAs are heuristic methods that mimic the collective behaviors of living flocks of creatures [15]. The aim is to find the optimal or near-optimal solutions. The most popular NIAs include the Genetic Algorithm (GA), Particle Swarm Optimization (PSO), and Ant Colony Optimization (ACO).

1) Advantages

- Global Optimization: These algorithms are capable of exploring a large search space to find globally optimal feature subsets.
- Flexibility: They can adapt to different types of data and problem domains.
- Handling Non-linearity: They can capture intricate and non-linear correlations among features.

2) Disadvantages

- Computational Cost: NIAs can be computationally expensive, requiring significant time and resources for convergence.
- Parameter Tuning: NIAs often require careful tuning of parameters, which can be challenging and time-consuming.

3) Impact on IDS

NIAs can improve an IDS since they can find features with complex relationships in the dataset, leading to improved detection accuracy and robustness. However, there is a cost for such an advantage, as NIAs need careful tuning and are computationally expensive compared to other methods. This disadvantage could potentially limit their practical use [10].

III. DATASET DESCRIPTION

The dataset used in this study is described in [2]. It is a comprehensive dataset that includes a variety of DDoS attacks, both common and unique. The reason behind this choice is that this particular dataset contains modern types of DDoS attacks, including SQL Injection Distributed Denial of Service (SIDDoS) and HTTP Flood. To the best of our knowledge, no other dataset contains such attacks. Moreover, many other datasets have duplicate and redundant records, leading to unrealistic results. In terms of the dataset itself, some attack types are shown in Table II and the 27 features are shown in Figure 1. A detailed description of these attacks, starting with those that are uniquely covered by this dataset, follows.

A. Attacks Exclusive in this Dataset

- SIDDoS: This attack entails flooding the target with a substantial quantity of simple IP packets, overwhelming the network infrastructure and causing a DoS. This simplicity makes it challenging for traditional detection systems to distinguish legitimate and malicious traffic.
- HTTP Flood: This attack aims to overwhelm a web server by sending many HTTP requests. Unlike traditional DDoS attacks that use a lot of bandwidth, HTTP flooding can be achieved with lower bandwidth, but still causes significant disruption by draining server resources.

TABLE II. ATTACK TYPES

Attack	Number of records
SIDDOS	6665
HTTP Flood	4110
UDP Flood	201344
Smurf	12590

```
1. SRC_ADD                15. PKT_IN
2. DES_ADD                16. PKT_OUT
3. PKT_ID                 17. PKT_R
4. FROM_NODE              18. PKT_DELAY_NODE
5. TO_NODE                19. PKT_RATE
6. PKT_TYPE               20. BYTE_RATE
7. PKT_SIZE               21. PKT_AVG_SIZE
8. FLAGS                  22. UTILIZATION
9. FID                    23. PKT_DELAY
10. SEQ_NUMBER            24. PKT_SEND_TIME
11. NUMBER_OF_PKT         25. PKT_RESEVED_TIME
12. NUMBER_OF_BYTE        26. FIRST_PKT_SENT
13. NODE_NAME_FROM        27. LAST_PKT_RESEVED
14. NODE_NAME_TO          28. PKT_CLASS
```

Fig. 1. Dataset features.

B. Other Included Attacks

- SYN Flood: This attack exploits the TCP handshake process by sending numerous SYN packets to a target, causing the server to allocate resources for half-open connections, ultimately leading to resource exhaustion [16].
- UDP Flood: This attack sends a large number of UDP packets to random ports on the target machine and overwhelms the system with packet processing tasks [16].
- ICMP Flood (Ping Flood): ICMP flood is the transmission of a significant number of ICMP echo request (ping) packets to a specific destination, overloading the network with ICMP traffic and causing service degradation [17].
- Slowloris: This attack establishes many connections with the target web server and maintains them for as long as possible by delivering incomplete HTTP requests, exhausting server resources [17].
- DNS Amplification: A reflection-based DDoS attack where the attacker employs DNS queries with a falsified source IP address (the victim's IP) to transmit to vulnerable DNS servers, resulting in overwhelming DNS response traffic directed at the victim [16, 18].
- NTP Amplification: This attack, similar to DNS amplification, utilizes Network Time Protocol (NTP) servers to inundate the target with a substantial volume of traffic by employing the victim's IP address in the request [17].
- Smurf Attack: A type of ICMP flood where ICMP packets are sent to the broadcast address of a network using a falsified source IP. This triggers a widespread inundation of responses from all devices on the network, causing the victim to be overwhelmed [19].

This dataset provides a thorough foundation for evaluating and enhancing IDSs, ensuring that they can be rigorously tested against a wide array of DDoS threats.

IV. THE PROPOSED ANFIS-IDS SYSTEM

The structure of the proposed method for the detection of DoS attacks has three steps, as shown in Figure 3.

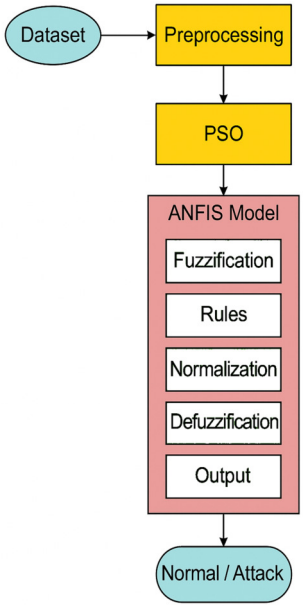

Fig. 2. System architecture.

A. Preprocessing

In the preprocessing step, records with null, missing, and duplicate values were removed. Then the target column PKT_CLASS was divided into two classes: normal and abnormal, converted into binary, where 0 means normal and 1 means abnormal. Finally, the rows were randomly shuffled, with 80% of the preprocessed data used for training, and 20% used for validation.

B. Feature Selection using PSO

The preprocessed data was used to obtain the most important features. Feature selection is a critical preprocessing step required for the efficacy of anomaly detection algorithms [20]. These selected features were used as input for the ANFIS model. This step helps reduce computational cost and improve model performance and detection accuracy. To obtain the most relevant features, PSO was used on the preprocessed dataset. The results are shown in Table III. To simplify the ANFIS, it is important to use a small number of inputs. Choosing 4 inputs

makes ANFIS easier to train and interpret, and faster to process.

TABLE III. SELECTED FEATURES

PKT_RATE
PKT_AVG_SIZE
FIRST_PKT_SENT
LAST_PKT_RECEIVED

C. ANFIS Model

ANFIS is a hybrid system that benefits from the strengths of Fuzzy Inference Systems (FIS) and Artificial Neural Networks (ANN) to provide a powerful tool for capturing the complex relationships in the dataset. ANFIS integrates the neural network's ability to learn from data. The ANFIS model used in this study was based on the Sugeno FIS, having five layers: fuzzification, rule, normalization, defuzzification, and output layers. Each layer contains multiple nodes determined by node functions. The output of each layer is the input of the next layer. Table IV illustrates the mathematical formulation of the ANFIS layers.

TABLE IV. MATHEMATICAL FORMULATION OF ANFIS LAYERS

Layer	Equation	Explanation
Layer 1	$O_1^j = \mu_{B_j}(z)$	O_1^j: Output of node j (fuzzified value). z: Input value to node j. $\mu_{B_j}(z)$: Membership function value for input z in fuzzy set B_j.
Layer 2	$O_2^j = v_j = \mu_{B_j}(z) \cdot \mu_{C_j}(w)$	O_2^j: Firing strength of rule j. v_j: Firing strength. $\mu_{B_j}(z), \mu_{C_j}(w)$: Membership functions for inputs z and w.
Layer 3	$O_3^j = \underline{v_j} = \frac{v_j}{\sum_{k=1}^{m} v_k}$	O_3^j: Normalized firing strength for rule j. $\underline{v_j}$: Firing strength from Layer 2. $\sum_{k=1}^{m} v_k$: Sum of all firing strengths.
Layer 4	$O_4^j = \underline{v_j} \cdot g_j = \underline{v_j} \cdot (a_j z + b_j w + c_j)$	O_4^j: Output of node j. $\underline{v_j}$: Normalized firing strength. g_j: Linear rule output. a_j, b_j, c_j: Parameters to be learned (consequent parameters).
Layer 5	$O_5 = \sum_{j=1}^{m} \underline{v_j} g_j$	O_5: Final output of the ANFIS system. $\underline{v_j}$: Normalized firing strength for rule j. g_j: Rule output.

TABLE V. HYPERPARAMETERS FOR ANFIS AND PSO

Component	Details
Type of FIS	Sugeno
Number of membership functions per input	3
Type of membership functions	Gaussian
Number of epochs (training iterations)	100
Optimization method used	Hybrid
Random seed	42
Number of particles	10
Number of iterations	20
Dataset split	80% training and 20% testing

1) Fuzzification Layer

This layer is important to transform crisp input values into fuzzy values to allow the system to handle uncertainty and approximate reasoning. This step generates Membership Functions (MFs) and linguistic variables for each input. Each node in this layer represents a membership function that determines the degree of association of each input value with the fuzzy set. Each node j in this layer is an adaptive node.

ANFIS can automatically generate linguistic variables, membership functions, and rules. Linguistic variables, which are qualitative descriptors such as "low," "medium," and "high," are generated based on the input data. Membership functions, which define the degree to which input belongs to these linguistic variables, are also automatically initialized and adjusted. In the proposed model, as shown in Figure 3, the ANFIS produced a pair of membership functions for the four input factors (PKT_RATE, PKT_AVG_SIZE, FIRST_PKT_SENT, LAST_PKT_RECEIVED). The fuzzification process results in a set of fuzzy values that represent the degree to which each input belongs to the defined linguistic variables. These fuzzy values are then passed to subsequent layers for further processing.

2) Rule Layer (Layer 2)

The rule layer uses fuzzy inputs to apply fuzzy rules and measure the rule strength for each input. This layer is responsible for applying fuzzy logic rules to the fuzzified inputs that are generated in the previous layer. Each node in this layer performs the multiplication of the signals it receives from the fuzzy layer. The output of each node represents the firing strength of the rule. The rules layer in this ANFIS uses subtractive clustering to automatically generate fuzzy rules by identifying natural groupings in the input data and defining relationships based on those clusters. The two conditional "if-then" statements are as follows:

1. If (PKT_RATE is in1cluster1) and (PKT_AVG_SIZE is in2cluster1) and (FIRST_PKT_SENT is in3cluster1) and (LAST_PKT_RECEIVED in4cluster1) then (PKT_CLASS is out1cluster1) (1)
2. If (PKT_RATE is in1cluster2) and (PKT_AVG_SIZE is in2cluster2) and (FIRST_PKT_SENT is in3cluster2) and (LAST_PKT_RECEIVED is in4cluster2) then (PKT_CLASS is out1cluster2) (1).

3) Normalization Layer (Layer 3)

This layer standardizes the activation levels (firing strengths). It ensures that the firing strengths of the rules are normalized so that their total is increased to one. Each node in this layer divides the firing strength of a rule by the sum of all the firing strengths.

4) Defuzzification Layer (Layer 4)

This layer evaluates the impact of each rule on the final outcome. Each node within this layer handles the result portion of a rule. The output of each node is the result of the normalized firing strength multiplied by a first-order polynomial representing the rule's output.

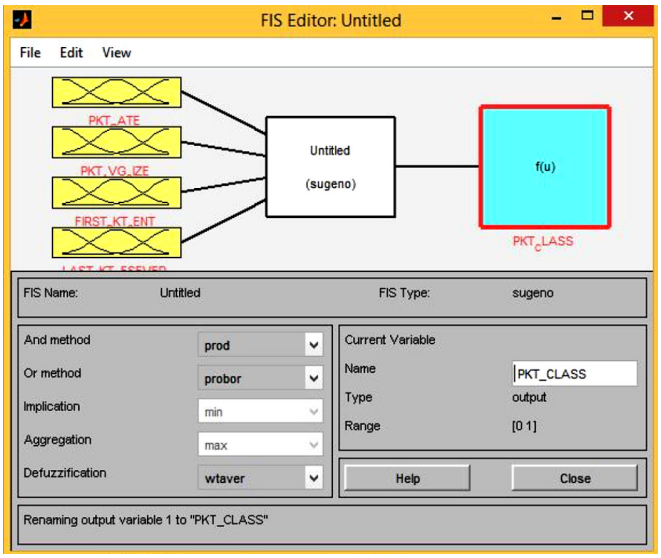

Fig. 3. MFs of the proposed ANFIS.

5) Output Layer (Layer 5)

This layer combines the contributions of each rule to generate the final output. The total output is calculated by the lone node in this layer as the sum of all incoming signals from the defuzzification layer. This sum represents the weighted average of all the rule outputs.

V. EXPERIMENTAL RESULTS

MATLAB's ANFIS Toolbox was used to execute the model and calculate the evaluation metrics. The performance of the ANFIS-trained model was evaluated by examining its accuracy, precision, TPR, FPR, and F1 score by comparing its predictions with the actual values. The evaluation was carried out with and without cross-validation (k=5), as shown in Table VI.

TABLE VI. RESULTS WITH CROSS-VALIDATION K=5 AND WITHOUT

Attack	Cross-validation (k=5)	Without cross-validation
Accuracy	0.98	0.98
TPR	0.97837	0.9781
FPR	0	0
Precision	1	1
F1-score	0.98895	0.98893
Recall	0.97811	0.97810

A. Accuracy

Accuracy is a fundamental metric that indicates the proportion of correct predictions made by the model out of all predictions. Both with and without cross-validation, the ANFIS-trained model achieved an impressive accuracy of 0.98. This high level of accuracy indicates that the model performed consistently well in predicting the correct classes.

B. True Positive Rate (TPR)

TPR, often referred to as recall or sensitivity, quantifies the model's capacity to accurately detect positive instances. With cross-validation, the TPR was slightly higher at 0.97837 compared to 0.9781 without. This marginal improvement indicates that cross-validation helps the model better generalize to unseen data, slightly enhancing its ability to detect true positives. The high TPR in both scenarios reflects the model's effectiveness in identifying the positive class, which is critical in many applications, especially those involving anomaly detection or medical diagnoses, where missing a positive instance could have significant consequences.

C. False Positive Rate (FPR)

FPR quantifies the ratio of negative cases that are mistakenly labeled positive [21]. This result indicates that the model does not produce false positives, which is a highly desirable outcome in classification tasks. A 0.004% FPR demonstrates that the model reduces false alarms, ensuring that most positive predictions are indeed correct.

D. Precision

Precision is the ratio of correctly predicted positive observations to the total predicted positives. It is an essential measurement in situations where the expense of incorrect positive results is significant. In this study, the precision was consistently perfect at 1 in both validation scenarios. This perfect precision score highlights the model's ability to provide reliable positive predictions, ensuring that all identified positive instances are accurate.

E. F1-score

The F1 score is a statistical measure that calculates the harmonic mean of precision and recall [22]. It serves as a unified metric that takes into account both precision and recall, striking a balance between them. With cross-validation, the F1 score was 0.98895, slightly higher than the 0.98893 achieved without it. This slight improvement again underscores the benefits of using cross-validation to enhance the model's generalization ability. A high F1 score in both cases suggests that the model effectively achieves a harmonious equilibrium between accuracy and recall [23], making it suitable for tasks where both false positives and false negatives are important considerations.

The comparative analysis between cross-validation and non-cross-validation scenarios reveals that while both methods yield excellent performance metrics, cross-validation provides marginally better results in terms of TPR and F1 scores. This improvement, although slight, suggests that cross-validation helps the model better capture the underlying patterns in the data, leading to improved generalization. Cross-validation guarantees the model's consistency in performance across diverse subsets of the data, reducing the risk of overfitting and improving its reliability when applied to new, unseen data [23].

VI. CONCLUSION

In the rapidly evolving field of cybersecurity, robust and efficient IDSs are essential to protect networks against increasingly sophisticated threats. This paper presented a novel approach that combines PSO for feature selection with an ANFIS to enhance IDS performance. The proposed system achieved an accuracy of 98%, an FPR of just 0.004%, a precision of 1.0, and an F1 score of 98.8%. The core

contribution of this work is the integration of PSO-based feature selection into the ANFIS framework, specifically designed for IoBT environments. This synergy improves detection accuracy while significantly reducing computational overhead. PSO, inspired by the swarm behavior of birds, effectively identified the most relevant features, reducing dimensionality and complexity. This streamlined data set enabled ANFIS to detect and classify intrusions more accurately and efficiently. The experimental results demonstrated that the PSO-ANFIS model outperformed conventional methods. Feature selection through PSO improved accuracy, reduced FPR, and improved runtime efficiency. These benefits make the proposed framework well-suited for complex and dynamic environments such as the Internet of Battlefield Things (IoBT).

In conclusion, the combination of PSO and ANFIS provides a scalable, accurate, and computationally efficient IDS solution, as it not only enhances detection capabilities but also meets the performance demands of large-scale cybersecurity systems. Compared to previous studies reporting 91-95% accuracy and higher FPRs, this model achieved superior precision and significantly fewer errors. The proposed system has a strong potential for deployment on modern cybersecurity infrastructures. Future work may explore hybridizing this approach with other machine learning models to further strengthen IDS performance in diverse environments.

REFERENCES

[1] W. I. Khedr, A. E. Gouda, and E. R. Mohamed, "P4-HLDMC: A Novel Framework for DDoS and ARP Attack Detection and Mitigation in SD-IoT Networks Using Machine Learning, Stateful P4, and Distributed Multi-Controller Architecture," *Mathematics*, vol. 11, no. 16, Jan. 2023, Art. no. 3552, https://doi.org/10.3390/math11163552.

[2] M. Alkasassbeh, G. Al-Naymat, A. B. Hassanat, and M. Almseidin, "Detecting distributed denial of service attacks using data mining techniques," *International Journal of Advanced Computer Science and Applications*, vol. 7, no. 1, pp. 436-445, 2016.

[3] A. K. Jain, R. P. W. Duin, and J. Mao, "Statistical pattern recognition: a review," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 22, no. 1, pp. 4–37, Jan. 2000, https://doi.org/10.1109/34.824819.

[4] J. S. R. Jang, "ANFIS: adaptive-network-based fuzzy inference system," *IEEE Transactions on Systems, Man, and Cybernetics*, vol. 23, no. 3, pp. 665–685, Feb. 1993, https://doi.org/10.1109/21.256541.

[5] J. Kennedy and R. Eberhart, "Particle swarm optimization," in *Proceedings of ICNN'95 - International Conference on Neural Networks*, Perth, WA, Australia, 1995, vol. 4, pp. 1942–1948, https://doi.org/10.1109/ICNN.1995.488968.

[6] A. P. Haripriya and K. Kulothungan, "Secure-MQTT: an efficient fuzzy logic-based approach to detect DoS attack in MQTT protocol for internet of things," *EURASIP Journal on Wireless Communications and Networking*, vol. 2019, no. 1, Apr. 2019, Art. no. 90, https://doi.org/10.1186/s13638-019-1402-8.

[7] M. Almseidin, J. Al-Sawwa, and M. Alkasassbeh, "Anomaly-based Intrusion Detection System Using Fuzzy Logic," in *2021 International Conference on Information Technology (ICIT)*, Amman, Jordan, Jul. 2021, pp. 290–295, https://doi.org/10.1109/ICIT52682.2021.9491742.

[8] M. Dorigo and T. Stützle, "Ant Colony Optimization: Overview and Recent Advances," in *Handbook of Metaheuristics*, M. Gendreau and J. Y. Potvin, Eds. Springer International Publishing, 2019, pp. 311–351.

[9] D. T. Pham, S. Otri, A. Afify, M. Mahmuddin, and H. Al-Jabbouli, "Data Clustering Using the Bees Algorithm," in *Proceedings of the 40th CIRP International Manufacturing Systems Seminar*, 2007.

[10] S. S. Ambarkar and N. Shekokar, "A Game theory based intrusion detection system for low constrained IoT devices." 2024, https://doi.org/10.21203/rs.3.rs-3975513/v1.

[11] J. Sharma, Sonia, K. Kumar, P. Jain, R. H. C. Alfilh, and H. Alkattan, "Enhancing Intrusion Detection Systems with Adaptive Neuro-Fuzzy Inference Systems," *Mesopotamian Journal of CyberSecurity*, vol. 5, no. 1, pp. 1–10, Jan. 2025, https://doi.org/10.58496/MJCS/2025/001.

[12] H. Q. Gheni, W. K. Oleiwi, Z. Al-Barmani, and M. A. M. Alabdali, "Optimizing Feature Selection for Intrusion Detection: A Hybrid Approach Using Cuckoo Search and Particle Swarm Optimization," *International Journal of Safety and Security Engineering*, vol. 14, no. 6, pp. 1907–1912, Dec. 2024, https://doi.org/10.18280/ijsse.140624.

[13] O. Rehman, H. Zhuang, A. Muhamed Ali, A. Ibrahim, and Z. Li, "Validation of miRNAs as Breast Cancer Biomarkers with a Machine Learning Approach," *Cancers*, vol. 11, no. 3, Mar. 2019, Art. no. 431, https://doi.org/10.3390/cancers11030431.

[14] F. Kherif and A. Latypova, "Principal component analysis," in *Machine Learning*, A. Mechelli and S. Vieira, Eds. Academic Press, 2020, pp. 209–225.

[15] T. Alshammari and I. Mahgoub, "Nature-Inspired Algorithms in Internet of Vehicles: A Survey and Analysis," *IEEE Internet of Things Journal*, vol. 12, no. 6, pp. 6347–6370, Mar. 2025, https://doi.org/10.1109/JIOT.2025.3528872.

[16] K. B. Adedeji, A. M. Abu-Mahfouz, and A. M. Kurien, "DDoS Attack and Detection Methods in Internet-Enabled Networks: Concept, Research Perspectives, and Challenges," *Journal of Sensor and Actuator Networks*, vol. 12, no. 4, Aug. 2023, Art. no. 51, https://doi.org/10.3390/jsan12040051.

[17] K. Singh, P. Singh, and K. Kumar, "Application layer HTTP-GET flood DDoS attacks: Research landscape and challenges," *Computers & Security*, vol. 65, pp. 344–372, Mar. 2017, https://doi.org/10.1016/j.cose.2016.10.005.

[18] M. S. Khan, K. Ferens, and W. Kinsner, "A chaotic measure for cognitive machine classification of distributed denial of service attacks," in *2014 IEEE 13th International Conference on Cognitive Informatics and Cognitive Computing*, London, UK, Aug. 2014, pp. 100–108, https://doi.org/10.1109/ICCI-CC.2014.6921448.

[19] T. H. H. Aldhyani and H. Alkahtani, "Cyber Security for Detecting Distributed Denial of Service Attacks in Agriculture 4.0: Deep Learning Model," *Mathematics*, vol. 11, no. 1, Jan. 2023, Art. no. 233, https://doi.org/10.3390/math11010233.

[20] R. Basfar, M. Y. Dahab, A. M. Ali, F. Eassa, and K. Bajunaied, "Enhanced Intrusion Detection in Software-Defined Networking using Advanced Feature Selection: The EMRMR Approach," *Engineering, Technology & Applied Science Research*, vol. 14, no. 6, pp. 19001–19008, Dec. 2024, https://doi.org/10.48084/etasr.9256.

[21] T. Sharma and S. K. Prasad, "Enhancing cybersecurity in IoT networks: SLSTM-WCO algorithm for anomaly detection," *Peer-to-Peer Networking and Applications*, vol. 17, no. 4, pp. 2237–2258, Jul. 2024, https://doi.org/10.1007/s12083-024-01712-z.

[22] B. Alkanjr and T. Alshammari, "IoBT Intrusion Detection System using Machine Learning," in *2023 IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC)*, Las Vegas, NV, USA, Mar. 2023, pp. 0886–0892, https://doi.org/10.1109/CCWC57344.2023.10099340.

[23] P. Michailidis, I. Michailidis, S. Gkelios, and E. Kosmatopoulos, "Artificial Neural Network Applications for Energy Management in Buildings: Current Trends and Future Directions," *Energies*, vol. 17, no. 3, Jan. 2024, Art. no. 570, https://doi.org/10.3390/en17030570.