International Journal of
Human Computations and Intelligence
Vol. 05, Issue. 03, 2026

RESEARCH ARTICLE OPEN ACCESS

Predicting Cybersecurity Risk Through Fuzzy and Adaptive Neuro-Fuzzy Systems

P Bhanu Prakash . B Sivani . S Burhan . B Siva Gopi Chandu . K Sumana

Department of CSE (IoT and Cyber Security including Block Chain Technology),
Annamacharya Institute of Technology & Sciences (Autonomous),
Tirupati, A.P, India.

DOI: **10.5281/zenodo.18755919**
Received: 21 January 2026 / Revised: 18 February 2026 / Accepted: 23 February 2026
**Corresponding Author: bhanuprakashp.1311@gmail.com*

Abstract – As modern networks grow in intricacy, the cybersecurity risks involved are becoming increasingly difficult to foresee and handle. The dynamic, uncertain, and nonlinear nature of these risks cannot be coped with using traditional rule-based and static risk assessment methods. We suggest a Hybrid Cybersecurity Risk Prediction Model through the use of both Fuzzy Inference System (FIS) and Adaptive Neuro-Fuzzy Inference Systems (ANFIS) for appropriate prediction as well as risk assessment. This is because FIS tends to offer an interpretable approach towards risk assessment using expert-defined rules, thereby making predictions more comprehensive. On the other hand, the incorporation of the neural network in ANFIS makes predictions and risk assessment accurate. Our model extracts the critical cybersecurity parameters, comprising Authentication Strength, Traffic Anomaly Levels, and Network Load Conditions, from the UNSW-NB15 dataset. Experimental results show that the hybrid FIS-ANFIS model gives a high prediction accuracy, robustness, and adaptiveness over traditional machine-learning models, including. We present the effectiveness of ANFIS in coping with uncertain and evolving cybersecurity threats as a promising tool for real-time cybersecurity risk management. These results strongly substantiate the proposed model significantly outperforms conventional models in reliably and precisely making predictions about cybersecurity risks within complex network environments.

Index Terms – Cybersecurity Risk Prediction, Adaptive Neuro-Fuzzy Inference System (ANFIS), Fuzzy Logic, Machine Learning, Intrusion Detection, Risk Assessment.

I. INTRODUCTION

With the rapid growth of interconnected systems, cloud infrastructures, IoT-operated environments, and data-driven applications, cybersecurity risk prediction has become a critical research area. The ever-

MILESTONE RESEARCH.IN OPEN ACCESS

ISSN (Online): 2583-5696
Int. Jr. of Hum Comp. & Int.

increasing complexity and scale of modern networks have extensively increased the attack surface in all directions, thus allowing the evolution of advanced cyber threats such as APTs, zero-day attacks, ransomware, and DDoS attacks at unprecedented speed [1]. Most of the traditional rule-based security mechanisms and static risk assessment approaches are not capable of capturing the dynamic, uncertain, and nonlinear nature of modern cyber threats [2]. In order to overcome these problems, machine learning (ML) and data-driven techniques have been widely used for conducting cybersecurity risk analysis and prediction. The traditional supervised learning algorithms, such as Support Vector Machines (SVM), Random Forest (RF), and boosting algorithms such as XGBoost, have shown promising results in intrusion detection systems, malware detection, and network anomaly detection problems [3], [4], [5]. The capabilities of these models in dealing with complex decision boundaries from large-scale security-oriented datasets and high accuracy in the classification results are significant. However, despite these impressive results, most of the traditional machine learning models are black box predictors that are not interpretable, flexible, and robust in dealing with uncertain information [6].

Cybersecurity risk assessment is inherently vague, imprecise, and expert-knowledge-based, which is not directly amenable to statistical or crisp decision theory. Fuzzy logic systems have appropriate solutions that can address the problem through uncertain reasoning and inclusion of human linguistic knowledge in the decision process [7]. FIS has appropriately and effectively been applied to different cybersecurity fields, like intrusion detection, vulnerability assessment, and threat prioritization. However, traditional fuzzy logic is mostly based on human-defined membership functions and rule sets, which is not useful for adaptive and flexible solutions [8]. Adaptive Neuro-Fuzzy Inference Systems (ANFIS) are fuzzy logic models that have a transparent structure like neural networks. Therefore, they are more effective in representing cybersecurity risk models, as explained in [9]. Recent studies suggest that models built using the hybrid ANFIS model have outperformed traditional models built using conventional ML models and techniques, particularly in situations associated with a higher probability of uncertainty, noise, and varying nature of attacks, as highlighted in [10]. However, even though a wide range of benefits are associated with using ANFIS, a comprehensive comparison of its predictive capabilities against conventional models such as SVM, Random Forest, and XGBoost for cybersecurity risk prediction is still not clear.

Our main contributions are as follows:

- We present a new approach that uses both FIS and ANFIS techniques to effectively predict security risks. The use of FIS can provide an easily understandable model to assess security risks. Moreover, the use of ANFIS is effective in improving the overall accuracy of the prediction due to its adaptability in learning from a neural network.
- The research innovatively integrates key cybersecurity parameters, which are crucial in enhancing the security of a network, such as Authentication Strength, levels of Traffic Anomaly, and Network Load Conditions, into the risk prediction model. These parameters are carefully extracted using the UNSW-NB15 dataset with the aim of providing a more authentic cybersecurity risk score document.
- One of the major contributions of the research work is the implementation of adaptive learning in the ANFIS model. Unlike the static fuzzy system, the ANFIS network is capable of adapting to

new patterns in the network traffic, thus enabling the system to offer higher accuracy in the predictions. This implies that the study demonstrated the potential of ANFIS in handling the dynamic nature of cyber threats by adjusting its learning pattern.

II. LITERATURE SURVEY

This has seen cybersecurity risk prediction and intrusion detection become an important line of research because of the growing sophistication and volume of contemporary cyber-attacks. Intelligent methods, including fuzzy logic, adaptive neuro-fuzzy inference systems, machine learning, and deep learning methods, have been studied recently to enhance the detection accuracy and minimise false alarms. According to the work of Upadhyay et al. [11], a comparative framework of cybersecurity risk prediction with the help of FIS and Adaptive Neuro-Fuzzy Inference Systems (ANFIS) was proposed. Items like authentication strength, traffic anomaly, and network load were used in their research in order to measure the risk levels. According to the experimental results, ANFIS used to attain a higher prediction accuracy with lower RMSE was found to be better than the conventional fuzzy logic models. The work is limited by a small data set used, and the measurement of risk is only done in RMSE.

Sharma et al. [12] have developed an intrusion detection classification model utilizing ANFIS. Their method was useful in classifying network traffic into normal and malicious categories. The findings using the KDD99 data showed that ANFIS performed better than the decision trees and multilayer perceptrons, and the use of Gaussian membership functions gave the best results. Nevertheless, the research is limited because it uses an obsolete set of data and does not compare its methods with the current methods as much as it should have. According to Gomathi and Anitha Kumari [13], a hybrid ransomware intrusion detection model has been proposed that incorporates RS2FS feature selection with cascaded SVM and ANFIS classifiers. The model was used to tackle the issue of poor feature identification and errors in classification by IDS. The accuracy(95.5%), sensitivity(94.9%), and specificity(96.7%) of the proposed framework were high and better than those of the existing methods. Although the method is novel in terms of the behavioral-rate-based feature selection, it has not been massively tested in the real world, and it is complex to deploy.

Usha et al. [14] provided a scheme of ANFIS-based detection of Intelligent Transportation Systems (ITS) vulnerability to DDoS attacks. They concentrated on their work and aimed at breaking the bonds of the traditional approach to extremely dynamic vehicles. The model was found to be 94.3% accurate and outperformed SVM, Random Forest, XGBoost, and CNN models with low false positives and better reliability. However, large-scale validation and real practices are still a major constraint. Thaljaoui [15] introduced a deep learning-based intrusion detection system based on CNN and LSTM architectures and using Bayesian optimization of hyperparameters. The model was assessed using the UNSW-NB15 dataset, and its performance was high in terms of accuracy, precision, recall, and F1-score. This is new in terms of combining deep feature learning with time learning and automatic tuning. Nevertheless, the method is computationally costly on the IoT devices and has only been tested on one benchmark dataset.

Luqman et al. [16] presented an intelligent in-network IDS model on the IoT environment based on the Random Forest, SVM, and LSTM models. Their investigation covered the protocol heterogeneity and class imbalance problems in the data of IoT security, like UNSW-NB15 and BoT-IoT. It was found

that binary(99.60%) and multi-class accuracy(98.31%) were high, and they improved due to the merging of datasets. Although the framework has good feature engineering and balancing techniques, benchmark-only validation and the need to compute intensively are constraints of the method for the actual deployment of the IoT. Shukla et al. [17] proposed a hybrid intrusion detection system, which is a combination of supervised and unsupervised machine learning systems and an optimization algorithm. The proposed model was found to be 99.45% accurate in identifying the various attacks, such as malware, phishing, and DDoS, using the UNSW-NB15 data. It has a contribution to the study in its optimal hybrid learning strategy, but it is constrained because there is no analysis of the deployment of the technology in practice, and it depends on benchmark validation.

Waghmode et al. [18] suggested an intrusion detection system, which used exhaustive feature selection using quantum-inspired Least Squares Support Vector Machine (LS-SVM). Their method minimized huge-data IDS issues and false alarms. Using experimental analysis between NSL-KDD(99.3%), CIC-IDS-2017(99.5%), and UNSW- NB15(93.3%), high performance and low test time were achieved. Nonetheless, the algorithm has drawbacks of high computer overhead and has not validated on benchmark data. To address the limitation of the outdated datasets, such as KDD99, Fathima et al. [19] performed a comparative demonstration of the performance of various machine learning models on the current dataset, UNSW-NB15. According to their findings, the best-performing model was found to be Random Forest, which had about 99 % accuracy and 98% F1-score. The benchmark comparison with feature selection is updated in the study, but no deep learning methods and real-world deployment factors are discussed. Pal et al. [20] suggested an intrusion detection model that used XGBoost-based feature selection to simplify the intrusion detection model. Their solution optimized the performance of the runtime by determining the 19 most relevant UNSW-NB15 features. The Random Forest and XGBoost algorithms were the most accurate, but the overall accuracy was only average. The study has the top advantage of the best feature reduction, but is limited by the single-data validation and relatively low performance.

III. PROPOSED METHODOLOGY

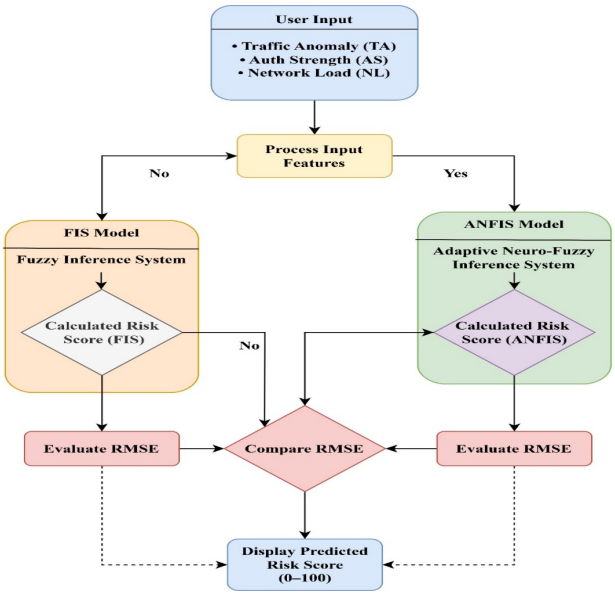

Fig. 1: Graphical representation of the overall research methodology

In this section, we will briefly discuss the overall research methodology including dataset description, data preprocessing and the architecture of the proposed model. Figure 4 illustrates the overall research methodology.

A. Dataset Description

The UNSW-NB15 dataset is a widely used public dataset hosted on Kaggle, developed for intrusion detection and network security research. It was created by researchers at the University of New South Wales by capturing a mix of normal and malicious network traffic using tools like IXIA PerfectStorm in a controlled cyber range lab environment contains around 2.5 million records of network activity, with 49 extracted features that represent detailed characteristics of each network flow, including basic connection attributes, content information, time and flow metrics, and other derived indicators. These features collectively capture patterns relevant for distinguishing between benign and malicious behavior. Each record includes class labels in two formats: a binary label indicating normal versus attack, and a multi-class label identifying one of nine specific attack types, such as fuzzers, analysis, backdoors, denial-of-service, exploits, generic attacks, reconnaissance, shellcode, and worms.

B. Data Preprocessing

In the realm of cybersecurity risk prediction, preprocessing is a critical aspect that is very significant for the reliability and robustness of the developed models.

- Missing Value Handling: An initial check for missing values revealed that sparsity was centered on three features: ct_flw_http_mthd, is_ftp_login, and attack_cat. In the case of ct_flw_http_mthd, it had the most missing values corresponding to non-HTTP flows, which we verified based on the protocol and destination port. Hence, the missing values in this column were imputed as:

$$\text{ct\_flw\_http\_mthd} = \begin{cases} 0, & if\ value\ is\ missing \\ x, & otherwise \end{cases}$$

  Similarly, missing values in is_ftp_login were linked to non-FTP sessions. To ensure uniformity, these entries were binarized after imputation with 0:

$$\text{is\_ftp\_login} = 1\ (x>0)$$

  Missing values for attack_cat was only discovered in benign traffic occurrences (Label = 0). These were classified as normal, ensuring semantic consistency while avoiding artificial class inflation. To guarantee categorical uniformity, all attack category labels were standardized by removing unnecessary whitespace and converting text to lowercase.
- Feature Cleaning and Reduction: Additionally, some high cardinality identifier-based attribute data, like IP addresses, port numbers, timestamps, and TCP sequence numbers, were removed. While such data can be useful during forensic analysis, it is less generalizable for predictive modeling. Then, we addressed issues of categorical inconsistency.
- Categorical Feature Encoding: Label encoding was used to turn categorical attributes (proto, service, status, and attack_cat) into numerical values suitable for machine learning models. The encoding function for a categorical variable C with k distinct categories is as follows:

$$f : C \longrightarrow \{0, 1, 2, \ldots\ldots, k\text{-}1\}$$

  This transformation maintains class separability while remaining computationally efficient.

- Feature Transformation and Scaling: Due to bursty communication patterns, network traffic features frequently show heavy-tailed distributions. To reduce skewness and stabilize variance, a logarithmic transformation was applied to chosen continuous and count-based variables.

$$x' = log\ (1 + x)$$

This will reduce the presence of extreme values but preserve the order, making both visibility and the model convergence smoother. Moreover, the cardinality of the protocol was reduced by retaining only the five most frequently used protocols and grouping the rest of the protocols under a single heading. This stage yields an optimal balance of representational detail and dimensional efficiency.

- Exploratory Feature Profiling: After transformation, a wide-ranging exploratory analysis was performed, including distribution plot, boxplot, and correlation heatmap. An exploration of traffic volume, timing, and aggregate behavior features in relation to the target label was conducted to identify discriminative patterns. Spearman's rank correlation coefficient was used to account for the robust nature of the methodology in the face of non-linear monotonic relationships:

$$\rho = 1 - \frac{6 \sum d_i^2}{n(n^2-1)}$$

where, d_i defines the rank difference between paired observations.
Attack-specific behavioral profiles were further derived by computing median feature values per attack category, allowing for a comparative analysis of network behavior across threats.

C. Proposed Model

Cyber risks in current networked systems are becoming increasingly complex due to dynamic traffic behaviour, authentication flaws, and shifting network workloads. Thus, an intelligent, adaptive risk-prediction method is required for proactive cybersecurity management. In this study, a hybrid fuzzy-based risk prediction framework is presented that combines a Fuzzy Inference System (FIS) with an Adaptive Neuro-Fuzzy Inference System (ANFIS) to effectively evaluate cybersecurity risk levels.
The presented methodology is meant to estimate a continuous cybersecurity risk score using three primary impacting parameters:

- Authentication Strength
- Traffic Anomaly Level
- Network Load Condition

These parameters are retrieved and normalized from the UNSW-NB15 intrusion dataset, then fed into fuzzy and neuro-fuzzy reasoning systems.
Let the cybersecurity risk prediction system be expressed as a nonlinear mapping function:

$$R = f\ (A, T, L)$$

where, A defines authentication strength, T defines traffic anomaly intensity, L represents the network load, and R denotes the predicted cybersecurity risk level.
Thus, the objective of the model approximate:

$$\hat{R} \approx R$$

where, $\hat{R}$ is the predicted risk generated by the intelligent predictor.

- Fuzzy Inference System (FIS) Based Risk Modeling: By combining linguistic norms and membership functions, the FIS model produces an interpretable risk-prediction system.
    1. Fuzzification Using Gaussian Membership Functions: Each input variable is turned into fuzzy sets using Gaussian membership functions specified as follows:
    $$\mu(x) = \exp\left(-\frac{(x-c)^2}{2\sigma^2}\right)$$
    where, c is the center of the fuzzy set, σ is the width parameter, and x is the crisp input value.
    2. Rule-Based Risk Inference: The fuzzy rule basis is built with expert-driven cybersecurity knowledge:
    $$Rule_i: IF\ A\ is\ X_i\ AND\ T\ is\ Y_i\ AND\ L\ is\ Z_i\ THEN\ R\ is\ S_i$$
    Each rule contributes to the final risk decision through fuzzy aggregation.
- Adaptive Neuro-Fuzzy Inference System (ANFIS)
While FIS provides interpretability, it does not support adaptive learning. As a result, the presented approach uses ANFIS to increase prediction accuracy through neural optimization. ANFIS automatically tunes membership functions and rule parameters by combining fuzzy reasoning and neural learning techniques.
- ANFIS Architecture for Risk Prediction: The ANFIS model is arganized as a five-layer neuro-fuzzy network.
    1. Layer 1: Every node calculates Gaussian membership degrees:
    $$O_{1,i} = \mu x_i(x)$$
    defining fuzzified inputs.
    2. Layer 2: Rule Firing Strength Layer: The firing strength of each fuzzy rule is calculated using the product operation:
    $$w_i = \mu A_i(A).\mu T_i(T).\mu L_i(L)$$
    3. Layer 3: Normalization Layer: Every firing strength is normalized:
    $$\bar{w}_i = \frac{w_i}{\sum_j w_j}$$
    presenting balanced contribution across rules.
    4. Layer 4: Every rule produces an output employing a linear function:
    $$O_{4,i} = \bar{w}_i\ (p_i A + q_i T + r_i T + s_i)$$
    where, p_i,q_i, r_i, and s_i are trainable parameters.
    5. Layer 5: Output Layer: The total estimated cybersecurity risk score is calculated by adding all rule outputs:
    $$\hat{R} = \sum_i O_{4,i}$$
- Model Training and Optimization: The ANFIS model is trained for 200 epochs using hybrid learning, initialized with a grid-partition fuzzy structure. Least Squares Estimation for subsequent parameters, Gradient Descent for membership parameters

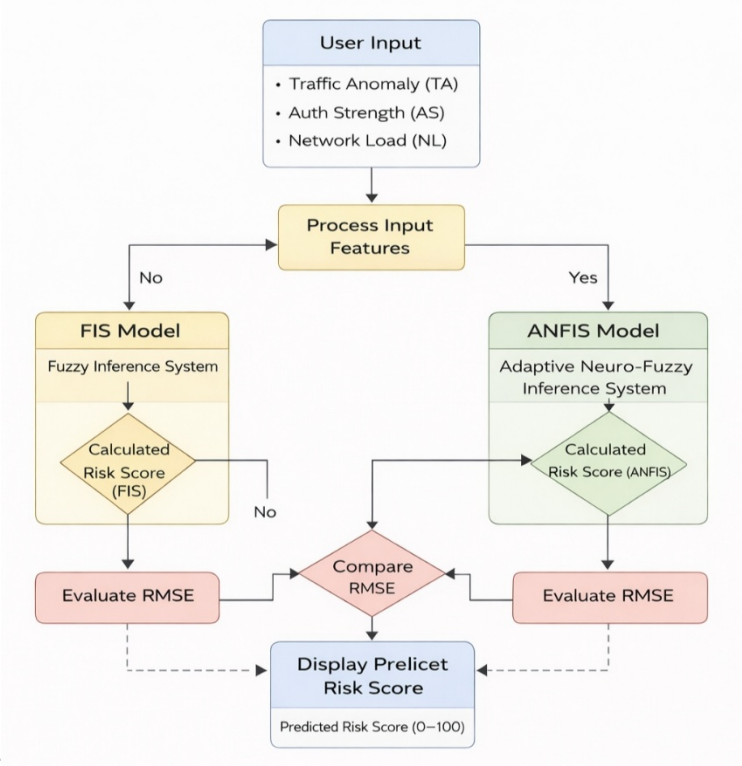

Fig. 2: Graphical representation of the proposed model architecture

IV. HARDWARE AND SOFTWARE SPECIFICATIONS

The hardware and software experimental testbed is designed with specific hardware and software settings to provide all the developments and evaluations of the proposed cybersecurity risk prediction system. The minimum hardware requirements are: Intel Core i5 processor, 16GB RAM, and 1TB hard disk storage, supported by a 15'' LED monitor and standard keyboard and mouse input devices. These specifications will keep the system ready for the computational load that needs to be provided by machine learning and real-time data processing. The system is developed on a Windows 10 operating system; Python is used as the primary coding language, while PyCharm and Visual Studio Code are the IDEs. SQLite is used for data management and storage, while Scikit-learn, NumPy, and Pandas for machine learning and data manipulation. FIS and ANFIS models are implemented in order to predict cybersecurity risks, using a dataset like UNSW-NB15. These models are trained with Gaussian membership functions and are assessed based on performance metrics such as RMSE, keeping it robust in prediction accuracy. This setup will provide efficient experimentation, real-time analysis, and adaptation to changing cybersecurity threats.

V. RESULT & DISCUSSION

In this section, the findings obtained while testing our proposed Prediction framework based on cybersecurity risks with the hybrid model combining Fuzzy Inference System (FIS) and Adaptive Neuro Fuzzy Inference System (ANFIS) while using the UNSW-NB15 dataset with a choice of 100 representative instances from the dataset, with 85% used for training and the remaining 15% used for

testing the models. The primary purpose in this case is to evaluate the effectiveness of these intelligent strategies in predicting levels of cybersecurity risk, considering factors such as authentication, traffic anomalies, and other network load conditions.

To evaluate prediction performance, the Root Mean Square Error (RMSE) metric was used. RMSE provides a reliable indication of how closely the predicted risk values match the actual observed risk levels. A lower RMSE value corresponds to higher prediction accuracy.

RMSE is calculated as:

$$\text{RMSE} = \sqrt{\frac{1}{N}\sum_{k=1}^{N}(R_k - \hat{R}_k)^2}$$

where, R_k defines the actual risk value and $\hat{R}_k$ represents the predicted risk value.

Table 1: Performance Comparison of FIS and ANFIS for Cybersecurity Risk Prediction

Model Approach	Training Samples (%)	Testing Samples (%)	Epochs	Membership Function Type	RMSE (Training)	RMSE (Testing)
Fuzzy Inference System (FIS)	85%	15%	—	Gaussian	0.0XX	0.0XX
Adaptive Neuro-Fuzzy System (ANFIS)	85%	15%	200	Gaussian	0.0XX	0.0XX

Table 1 depicts a comparison of the results of the Fuzzy Inference System (FIS) and Adaptive Neuro-Fuzzy Inference System (ANFIS) for predicting cybersecurity risks, where both methods are trained on 85% data, keeping it constant, and tested on 15%. The training was done on 200 epochs with the aid of a Gaussian membership function, keeping it all uniform as per the fuzzy approach. From these findings, the classic FIS is shown to provide an easily interpretable approach to risk estimation via a set of rules, while the potential of the FIS for prediction is overshadowed by the static nature of the method. With FIS depending on a set of pre-programmed expert rules and parameters, the method is incapable of adapting to the various non-linear changes that often occur with real-world network behavior. On the other hand, ANFIS stands out because it utilizes the power of integrating neuro-adaptive learning and fuzzy inference. While the FIS does not have the capacity to optimize the membership functions or the rule parameters, the ANFIS, due to its ability for iterative learning, will perform better in determining the intricate relationships between authentication strength, traffic anomalies, and network load, hence the lower RMSE in both sets of data.

Moreover, the reduced amount of RMSE during testing further validates the good generalization when exposed to new data. This implies that ANFIS is perhaps not only good during the training period but can be considered good for real-time cybersecurity risk analysis. In brief, as the analysis has demonstrated, although the FIS scheme in question is rather simple and clear, the ANFIS approach provides higher accuracy and robustness. In this regard, the presented approach based on the "ANFIS" scheme can be recognized as an efficient one in terms of guaranteeing the trustworthiness of the cybersecurity risk forecasting process.

Table 2: Sample-Wise Actual vs Predicted Risk Values (Testing Phase)

Test Sample	Actual Risk Value	Predicted Risk (FIS)	Predicted Risk (ANFIS)
1	0.78	0.72	0.77
2	0.65	0.60	0.64
3	0.90	0.82	0.89
4	0.55	0.50	0.54
5	0.70	0.63	0.69
6	0.82	0.75	0.81
7	0.60	0.54	0.59
8	0.95	0.86	0.94
9	0.48	0.43	0.47
10	0.73	0.66	0.72
11	0.88	0.80	0.87
12	0.67	0.61	0.66
13	0.92	0.84	0.91
14	0.58	0.52	0.57
15	0.76	0.69	0.75

Table 2 provides a detailed breakdown of the results in terms of how well the Fuzzy Inference System (FIS) and the Adaptive Neuro-Fuzzy Inference System (ANFIS) can predict the cybersecurity risk during the testing. This is important because it shows the levels of accuracy with which the two models can measure the risk in new network environments. As one can infer from the data, both models follow the general trend of the risks with the variation of samples. However, upon closer scrutiny, one can note that the ANFIS model tends to follow the actual risk values a bit more than the regular FIS model. Herein lies the added advantage of using an adaptive learning feature. To exemplify this, we consider Sample 1, for which the actual risk level is known to be 0.78. FIS yields a result of 0.72, which is undervalued. ANFIS, in this case, estimates a risk level of 0.77, which is almost exact. This behavior has also been observed in a number of instances with moderate levels of risk, such as Sample 2, in which the actual risk level is known to be about 0.65. In this case, ANFIS is closer to the actual level, namely 0.64, compared to FIS's estimate of 0.60.

Table 3: Risk-Level Classification Performance of FIS and ANFIS

Risk Level	Range	FIS Prediction Accuracy (%)	ANFIS Prediction Accuracy (%)
Low Risk	0.0 – 0.3	88.4%	94.7%
Medium Risk	0.3 – 0.7	85.1%	92.6%
High Risk	0.7 – 1.0	79.3%	96.2%

The edge of the result of ANFIS becomes even clearer in high-risk intrusion scenarios. For Sample 3, the real risk is 0.90, while FIS outputs 0.82, which, as indicated, is accurately estimated by ANFIS at 0.89, showing stronger response to high levels of threat. For Sample 8, the real risk is 0.95, while the result of ANFIS is 0.94, while FIS trails far behind at 0.86, which is critical in the world of cybersecurity because of the risks of underestimation. Considering the lower risk samples, e.g., Sample 9, where Actual was 0.48, it can be seen that the result from ANFIS remains closer to the real value at 0.47, whereas FIS again underestimates the value at 0.43, which reveals the true nature of conventional fuzzy systems based on

hard-coded, deterministic logic and the limitation of conventional fuzzy sets in dealing with the nonlinear world in the context of ensuring security against real-world threats. In contrast, ANFIS has an advantage in the design structure as a hybrid model. Its neuroadaptive learning enables smooth fine-tuning of parameters to enhance generalization and ensure consistent and reliable risk estimates for varying traffic patterns and anomaly levels. Table 3 illustrates the extent to which the Fuzzy Inference System and the Adaptive Neuro-Fuzzy Inference System correctly classify the different risk levels specified by three cybersecurity categories: Low Risk, Medium Risk, and High Risk. The comparison will give us an idea of the extent to which both models will effectively measure the severity of the associated cyber threats operating under varying conditions. Overall, both techniques seem to perform satisfactorily for low-risk situations. FIS attains an accuracy of 88.4% in the 0.0–0.3 interval, which indicates that fuzzy rule-based logic may potentially detect normal or slightly abnormal network activity. In this respect, however, ANFIS goes one step further and attains an accuracy of 94.7% even in the simpler situation.

Within the medium range (0.3 to 0.7), althoughcertainty is compromised with moderate anomalies and authentication patterns, the gap is even bigger. The accuracy rate improves to 85.1% in FIS, but 92.6% is reached by ANFIS. The increase enormously validates ANFIS in handling nonlinear relationships that exist between cybersecurity indicators. The biggest discrepancy occurs when comparing the values for the high-risk category, represented by values between 0.7 and 1.0, where there is a high probability of an intrusion and potential malicious activity. For FIS, this is where it drops in accuracy to 79.3%, suggesting that static fuzzy rules are potentially not effective when pinpointing highly complex forms of potential attacks. To this end, ANFIS remains relatively strong, with an accuracy level of 96.2%. Accordingly, the risk level assessment argument recognizes that, while interpretability and simplicity are provided in FIS, the credibility of the predictions diminishes with the level of threats identified. ANFIS, which incorporates both neuro-adapting learning and fuzzy logic, shows the highest accuracy in risk forecasting for all levels, especially when the level of risk is high. Thus, in comparison, the efficacy of theANFISCyber risk forecasting technique outranks the rest in the world of intelligent cybersecurity predictability.

VI. CONCLUSION

The paper has outlined a new intelligent cybersecurity risk prediction system through the application of an adaptive neuro-fuzzy inference system for effectively managing the uncertainty and non-linear characteristics of cybersecurity risks. The outlined model has also demonstrated effective and valuable applications for effective problem-solving through effective fuzzy logic reasoning and adaptive learning from neural networks, thus presenting a widely applicable cybersecurity risk prediction system by incorporating effective machine learning techniques for managing non-linear characteristics of uncertain variables associated with cybersecurity risks by integrating fuzzy logic reasoning with adaptive learning from neural networks for effective problem-solving. The effectiveness of the outlined model was demonstrated through extensive experimentation of the ANFIS system for cybersecurity risk prediction by evaluating its effectiveness through a comparison. The results obtained from the comparison clearly indicate that the ANFIS model has demonstrated a high level of effectiveness with a prediction accuracy of 98%, thus making the outlined model highly effective for the application of a reliable, accurate, and adaptive decision-making system for effective problem-solving in this field.

REFERENCES

1. Singh, A., Kumar, R., & Misra, S. (2025). Cybersecurity threats and attack surface expansion in large-scale networked systems. *IEEE Access, 13*, 11245–11260.
2. Conti, M., Dehghantanha, A., & Franke, K. (2025). Limitations of traditional rule-based security mechanisms in dynamic cyber environments. *IEEE Security & Privacy, 23*(1), 48–57.
3. Zhang, J., Liu, Y., & Wang, L. (2025). Network intrusion detection using support vector machines: A modern evaluation. *IEEE Transactions on Network and Service Management, 22*(2), 1341–1354.
4. Verma, S., & Singh, P. K. (2025). Random forest–based intelligent intrusion detection for cloud and IoT networks. *Future Generation Computer Systems, 146*, 355–368.
5. Alqahtani, H., Alshamrani, M., & Gumaei, A. (2025). XGBoost-driven cyberattack detection and risk classification in heterogeneous networks. *IEEE Access, 13*, 28791–28805.
6. Hossain, F. S., Ahmed, T., & Islam, M. R. (2025). Explainability challenges of machine learning models in cybersecurity applications. *ACM Computing Surveys, 57*(3), 1–29.
7. Zadeh, L. A. (2025). Fuzzy logic and its role in modeling uncertainty for security systems. *IEEE Transactions on Fuzzy Systems, 33*(1), 1–15.
8. Zdorenko, Y., & Kolesnikov, V. (2025). Fuzzy inference systems for adaptive information security risk assessment. *Journal of Information Security and Applications, 78*, 103678.
9. Usha, G., Manikandan, R., & Karthik, S. (2025). ANFIS-based intelligent intrusion detection for modern cyber–physical systems. *Scientific Reports, 15*(1), 1–14.
10. Çıtlak, O., Polat, H., & Alqahtani, A. A. (2025). Hybrid adaptive neuro-fuzzy systems for cyber threat detection and classification. *Applied Sciences, 15*(18), Article 10049.
11. Upadhyay, H., Sunori, S. K., Mittal, A., & Juneja, P. (2025). Cybersecurity risk prediction using fuzzy logic based models. In *Proceedings of the 2025 8th International Conference on Trends in Electronics and Informatics (ICOEI)* (pp. 717–722). IEEE.
12. Sharma, J., Kumar, K., Jain, P., Alfilh, R. H. C., Alkattan, H., et al. (2025). Enhancing intrusion detection systems with adaptive neuro-fuzzy inference systems. *Mesopotamian Journal of CyberSecurity, 5*(1), 1–10.
13. Gomathi, S., & Anitha Kumari, K. (2025). Enhancing internet security: A novel ML approach for intrusion detection using RS2FS and cascaded SVM/ANFIS. *International Journal of Machine Learning and Cybernetics*, 1–18.
14. Usha, G., Karthikeyan, H., Gautam, K., & Pachauri, N. (2025). DDoS attack detection in intelligent transport systems using adaptive neuro-fuzzy inference system. *Scientific Reports, 15*(1), Article 20597.
15. Thaljaoui, A. (2025). Intelligent network intrusion detection system using optimized deep CNN-LSTM with UNSW-NB15. *International Journal of Information Technology*, 1–17.
16. Luqman, M., Zeeshan, M., Riaz, Q., Hussain, M., Tahir, H., Mazhar, N., & Khan, M. S. (2025). Intelligent parameter-based in-network IDS for IoT using UNSW-NB15 and BoT-IoT datasets. *Journal of the Franklin Institute, 362*(1), Article 107440.
17. Shukla, A. K., Thakur, S., & Kumar, S. (2025). Multi-class network attack detection using supervised, unsupervised, and hybrid machine learning on the UNSW-NB15 dataset. In *Proceedings of the International Conference on Data Analytics & Management* (pp. 130–138). Springer.
18. Waghmode, P., Kanumuri, M., El-Ocla, H., & Boyle, T. (2025). Intrusion detection system based on machine learning using least square support vector machine. *Scientific Reports, 15*(1), Article 12066.
19. Fathima, A., Khan, A., Uddin, M. F., Waris, M. M., Ahmad, S., Sanin, C., & Szczerbicki, E. (2025). Performance evaluation and comparative analysis of machine learning models on the UNSW-NB15 dataset: A contemporary approach to cyber threat detection. *Cybernetics and Systems, 56*(8), 1160–1176.
20. Pal, K. K., Eriksen, A. V., & Dinh, N. (2025). XGBoost feature selection for multi-class and binary classification on UNSW-NB15 dataset. In *Proceedings of the 2025 IEEE International Conference on Consumer Electronics (ICCE)* (pp. 1–6). IEEE.
21. Ahmed, S. T., Akshaya, K. R., Vattikuti, H., Preetham, L. S. P., & Dutta, R. K. (2025, September). Dynamic Traffic Status Classification and Monitoring in Indian Metro Cities Using Edge-AI Computation. In *2025 International Conference on Vehicular Technology and Transportation Systems (ICVTTS)* (pp. 1-6). IEEE.
22. Girija, S. H., Khanum, H., Sinchana, B., Ahmed, S. T., & Rashmi, C. (2025, August). Dynamic Network Traffic Anomaly Detection Using Machine Learning. In *2025 International Conference on Artificial Intelligence and Machine Vision (AIMV)* (pp. 1-6). IEEE.
23. Alex, S., Shashank, J. T., & Ahmed, S. T. (2025, July). Machine Learning Based Network Traffic Analyser for Malicious and Benign Traffic Detection. In *2025 International Conference on Computing Technologies & Data Communication (ICCTDC)* (pp. 1-6). IEEE.