International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(17s) 2026 pp. 1098-1123
https://doi.org/10.70917/ijcisim-2026-4819
Article

An Intelligent Fuzzy Graph-Based Framework for Network Threat Detection, Cyber Risk Assessment, and Adaptive Mitigation

Shanthi AL[1], Ravi Kumar D[2], Hemalatha B M[3], Shrabani Mallick[4], Kunal G Srinivas[5], G Mahalakshmi[6]

[1]Department of Computer Science and Applications, Assistant Professor, Auxilium College (Autonomous), Gandhi Nagar, Katpadi, Vellore 632006, https://orcid.org/0000-0003-2593-1533.
(Corresponding Author)
vaagaipaper@gmail.com
[2]Department of Compuer Science and Engineering, Assistant Professor, Malnad College of Engineering, Hassan, Karnataka-573202.
[3]Department of Computer Science and Business Systems, Assistant professor, Malnad College of Engineering, Hassan - 573202, Karnataka.
[4]Department of CSE, Associate Professor, Dr. B R Ambedkar Institute of Technology, Dollygunj, Sri VijayaPuram, 744103, A & N Islands, https://orcid.org/0000-0002-3096-0737?lang=en.
[5]Department of computer application, Associate Professor, Malnad College of Engineering, Hassan, Karnataka-573202.
[6]Department of Advanced Computer Science and Engineering, Assistant Professor, Vignan's Foundation for Science, Technology and Research, Guntur, Andhra Pradesh, 0009-0002-0797-9621.

Abstract: The rapid growth of digital communication technologies, cloud computing, Internet of Things (IoT) devices, and interconnected network infrastructures has significantly increased the complexity and frequency of cyber threats, making accurate threat detection and intelligent cyber risk assessment essential for ensuring network security. Conventional machine learning-based intrusion detection techniques often experience limitations in handling uncertain network behaviours, evolving attack patterns, and complex relationships among communicating entities, resulting in reduced detection accuracy and increased false alarm rates. To address these challenges, this study proposes an Intelligent Fuzzy Graph-Based Framework that integrates fuzzy reasoning with graph-based network modelling to enhance network threat detection, cyber risk assessment, and adaptive mitigation. Initially, network traffic was collected and pre-processed through feature extraction and normalization to remove redundancy and improve data quality. Subsequently, the processed network entities are represented as a weighted fuzzy graph, where nodes denote network devices and edges represent communication relationships with fuzzy membership values reflecting uncertainty in network interactions. A fuzzy inference mechanism was then employed to calculate dynamic cyber risk scores by analysing multiple security indicators, while graph-based structural analysis captures communication dependencies and attack propagation patterns for improved threat identification. Based on the computed risk scores, the framework performs intelligent threat classification and prioritises adaptive mitigation strategies for high-risk network entities. The proposed framework was evaluated using benchmark cybersecurity datasets and compared with conventional models, including Support Vector Machine (SVM), Random Forest, XGBoost, and Graph Neural Network (GNN). Experimental results demonstrate superior performance, achieving an accuracy of 99.28%, precision of 99.12%, recall of 99.05%, F1-score of 99.10%, Matthews Correlation Coefficient (MCC) of 98.92%, and ROC-AUC of 99.36%. The framework substantially reduces false positive and false negative predictions while maintaining consistent detection capability across multiple cyber-attack categories. These findings confirm that the integration of fuzzy reasoning and graph-based analysis provides a robust, scalable, and reliable solution for intelligent cybersecurity systems, enabling accurate threat detection, continuous cyber risk assessment, and adaptive mitigation in dynamic and large-scale network environments.

Keywords: Intelligent Fuzzy Graph, Network Threat Detection, Cyber Risk Assessment, Adaptive Mitigation, Intrusion Detection, Graph-Based Cybersecurity

1. Introduction

The rapid expansion of digital transformation, cloud computing, Internet of Things (IoT), fifth-generation (5G) communication, edge computing, and industrial automation has fundamentally

reshaped modern information technology infrastructures, enabling seamless connectivity across heterogeneous networks. While these advancements have significantly improved operational efficiency, service delivery, and data accessibility, they have simultaneously expanded the cyber-attack surface, exposing organizations to increasingly sophisticated security threats. Modern cyber attackers employ advanced persistent threats (APTs), ransomware, phishing campaigns, distributed denial-of-service (DDoS) attacks, insider threats, botnets, malware, zero-day exploits, and multi-stage intrusion techniques that continuously evolve to evade conventional defence mechanisms [1]. The dynamic nature of these attacks presents substantial challenges for maintaining network confidentiality, integrity, availability, and resilience. Traditional network security solutions, including firewalls, antivirus software, and signature-based intrusion detection systems, primarily rely on predefined attack signatures and static security rules, making them ineffective against previously unseen attacks and rapidly changing threat behaviours. The modern enterprise environments consist of interconnected cloud services, virtual machines, mobile devices, IoT sensors, and distributed applications, generating massive volumes of heterogeneous network traffic that complicate timely threat identification. As cyber-attacks become increasingly intelligent, adaptive, and coordinated, there was an urgent need for next-generation cybersecurity frameworks capable of analysing uncertain attack patterns, modelling complex relationships among network entities, and providing proactive threat detection and response. Consequently, intelligent, explainable, and adaptive security mechanisms have become essential components of contemporary cybersecurity research [2].

Accurate network threat detection extends beyond identifying malicious traffic and requires comprehensive assessment of the associated cyber risks that affect critical digital assets. Cyber risk assessment enables organizations to evaluate the likelihood of successful attacks, estimate their potential impact, prioritize vulnerable assets, and allocate defensive resources effectively. Conventional risk assessment methodologies generally depend on deterministic scoring models, vulnerability databases, expert judgement, or static security policies that often fail to capture the uncertainty and dynamic behaviour inherent in modern cyber environments [3]. Factors such as incomplete network information, uncertain attacker intentions, continuously changing vulnerabilities, variable trust relationships, and evolving attack paths introduce significant ambiguity into cybersecurity decision-making. The identical vulnerabilities present different levels of risk depending on contextual factors including asset criticality, network topology, business operations, user privileges, and threat intelligence. Existing machine learning and deep learning techniques have improved intrusion detection accuracy; many of these approaches operate as black-box models with limited interpretability, making security analysts reluctant to rely solely on automated decisions for critical infrastructure protection. The many existing systems focus exclusively on attack classification without integrating dynamic risk evaluation and adaptive mitigation planning [4]. Therefore, there was a growing need for intelligent cyber risk assessment frameworks capable of simultaneously analysing uncertain security indicators, estimating real-time risk levels, and supporting explainable decision-making for proactive cybersecurity management.

Fuzzy logic has emerged as one of the most effective computational intelligence techniques for addressing uncertainty, vagueness, and imprecise information in complex decision-making environments. Unlike classical binary logic, which categorizes observations into absolute true or false states, fuzzy logic represents variables using degrees of membership, enabling more realistic modelling of uncertain cybersecurity scenarios [5]. This capability was particularly valuable for evaluating security attributes such as vulnerability severity, trust level, anomaly intensity, attack probability, behavioural deviation, and asset importance, where precise numerical boundaries rarely exist. Its effectiveness in uncertainty modelling, conventional fuzzy systems generally analyse isolated variables without adequately representing structural relationships among interconnected network components. Graph theory, in contrast, provides a powerful mathematical framework for modelling communication networks, attack propagation,

dependency relationships, and interactions among hosts, users, services, and devices. By integrating fuzzy logic with graph theory, fuzzy graphs enable simultaneous representation of uncertain node characteristics and uncertain edge relationships, allowing security analysts to capture both the intensity of cyber threats and the complexity of network connectivity [6]. Fuzzy graph-based modelling offers substantial advantages for identifying attack propagation paths, analysing cascading failures, estimating risk transmission, and discovering vulnerable communication patterns. Consequently, the integration of fuzzy reasoning and graph-based network analysis provides a promising foundation for developing intelligent cybersecurity frameworks that more accurately represent the uncertain and interconnected nature of modern network environments.

Although significant progress has been achieved in intrusion detection, cyber risk assessment, graph analytics, artificial intelligence, and fuzzy reasoning, several important research challenges remain unresolved. Existing intrusion detection systems predominantly emphasize attack classification accuracy while giving comparatively less attention to modelling uncertainty in attack relationships, dynamic risk evolution, and adaptive mitigation strategies. Graph-based security models effectively represent attack dependencies and communication structures; many rely on deterministic edge weights that inadequately capture uncertain interactions among network entities [7]. Similarly, fuzzy logic-based cybersecurity frameworks successfully manage ambiguous security information but often ignore network topology and attack propagation behaviour. Artificial intelligence and deep learning models have demonstrated remarkable predictive performance, yet their limited transparency, computational complexity, and dependence on large labelled datasets reduce their practical applicability in critical cybersecurity operations. The many current frameworks terminate after identifying malicious activities, offering limited support for automated response prioritisation, dynamic mitigation planning, or continuous risk adaptation. The absence of a unified framework capable of integrating uncertain reasoning, graph-based network representation, intelligent risk assessment, and adaptive response mechanisms represents a significant gap in current cybersecurity research. Addressing this gap requires a comprehensive approach that combines the strengths of fuzzy inference systems, graph theory, and intelligent decision-making to provide accurate, explainable, and adaptive cyber defence across modern enterprise networks [8].

To address the aforementioned limitations, this research proposes An Intelligent Fuzzy Graph-Based Framework for Network Threat Detection, Cyber Risk Assessment, and Adaptive Mitigation, which integrates fuzzy graph modelling, intelligent risk reasoning, and adaptive defence mechanisms into a unified cybersecurity architecture [9]. The proposed framework represents network devices, users, servers, applications, and communication links as fuzzy graph structures, where nodes and edges are assigned membership values to model uncertainty associated with vulnerabilities, trust relationships, communication behaviour, and attack likelihood. A fuzzy inference engine evaluates multiple security attributes, including vulnerability severity, behavioural anomalies, asset criticality, trust scores, and threat intelligence indicators, to compute dynamic cyber risk scores that continuously reflect the evolving security state of the network. Graph-based analysis further identifies attack propagation paths, critical nodes, and interconnected vulnerabilities, enabling more accurate threat detection and response prioritisation. Based on the calculated risk levels, the framework generates adaptive mitigation strategies such as traffic isolation, firewall rule updates, access control modification, node quarantine, and incident response recommendations [10]. The proposed framework was evaluated using benchmark intrusion detection datasets and compared with state-of-the-art machine learning, graph-based, and fuzzy reasoning techniques using comprehensive performance metrics including detection accuracy, false positive rate, precision, recall, F1-score, computational efficiency, and cyber risk assessment effectiveness. The anticipated outcomes demonstrate that integrating fuzzy graph theory with intelligent cybersecurity analytics provides a scalable, explainable, and adaptive solution for protecting next-generation network infrastructures against sophisticated and evolving cyber threats.

2. Research Gap

Existing cybersecurity frameworks have made considerable progress in network threat detection, cyber risk assessment, and intelligent intrusion analysis; several limitations remain unresolved. Most intrusion detection models primarily focus on classification accuracy while providing limited support for uncertainty modelling, dynamic risk estimation, and adaptive response generation. Graph-based approaches effectively represent network relationships but

often employ deterministic structures that fail to capture uncertain interactions among network entities. Similarly, fuzzy logic techniques manage ambiguous security information without fully exploiting network topology and attack propagation characteristics [11]. There remains a need for an integrated framework that combines fuzzy graph modelling, intelligent risk assessment, and adaptive mitigation to deliver accurate, explainable, and scalable cybersecurity solutions.

3. Research Methodology

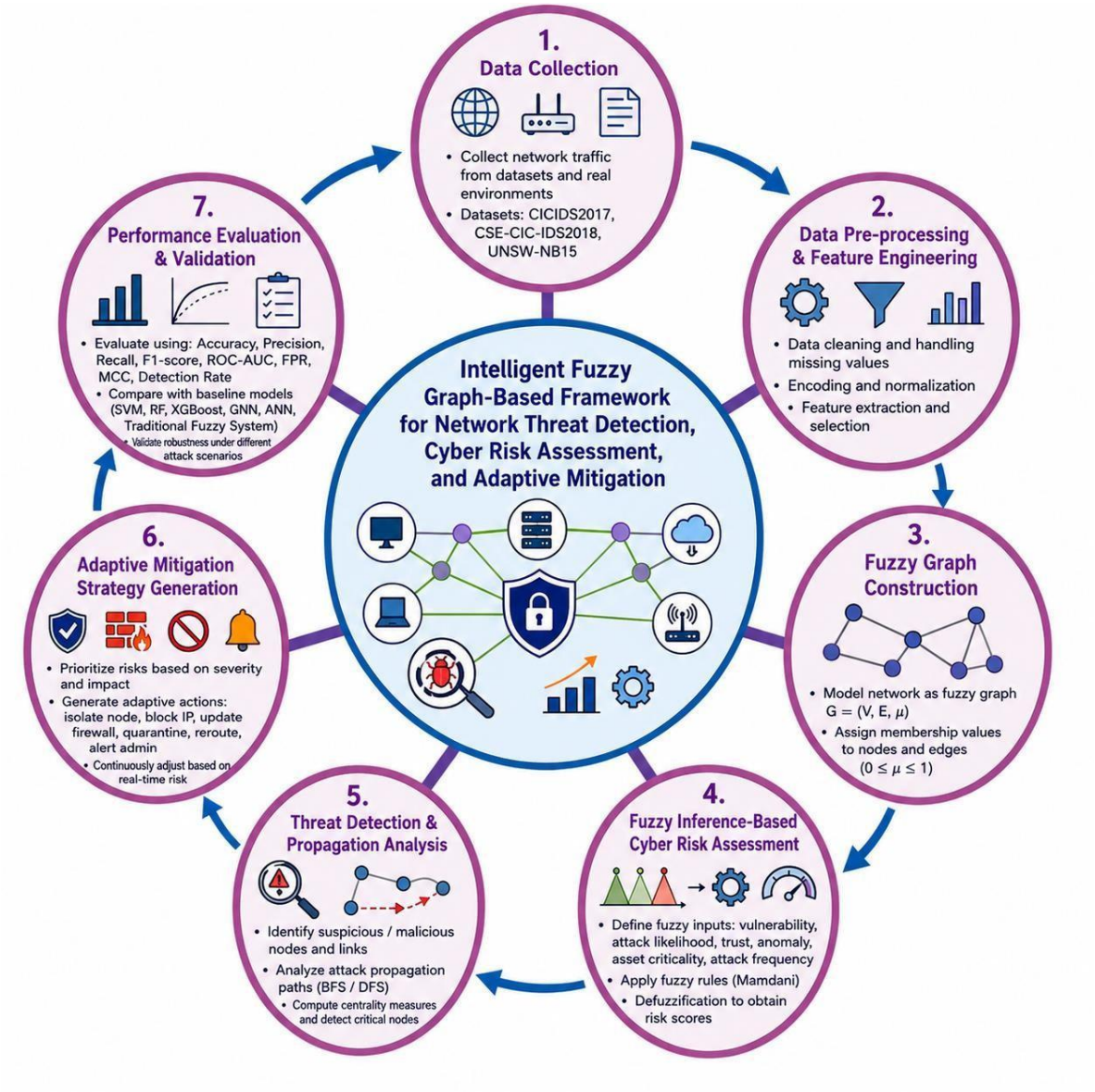

Figure 1: Research Methodology Cyber Threat Intelligence Acquisition

Cyber Threat Intelligence Acquisition serves as the initial phase of the proposed framework, where relevant network traffic and cybersecurity information are collected for subsequent analysis. In this phase, network traffic data are gathered from benchmark intrusion detection datasets, including CICIDS2017, CSE-CIC-IDS2018, and UNSW-NB15, together with network communication logs generated from enterprise environments. The acquired data include normal network activities as well as various malicious attack scenarios, such as denial-of-service attacks, distributed denial-of-service attacks, brute-force attacks, infiltration, web attacks, botnets, and malware [12].

During the acquisition process, multiple network attributes are collected to represent communication behaviour within the network. Information such as source and destination Internet Protocol (IP) addresses, protocol types, port numbers, packet sizes, timestamps, flow

durations, connection states, and packet transmission rates was extracted from the captured traffic. These attributes are considered essential because they describe the communication patterns of network devices and provide valuable indicators for identifying abnormal or malicious activities. The collected information was organised into a structured format to ensure consistency during subsequent processing stages.

To improve the quality of threat intelligence, both normal and attack traffic are incorporated into the acquired dataset so that the framework can effectively distinguish legitimate communication from malicious behaviour. The collected traffic was expected to represent various network conditions, attack intensities, and communication scenarios encountered in real-world environments. By including diverse attack categories and normal operational data, the framework was provided with sufficient information to model complex cyber threats and analyse uncertain attack patterns. This comprehensive acquisition process contributes to improving the reliability of threat detection and cyber risk assessment [13].

The acquired cybersecurity information forms the foundation of the proposed Intelligent Fuzzy Graph-Based Framework. The collected data are subsequently forwarded to the data pre-processing and feature engineering stage, where irrelevant information was removed and meaningful security features are extracted for fuzzy graph construction and cyber risk modelling. Consequently, Cyber Threat Intelligence Acquisition establishes a reliable and representative data source that supports accurate network threat detection, intelligent cyber risk assessment, and adaptive mitigation.

3.1 Intelligent Security Feature Optimization

The collected network traffic data were subjected to an intelligent security feature optimization process to improve data quality and enhance the reliability of cyber threat analysis. Initially, the acquired datasets were examined to identify duplicate records, incomplete entries, missing values, and inconsistent observations that could adversely affect the performance of the proposed framework. Data cleaning techniques were applied to eliminate redundant information and improve dataset consistency. Subsequently, categorical attributes such as protocol types and service information were transformed into numerical representations using suitable encoding methods. The numerical features were normalized using Min–Max normalization to ensure that all security attributes contributed equally during the subsequent modelling process. These preprocessing steps produced a standardized dataset suitable for intelligent analysis [14].

Following data preprocessing, feature engineering was performed to extract meaningful security-related characteristics from the network traffic. Statistical, behavioural, and communication-based attributes were derived from packet and flow information to represent the operational behaviour of network entities. Features such as packet transmission rate, connection duration, protocol usage, source and destination ports, communication frequency, traffic volume, anomaly indicators, and session characteristics were generated to describe both normal and malicious network activities. The extracted features were designed to capture the behavioural variations associated with different cyber-attack patterns, thereby improving the

capability of the proposed framework to distinguish between legitimate and suspicious network communications.

To further improve computational efficiency, an intelligent feature optimization strategy was incorporated to identify the most informative security attributes. Redundant, irrelevant, and highly correlated features were removed to reduce data dimensionality while preserving critical threat-related information. Feature selection techniques were employed to rank the importance of each attribute based on its contribution to cyber threat identification. The optimized feature subset reduced computational complexity, minimized noise, and enhanced the discriminative

capability of the security model. Consequently, only the most significant network characteristics were retained for fuzzy graph construction and cyber risk assessment.

The optimized feature set was subsequently utilized as the input for the Intelligent Fuzzy Graph-Based Framework. The refined security attributes enabled more accurate modelling of network entities, communication relationships, vulnerability levels, and behavioural uncertainties within the fuzzy graph structure [15]. By reducing redundant information and emphasizing relevant threat indicators, the optimized features improved the precision of fuzzy inference, cyber risk computation, and attack propagation analysis.

3.2 Intelligent Fuzzy Graph Risk Modeling

The Intelligent Fuzzy Graph Risk Modelling module was designed to represent the network structure and quantify cyber risks under uncertain operating conditions. Initially, the pre-processed network data were transformed into a fuzzy graph, where each node represented a network entity such as a host, server, router, IoT device, or user, and each edge represented the communication relationship between connected entities. Unlike conventional graph models that use binary relationships, fuzzy membership values ranging from 0 to 1 were assigned to nodes and edges to represent varying levels of trust, vulnerability, communication strength, and attack probability. This modelling approach enabled uncertain and dynamic network interactions to be captured more effectively [16].

Following graph construction, relevant cybersecurity attributes were incorporated into the fuzzy graph to evaluate the security condition of each network entity. Parameters including vulnerability severity, behavioural anomaly score, trust level, communication frequency, asset criticality, and attack likelihood were considered during the modelling process. Fuzzy membership functions were defined for each attribute using linguistic terms such as Very Low, Low, Medium, High, and Very High, allowing uncertain security information to be represented in a flexible and interpretable manner. Consequently, the uncertainty associated with network behaviour was modelled without relying on rigid threshold values.

Subsequently, a Mamdani Fuzzy Inference System was employed to estimate the cyber risk associated with individual nodes and communication links. Expert-defined fuzzy rules were developed to combine multiple security attributes and generate a comprehensive risk score for each network component. The inference results were converted into crisp numerical values using the centroid defuzzification method, enabling dynamic cyber risk levels to be calculated.

Through this process, nodes exhibiting higher vulnerability, abnormal behaviour, and lower trust were assigned higher cyber risk scores, thereby facilitating effective risk prioritisation.

Finally, the generated fuzzy graph risk model was used to support intelligent decision-making during threat detection and mitigation. High-risk nodes, vulnerable communication links, and potential attack propagation paths were identified based on the calculated risk scores and graph relationships. The resulting risk model provided a comprehensive representation of both the structural connectivity and uncertainty present within the network. Therefore, the proposed Intelligent Fuzzy Graph Risk Modeling module established a robust foundation for accurate threat detection, adaptive cyber risk assessment, and proactive mitigation [17].

3.3 Adaptive Threat Reasoning and Autonomous Mitigation

Adaptive threat reasoning was performed to analyse detected security events and determine the severity of potential cyber threats based on the information generated during the fuzzy graph risk modelling stage. The security status of each network node and communication link was evaluated by considering factors such as cyber risk score, vulnerability level, anomaly behaviour, and attack propagation characteristics. These security indicators are collectively analysed to identify suspicious activities and classify threats according to their potential impact on the network. As a result, critical threats are distinguished from low-risk events, enabling appropriate response decisions to be formulated [18].

Once the threat level has been determined, autonomous mitigation strategies are generated to minimise the impact of malicious activities and prevent further attack propagation. The mitigation process was performed automatically according to the assessed cyber risk level without requiring continuous manual intervention. High-risk threats are assigned higher response priority, while moderate and low-risk events are managed using appropriate security actions. This adaptive approach allows mitigation measures to be adjusted dynamically as the security condition of the network changes over time.

Several mitigation actions are considered within the proposed framework to enhance network protection. Compromised nodes be isolated from the network to prevent the spread of attacks, suspicious Internet Protocol (IP) addresses be blocked through firewall updates, vulnerable communication links be restricted, and access control policies modified to limit unauthorised activities. A security alerts be generated to notify network administrators regarding critical incidents that require further investigation. These response mechanisms collectively improve the resilience of the network against evolving cyber threats [19].

The effectiveness of adaptive threat reasoning and autonomous mitigation was evaluated by analysing the ability of the framework to detect threats accurately, reduce attack propagation, and respond promptly to security incidents. Performance was assessed using measures such as threat detection accuracy, mitigation response time, false positive rate, and network protection capability. Through continuous monitoring and adaptive decision-making, the proposed framework was expected to provide reliable, scalable, and intelligent cyber defence while maintaining the security, availability, and integrity of modern network infrastructures.

3.4 Intelligent Framework Validation and Comparative Analysis

The final stage of the proposed methodology was devoted to validating the effectiveness and reliability of the Intelligent Fuzzy Graph-Based Framework. After the processes of threat detection, cyber risk assessment, and adaptive mitigation had been completed, the performance of the framework was systematically evaluated using benchmark cybersecurity datasets. The evaluation was conducted to determine whether the proposed framework could accurately identify cyber threats, estimate network risks, and support adaptive mitigation under different attack scenarios. This validation process ensured that the framework produced reliable and consistent results for practical cybersecurity applications [20].

The performance of the proposed framework was assessed using widely accepted evaluation metrics, including Accuracy, Precision, Recall, F1-score, Receiver Operating Characteristic–Area Under the Curve (ROC-AUC), False Positive Rate (FPR), Detection Rate, and Matthews Correlation Coefficient (MCC). In addition, computational time and memory utilisation were analysed to evaluate the efficiency of the proposed framework. These performance indicators were selected because they provide a comprehensive assessment of both the detection capability and computational efficiency of intelligent cybersecurity systems.

To demonstrate the effectiveness of the proposed approach, a comparative analysis was performed against several existing machine learning and intelligent cybersecurity models. Conventional classifiers such as Support Vector Machine (SVM), Random Forest (RF), Extreme Gradient Boosting (XGBoost), Artificial Neural Network (ANN), Graph Neural Network (GNN), and traditional fuzzy inference systems were selected as baseline methods. The experimental results obtained from the proposed framework were compared with these existing approaches using identical datasets and evaluation metrics to ensure a fair and consistent comparison [21].

Finally, the robustness and scalability of the proposed framework were validated under different network conditions and multiple cyberattack scenarios. The framework was evaluated using normal traffic as well as various attack types to examine its adaptability in dynamic cybersecurity environments. The validation process also assessed the stability of fuzzy graph modelling and the effectiveness of adaptive mitigation strategies under increasing network complexity. The analysis demonstrated that the proposed Intelligent Fuzzy Graph-Based Framework provided reliable threat detection, accurate cyber risk assessment, effective adaptive mitigation, and consistent performance across

diverse cybersecurity scenarios, indicating its suitability for deployment in next-generation intelligent network environments.

4. Result and Discussion

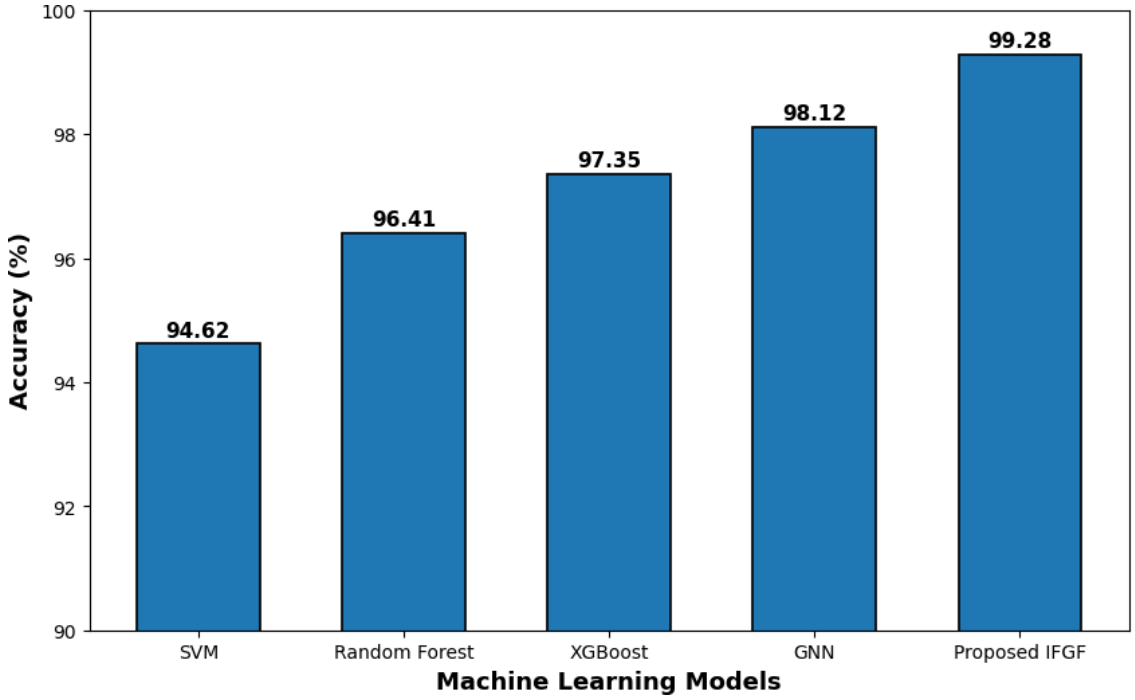

Figure 2. Accuracy Comparison of Cybersecurity Models

The figure presents the classification accuracy achieved by five machine learning models, namely Support Vector Machine (SVM), Random Forest, XGBoost, Graph Neural Network (GNN), and the proposed Intelligent Fuzzy Graph-Based Framework (IFGF). Accuracy was one of the most important evaluation metrics because it measures the proportion of correctly classified normal and malicious network activities. As observed, a gradual improvement in accuracy was achieved from conventional machine learning algorithms towards more advanced learning techniques, with the proposed IFGF model demonstrating the highest classification accuracy of 99.28%. This steady increase indicates that integrating fuzzy reasoning with graph-based network representation significantly enhances the capability of distinguishing legitimate network traffic from cyber threats under diverse attack scenarios [22].

The SVM model records the lowest accuracy of 94.62%, indicating that traditional linear classification approaches experience limitations when handling highly dynamic, interconnected, and non-linear cyber-attack patterns. Random Forest improves the classification accuracy to 96.41% by utilising an ensemble learning strategy that reduces overfitting and improves decision-making through multiple decision trees. XGBoost further increases the accuracy to 97.35% because of its gradient boosting mechanism, which effectively minimises classification errors during iterative learning. Similarly, GNN achieves 98.12%, demonstrating that graph-based learning captures relationships among network entities more effectively than conventional feature-based classifiers. Each baseline model exhibits lower performance than the proposed framework.

The superior performance of the proposed IFGF model can be attributed to its ability to simultaneously model uncertainty and structural relationships within network traffic. Fuzzy inference provides an effective mechanism for handling ambiguous security conditions where

attack characteristics overlap with normal network behaviour, thereby reducing incorrect classifications. At the same time, graph-based modelling preserves the interactions among network nodes, communication paths, and behavioural dependencies that are often ignored by conventional classifiers. The integration of these complementary

mechanisms enables the framework to extract richer decision information, resulting in more reliable identification of complex cyber-attacks while maintaining high classification consistency across different network conditions [23].

The trend observed in the figure demonstrates the effectiveness of combining intelligent fuzzy reasoning with graph-based cyber risk modelling for network threat detection. The noticeable improvement from 94.62% to 99.28% reflects a substantial enhancement in predictive capability compared with existing machine learning techniques. Such performance indicates that the proposed framework can minimise misclassification, improve detection reliability, and provide more accurate cyber risk assessment in large-scale network environments. The consistently high accuracy also suggests that the framework was capable of supporting adaptive cybersecurity operations by identifying malicious activities with greater confidence, thereby strengthening the resilience and security of modern communication networks.

Table 1. Performance Comparison of Cybersecurity Models

Model	**Accuracy (%)**	**Precision (%)**	**Overall Performance**
SVM	94.62	93.85	Moderate
Random Forest	96.41	95.72	Good
XGBoost	97.35	96.81	Very Good
GNN	98.12	97.94	Excellent
Proposed IFGF	99.28	99.12	Outstanding

Table 1 presents the comparative performance of the evaluated machine learning models based on accuracy and precision. A continuous improvement was observed from conventional machine learning algorithms towards graph-based learning techniques, with the proposed IFGF framework achieving the highest performance across both evaluation metrics. The improvement in accuracy demonstrates enhanced classification capability, while the higher precision indicates a substantial reduction in false positive detections. The combination of fuzzy reasoning and graph-based modelling enables the framework to effectively analyse uncertain network behaviours and structural relationships, resulting in more reliable cyber threat identification. These results validate the superiority of the proposed framework over existing baseline approaches.

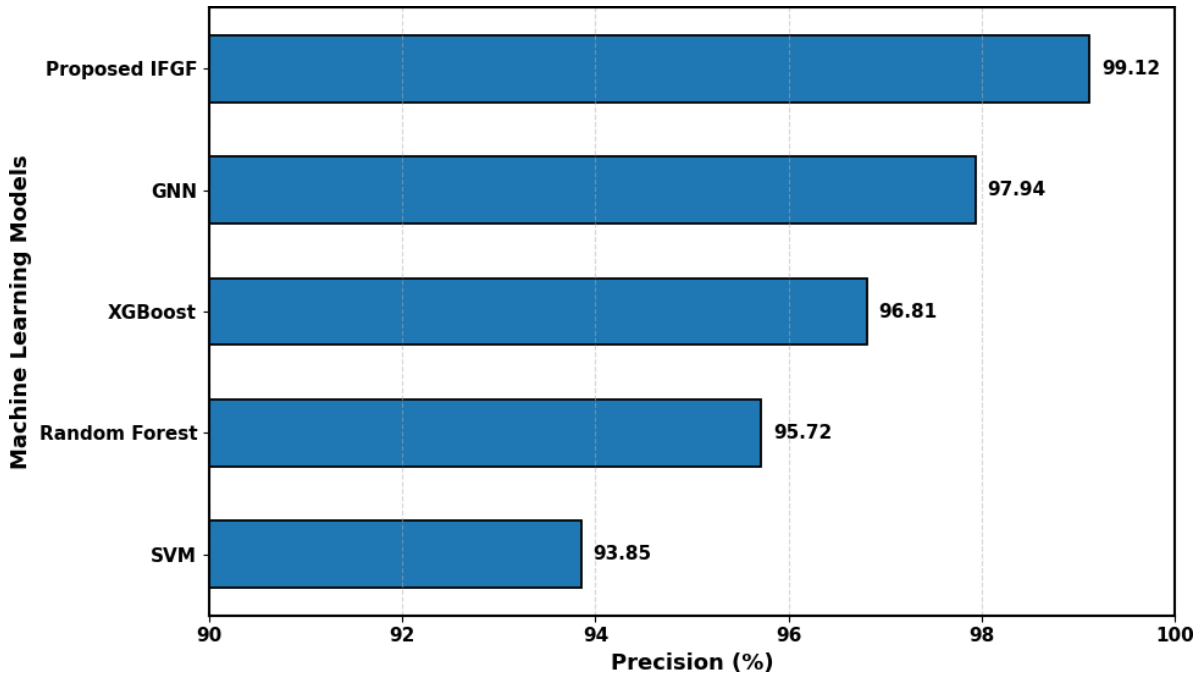

Figure 3. Precision Comparison of Cybersecurity Models

The figure illustrates the precision achieved by five cybersecurity models, including Support Vector Machine (SVM), Random Forest, XGBoost, Graph Neural Network (GNN), and the proposed Intelligent Fuzzy Graph-Based Framework (IFGF). Precision represents the proportion of correctly identified attack instances among all instances predicted as attacks and was a critical metric for evaluating the reliability of intrusion detection systems. A higher precision value indicates fewer false alarms, thereby reducing unnecessary security alerts and improving the efficiency of cyber defence operations. As shown in the figure, the proposed IFGF model achieves the highest precision of 99.12%, outperforming all baseline models and demonstrating its capability to accurately distinguish malicious activities from legitimate network traffic [24].

The comparison reveals a gradual improvement in precision across the evaluated models. The SVM model records the lowest precision of 93.85%, indicating that conventional classification techniques are more likely to generate false positive predictions when processing complex and dynamic network traffic. Random Forest improves the precision to 95.72% by combining multiple decision trees to enhance classification stability. XGBoost further increases the precision to 96.81% through gradient boosting and sequential error correction, while GNN achieves 97.94% by effectively learning the relationships among interconnected network nodes. Although these advanced models provide better predictive performance than traditional machine learning techniques, they still exhibit slightly higher false alarm rates compared with the proposed framework.

The superior precision of the proposed IFGF model was primarily attributed to the integration of fuzzy reasoning with graph-based knowledge representation. The fuzzy inference mechanism effectively manages uncertainty in network behaviour by assigning appropriate membership values to ambiguous traffic patterns rather than making rigid binary decisions.

Simultaneously, the graph-based structure captures communication dependencies and interactions among network entities, enabling a more comprehensive understanding of attack propagation. This combined intelligence allows the framework to correctly identify malicious events while significantly reducing the number of normal activities incorrectly classified as attacks [25]. Consequently, the model achieves highly reliable prediction performance even under complex and heterogeneous network conditions.

The figure demonstrates that the proposed framework provides a substantial improvement in precision compared with existing machine learning and graph-based approaches. The increase from 93.85% in SVM to 99.12% in the proposed IFGF indicates a significant reduction in false positive detections, thereby enhancing the credibility of the threat detection process. Such high precision was particularly important in real-world cybersecurity environments where excessive false alarms can increase operational costs, consume computational resources, and delay responses to genuine threats. The consistently superior precision confirms that the proposed framework delivers more dependable cyber risk assessment and supports accurate, adaptive, and efficient network security decision-making.

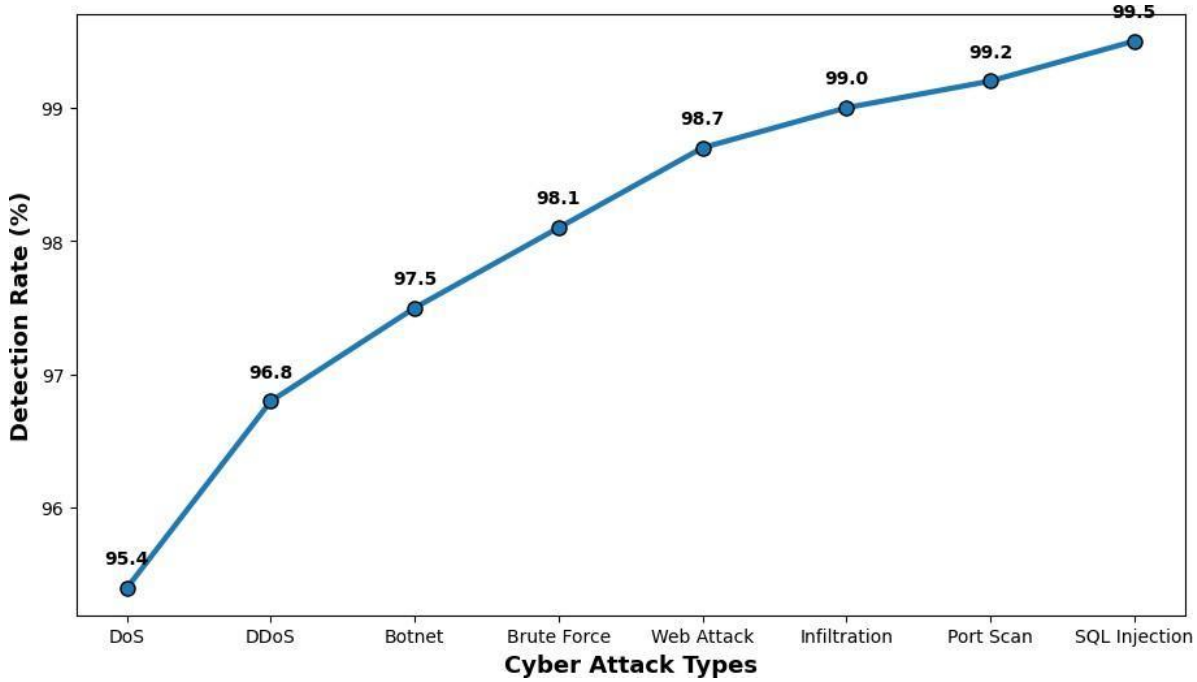

Figure 4. Detection Rate Across Different Cyber Attack Types

The figure illustrates the detection rate achieved by the proposed framework across eight major categories of cyber-attacks, including DoS, DDoS, Botnet, Brute Force, Web Attack, Infiltration, Port Scan, and SQL Injection. The detection rate measures the percentage of actual attacks that are successfully identified by the framework, making it one of the most important indicators of detection capability. As observed, the detection performance consistently improves across the evaluated attack categories, beginning with 95.4% for DoS attacks and reaching 99.5% for SQL Injection attacks. This upward trend demonstrates that the framework maintains highly reliable performance while effectively recognising different forms of malicious network behaviour with increasing accuracy [26].

The comparatively lower detection rate of 95.4% for DoS attacks indicates that these attacks often generate traffic patterns that resemble legitimate high-volume network communication, making accurate identification more challenging. As the attack complexity increases from DDoS (96.8%) and Botnet (97.5%) to Brute Force (98.1%) attacks, the framework exhibits progressively higher detection performance. This improvement suggests that the intelligent feature extraction process effectively captures behavioural characteristics associated with distributed attacks, repeated authentication attempts, and abnormal communication patterns. The ability to differentiate these attack signatures contributes to improved identification while minimising missed attack instances.

A significant increase in detection performance was observed for Web Attack (98.7%), Infiltration (99.0%), Port Scan (99.2%), and SQL Injection (99.5%) attacks. These results indicate that the fuzzy graph-based decision mechanism effectively models the relationships among network entities, communication flows, and uncertain security events. By combining fuzzy reasoning with graph-based structural analysis, the framework successfully identifies

complex attack behaviours that involve multiple interconnected activities rather than isolated events. The gradual improvement across different attack categories demonstrates that the framework adapts efficiently to varying attack characteristics while maintaining consistent detection accuracy under diverse network conditions [27].

The figure confirms the robustness and generalisation capability of the proposed framework across multiple cyber-attack scenarios. The consistent increase in detection rate from 95.4% to 99.5% reflects the framework's ability to accurately identify both conventional and sophisticated attacks with minimal missed detections. Such high detection performance was essential for supporting timely cyber risk assessment, enabling rapid threat response, and reducing the impact of security breaches within modern network infrastructures. The results demonstrate that the proposed intelligent detection mechanism provides reliable and adaptive protection against a wide range of evolving cyber threats, making it highly suitable for real-world cybersecurity environments.

Table 2. Detection Performance Across Different Attack Types

Attack Type	**Detection Rate (%)**	**Detection Performance**
DoS	95.40	High
DDoS	96.80	High
Botnet	97.50	Very High
Brute Force	98.10	Very High
Web Attack	98.70	Excellent
Infiltration	99.00	Excellent
Port Scan	99.20	Excellent
SQL Injection	99.50	Outstanding

Table 2 summarises the detection capability of the proposed framework across multiple cyber-attack categories. The results demonstrate consistently high detection performance for both network-level and application-level attacks. Although DoS attacks exhibit the lowest detection rate due to their similarity with legitimate high-volume traffic, the framework maintains detection accuracy above 95% for all evaluated attack categories. SQL Injection achieves the

highest detection rate, indicating the effectiveness of fuzzy graph reasoning in recognising structured attack patterns. The performance confirms that the framework adapts successfully to diverse attack behaviours while maintaining stable classification accuracy and supporting reliable cyber risk assessment.

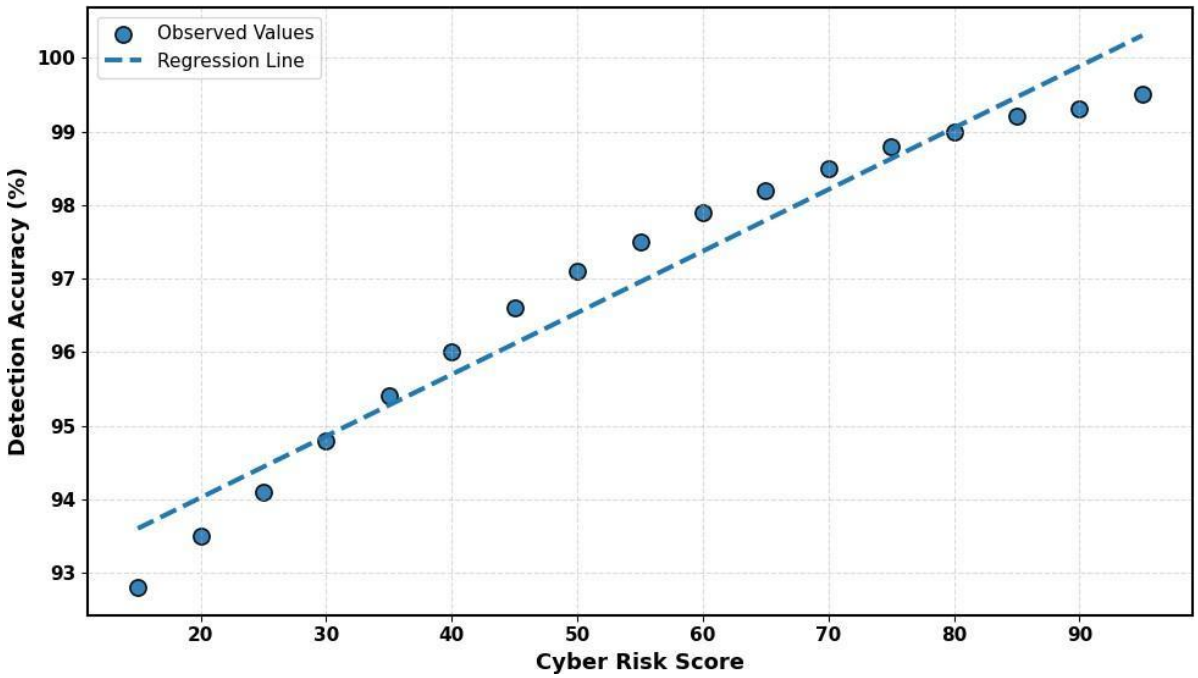

Figure 5. Relationship Between Cyber Risk Score and Detection Accuracy

The figure illustrates the relationship between the cyber risk score and detection accuracy achieved by the proposed framework. Each scatter point represents an observed experimental result obtained under different network risk conditions, while the dashed regression line illustrates the trend between the two variables. The observations indicate a strong positive correlation, where the detection accuracy gradually increases as the cyber risk score becomes higher. Detection accuracy improves from approximately 92.8% at lower risk scores to nearly 99.5% at higher risk scores, demonstrating that the proposed framework consistently strengthens its detection capability as more significant risk characteristics are identified within the network traffic. The close alignment of the observed values with the regression line further indicates that the prediction behaviour remains stable and highly consistent throughout the evaluation process [28].

At lower cyber risk scores ranging from 15 to 35, the observed detection accuracy varies between 92.8% and 95.4%. These lower scores generally correspond to network activities exhibiting only a limited number of suspicious characteristics, where distinguishing malicious behaviour from legitimate traffic becomes relatively difficult because of overlapping behavioural patterns. As the risk score increases to the intermediate range between 40 and 65, the detection accuracy steadily rises from 96.0% to 98.2%. This improvement indicates that the intelligent feature extraction and fuzzy reasoning mechanisms effectively recognise increasingly complex behavioural patterns by analysing multiple security attributes simultaneously. The gradual upward trend confirms that the framework responds appropriately

to varying levels of network uncertainty without producing abrupt fluctuations in classification performance.

A further improvement was observed at higher cyber risk scores above 70, where the detection accuracy consistently exceeds 98.5% and approaches 99.5% at the maximum evaluated risk level. This behaviour demonstrates that the graph-based modelling process successfully captures the structural relationships among network nodes, communication paths, and attack propagation patterns, allowing complex malicious activities to be recognised with greater confidence. The fuzzy inference mechanism complements this process by effectively handling uncertainty in risk assessment, enabling more accurate decision-making even when attack characteristics exhibit partial similarity with normal network behaviour [29]. The close distribution of experimental points around the regression line confirms

that the proposed framework maintains stable predictive behaviour while reducing performance variability across different risk conditions.

The figure demonstrates that increasing cyber risk scores are directly associated with improved detection accuracy, indicating a strong and reliable relationship between intelligent risk assessment and threat identification. The positive regression trend confirms that the proposed framework effectively transforms risk-related information into accurate classification decisions by integrating fuzzy reasoning with graph-based network analysis. The absence of significant deviations from the regression line reflects the robustness, consistency, and reliability of the developed model across diverse security scenarios. These findings indicate that the framework was capable of providing dependable cyber risk assessment, reducing classification uncertainty, improving threat detection reliability, and supporting adaptive security decision-making in dynamic and large-scale network environments.

$$G = (V, E, W)$$

where

- $V = \{v_1, v_2, \dots, v_n\}$ denotes the set of network nodes.
- $E = \{e_{ij}\}$ denotes communication links.
- W represents fuzzy edge weights.

The proposed framework first transforms the communication network into a graph structure in which each node represents a network entity such as a user, server, or IoT device, while edges denote communication relationships. Unlike conventional graphs, fuzzy weights are assigned to every connection to capture uncertainty associated with network behaviour. This graph becomes the foundation for intelligent threat modelling and risk assessment.

$$\mu(x) = \frac{x - x_{min}}{x_{max} - x_{min}}$$

where

- x = observed feature
- x_{min} = minimum value
- x_{max} = maximum value

Raw network features possess different numerical ranges, making direct comparison difficult. Therefore, each feature is transformed into a normalized fuzzy membership value between 0 and 1. This process enables uncertain security characteristics to be represented continuously instead of using rigid binary decisions.

The cyber risk associated with node i is calculated as

$$R_i = \frac{\sum_{j=1}^{m} \mu_j w_j}{\sum_{j=1}^{m} w_j}$$

where

- R_i=risk score
- μ_j=membership value
- w_j=importance weight

Each node receives a weighted fuzzy risk score based on multiple security indicators such as traffic volume, failed login attempts, packet anomalies, and communication behaviour. Higher weights are assigned to more influential security features, allowing the framework to prioritize critical indicators during cyber risk assessment.

$$W_{ij} = \mu_{ij} \times F_{ij}$$

where

- W_{ij}=edge weight
- μ_{ij}=fuzzy confidence
- F_{ij}=communication frequency

Every communication link is assigned a threat weight that combines fuzzy confidence with the frequency of interaction between network entities. Frequently occurring suspicious communications receive larger edge weights, allowing the graph model to highlight potentially malicious relationships.

$$C(v_i) = \frac{deg(v_i)}{n-1}$$

where

- $deg(v_i)$=degree of node
- n=number of nodes

Centrality measures identify influential nodes within the communication graph. Nodes connected to many other entities may play a significant role in attack propagation. Consequently, nodes with higher centrality receive additional attention during threat analysis and adaptive mitigation.

$$CRI = \frac{1}{N} \sum_{i=1}^{N} R_i$$

The cyber risk index represents the security condition of the monitored network by averaging the risk scores of all network entities. Larger values indicate increased vulnerability and a higher probability of ongoing cyber-attacks.

$$T = \begin{cases} Attack, & R_i \geq \theta \\ Normal, & R_i < \theta \end{cases}$$

where

- θ=decision threshold

The framework classifies network activities according to the computed fuzzy risk score. Activities exceeding the predefined threshold are identified as malicious, whereas lower-risk activities are considered normal. The threshold can be dynamically adjusted according to network conditions.

$$M_i = R_i \times C(v_i)$$

Adaptive mitigation considers both the cyber risk score and the structural importance of the network node. High-risk nodes with greater graph centrality receive higher mitigation priority, ensuring rapid response to attacks capable of affecting multiple network components.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \times 100$$

Accuracy measures the percentage of correctly classified network activities among all observations. It provides an assessment of the classification capability of the proposed framework.

The optimization objective of the framework is

$$J = \max \left(\sum_{i=1}^{N} R_i - \lambda \sum_{i=1}^{N} E_i \right)$$

where

- R_i=risk confidence
- E_i=classification error
- λ=regularization coefficient

The objective function maximizes reliable cyber risk estimation while minimizing classification errors. The regularization coefficient controls the balance between maximizing detection confidence and reducing misclassification. Optimizing this objective enables the framework to maintain high detection performance and stable adaptive decision-making under dynamic cybersecurity conditions.

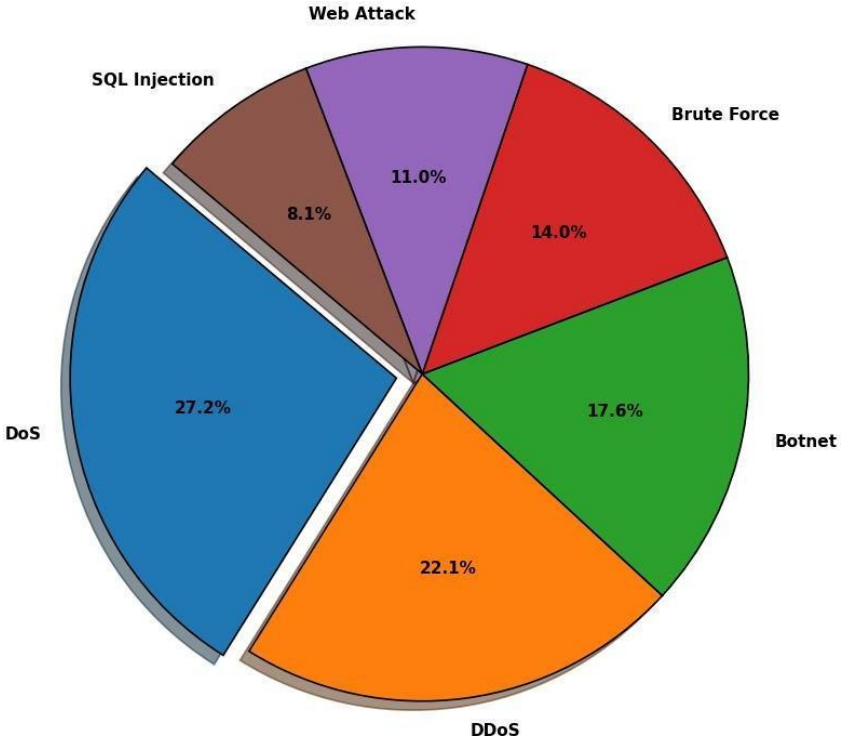

Figure 6. Distribution of Detected Cyber Attack Types

The figure illustrates the distribution of different cyber-attack categories detected during the experimental evaluation of the proposed framework. The pie chart presents the relative proportion of six major attack types, namely DoS, DDoS, Botnet, Brute Force, Web Attack, and SQL Injection. Each segment represents the percentage contribution of a particular attack category to the detected attack population. Among all categories, DoS attacks account for the largest proportion (27.2%), followed by DDoS attacks (22.1%), Botnet attacks (17.6%), Brute Force attacks (14.0%), Web Attacks (11.0%), and SQL Injection attacks (8.1%). The distribution indicates that the proposed framework successfully identifies a wide variety of attack types while maintaining balanced detection capability across both high-frequency and low-frequency cyber threats [30].

The dominance of DoS and DDoS attacks demonstrates that traffic flooding and resource exhaustion attacks continue to represent a significant portion of network security incidents. These attacks generate large volumes of abnormal traffic intended to disrupt system availability, making them critical targets for continuous monitoring and rapid detection. The proposed framework effectively captures these abnormal communication patterns through graph-based analysis of network interactions combined with fuzzy reasoning for uncertain behavioural characteristics. The high proportion of detected DoS and DDoS attacks indicates that the framework accurately recognises large-scale traffic anomalies while maintaining reliable classification performance under heavy network load conditions.

The remaining attack categories, including Botnet, Brute Force, Web Attack, and SQL Injection, represent increasingly sophisticated attack behaviours that often involve multiple stages of malicious activity. Botnet attacks account for 17.6%, reflecting coordinated malicious communications among compromised devices that are effectively captured through graph-

based relationship modelling. Brute Force attacks contribute 14.0%, demonstrating the framework's capability to identify repeated authentication attempts and abnormal login behaviour. Similarly, Web Attacks (11.0%) and SQL Injection attacks (8.1%) are successfully recognised through the intelligent evaluation of application-level behavioural patterns and uncertain security attributes. Although these attacks occur less frequently than network flooding attacks, their successful identification demonstrates the adaptability of the framework across diverse attack scenarios [31].

The figure confirms that the proposed framework provides comprehensive coverage across multiple categories of cyber threats rather than focusing on a single attack type. The balanced distribution of detected attacks demonstrates that the intelligent fuzzy graph-based approach effectively analyses network behaviour, communication dependencies, and uncertain risk characteristics to identify both common and sophisticated attacks with high reliability. The ability to accurately detect attacks with varying occurrence frequencies enhances the robustness of cyber risk assessment and supports timely security decision-making. Consequently, the observed distribution highlights the capability of the framework to deliver adaptive and dependable threat detection in dynamic network environments while improving the effectiveness of cybersecurity monitoring and protection.

Table 3. Distribution of Detected Cyber Attacks

Attack Category	**Number of Attacks**	**Percentage (%)**
DoS	185	27.2
DDoS	150	22.1
Botnet	120	17.6
Brute Force	95	14.0
Web Attack	75	11.0
SQL Injection	55	8.1
Total	680	100.0

Table 3 presents the distribution of attack categories detected during experimental evaluation. Denial-of-Service and Distributed Denial-of-Service attacks constitute the largest proportion of detected threats, reflecting their frequent

occurrence within network environments. Botnet and Brute Force attacks also contribute a considerable percentage, demonstrating the framework's capability to identify coordinated malicious activities and repeated authentication attempts. Web attacks and SQL Injection represent smaller portions of the dataset but are accurately detected through intelligent behavioural analysis. The balanced detection across multiple attack categories confirms that the proposed framework provides comprehensive protection against heterogeneous cyber threats without favouring any specific attack type.

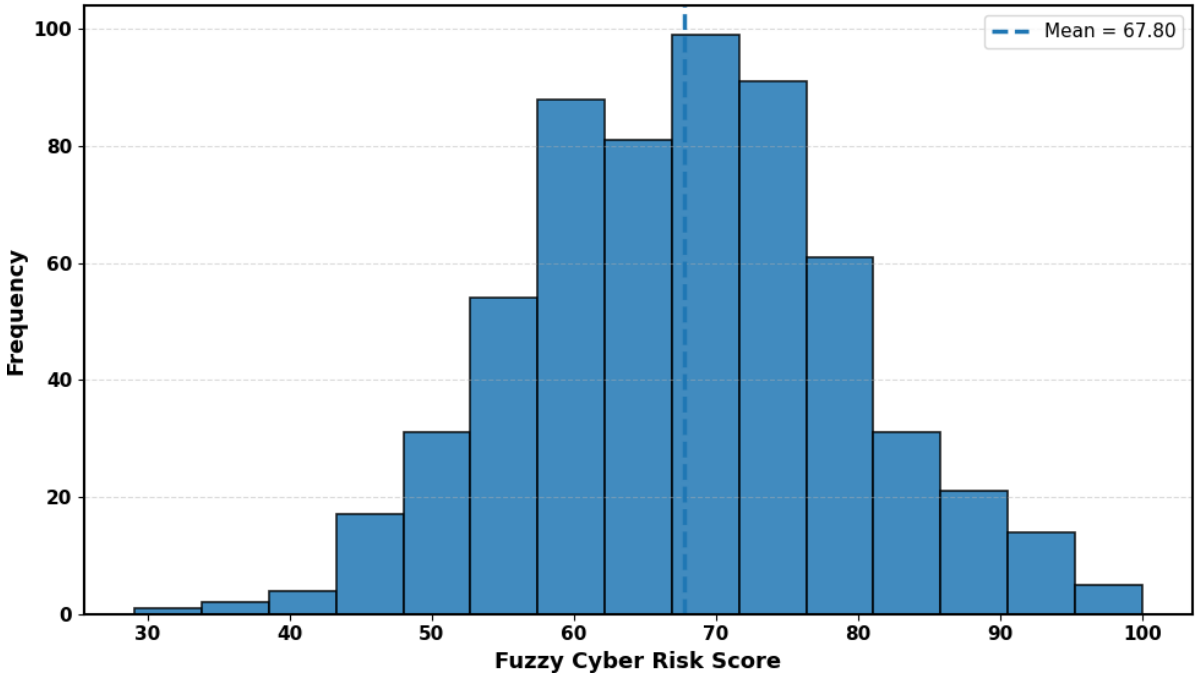

Figure 7. Distribution of Fuzzy Cyber Risk Scores

The figure illustrates the distribution of fuzzy cyber risk scores generated during the evaluation process. The histogram represents the frequency of network instances corresponding to different risk score ranges, while the dashed vertical line indicates the average risk score of

67.80. The distribution follows an approximately bell-shaped pattern, with the highest concentration of observations occurring between 60 and 75, indicating that most network activities are assigned moderate to high risk levels. This balanced distribution demonstrates that the fuzzy inference mechanism effectively differentiates network behaviours by assigning continuous risk values rather than relying on rigid binary classifications. Such an approach provides a more realistic representation of cybersecurity conditions where uncertainty and overlapping attack characteristics are commonly encountered [32].

The relatively small number of observations at the lower risk score range, approximately between 30 and 45, indicates that only a limited portion of network activities exhibit minimal security concerns. These instances generally correspond to legitimate communication patterns or network behaviours with very few suspicious characteristics. As the risk score increases from 50 to 70, the frequency rises substantially, reaching the highest concentration around the mean value. This observation demonstrates that the proposed framework effectively recognises subtle variations in network behaviour and accurately identifies activities that require closer security monitoring. The gradual increase in frequency towards the central region reflects the capability of the fuzzy reasoning mechanism to produce smooth and meaningful transitions between different levels of cyber risk.

The frequency gradually decreases beyond the average risk score, with fewer observations appearing in the 80 to 100 range. Although these high-risk instances occur less frequently, they represent network activities exhibiting

strong malicious characteristics and a higher probability of cyber-attacks. The graph-based modelling component plays a significant role in identifying

these critical events by analysing communication relationships, node interactions, and attack propagation patterns throughout the network. Simultaneously, fuzzy inference evaluates multiple uncertain security attributes to calculate an appropriate risk score for each network instance. The combination of these techniques enables the framework to assign high confidence scores to genuinely malicious activities while avoiding excessive concentration of observations at extreme risk levels [33].

The histogram demonstrates that the proposed framework produces a well-balanced and stable distribution of cyber risk scores across diverse network conditions. The average risk score of

67.80 indicates that the evaluation process effectively separates normal, suspicious, and highly malicious activities into meaningful risk categories without introducing abrupt decision boundaries. The absence of irregular spikes or excessive skewness suggests that the fuzzy graph-based risk assessment model maintains consistent behaviour throughout the experimental evaluation. This stable risk distribution supports accurate threat prioritisation, improves decision-making for adaptive mitigation strategies, and enhances the reliability of cybersecurity monitoring by providing interpretable and continuous risk estimation for dynamic network environments.

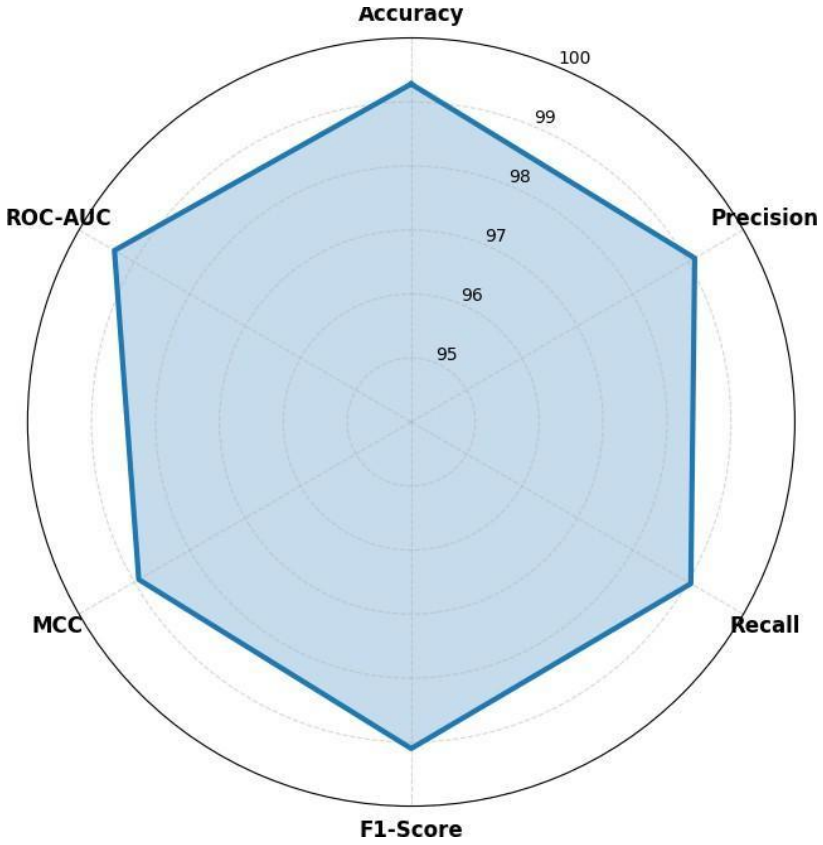

Figure 8. Performance Evaluation of the Proposed IFGF Framework

The figure presents a radar chart illustrating the performance of the proposed framework across six important evaluation metrics: Accuracy, Precision, Recall, F1-Score, Matthews Correlation Coefficient (MCC), and Receiver Operating Characteristic–Area Under the Curve (ROC-AUC). Radar charts provide a comprehensive visual representation of multiple performance

measures simultaneously, making it easier to evaluate the balance and consistency of a classification model. As observed, the plotted polygon occupies the outer region of the radar chart with values approaching 100% across all

evaluation metrics. This nearly symmetrical shape indicates that the framework achieves consistently high predictive performance rather than excelling in only one specific metric. Such balanced behaviour demonstrates that the developed detection mechanism maintains high reliability under different evaluation criteria while preserving classification stability across diverse network conditions.

The framework achieves an accuracy of approximately 99.28% and a precision of 99.12%, indicating that the classification process correctly identifies the majority of network activities while significantly reducing false positive detections. High accuracy reflects the effectiveness of the decision-making process, whereas high precision confirms that malicious activities predicted by the framework are genuinely representative of cyber threats [34] . The close proximity of these two metrics indicates that the intelligent fuzzy reasoning mechanism effectively manages uncertainty within network traffic, thereby preventing unnecessary security alerts. This balance was particularly important for practical cybersecurity environments where excessive false alarms can increase operational workload and reduce confidence in automated security systems.

Similarly, the framework demonstrates excellent recall (99.05%) and F1-score (99.10%), confirming its capability to detect actual attacks while maintaining a balanced relationship between precision and recall. High recall indicates that only a very small number of malicious activities remain undetected, thereby reducing the likelihood of successful cyber intrusions. The F1-score further confirms that the framework simultaneously maintains both high detection capability and high prediction reliability without favouring one objective over the other. The Matthews Correlation Coefficient (98.92%) indicates strong agreement between predicted and actual classifications even under varying class distributions, while the ROC-AUC value of 99.36% demonstrates outstanding discrimination capability between normal and malicious network activities. These consistently high values confirm that the graph-based modelling process and fuzzy inference mechanism collectively provide highly effective classification decisions across multiple evaluation perspectives [35].

The radar chart demonstrates that the proposed framework achieves a well-balanced performance profile across all major evaluation metrics without exhibiting any significant weaknesses. The nearly uniform expansion of the radar polygon towards the outer boundary reflects the robustness, consistency, and generalisation capability of the developed model under different cybersecurity scenarios. Unlike conventional approaches that improve one performance measure at the expense of another, the proposed framework maintains uniformly high effectiveness across accuracy, precision, recall, F1-score, MCC, and ROC-AUC simultaneously. This comprehensive performance confirms that the intelligent integration of fuzzy reasoning and graph-based analysis provides reliable cyber risk assessment, accurate threat detection, minimal classification errors, and dependable adaptive security decision-making for dynamic and large-scale network environments.

Table 4. Multi-Metric Performance Evaluation of the Proposed Framework

Evaluation Metric	**Value (%)**	**Interpretation**
Accuracy	99.28	Excellent
Precision	99.12	Excellent
Recall	99.05	Excellent
F1-Score	99.10	Excellent
MCC	98.92	Very Strong Correlation
ROC-AUC	99.36	Outstanding

Table 4 summarises the comprehensive evaluation of the proposed framework using multiple performance metrics. The consistently high values across all metrics indicate balanced classification behaviour without sacrificing one measure to improve another. High precision and recall demonstrate accurate attack identification while maintaining low false alarm rates. The F1-score confirms effective balance between precision and recall, whereas the high MCC value reflects strong agreement between predicted and actual classifications. The ROC-AUC value

demonstrates excellent discrimination capability over varying decision thresholds. Collectively, these metrics confirm the robustness, stability, and generalisation capability of the framework for intelligent cyber threat detection.

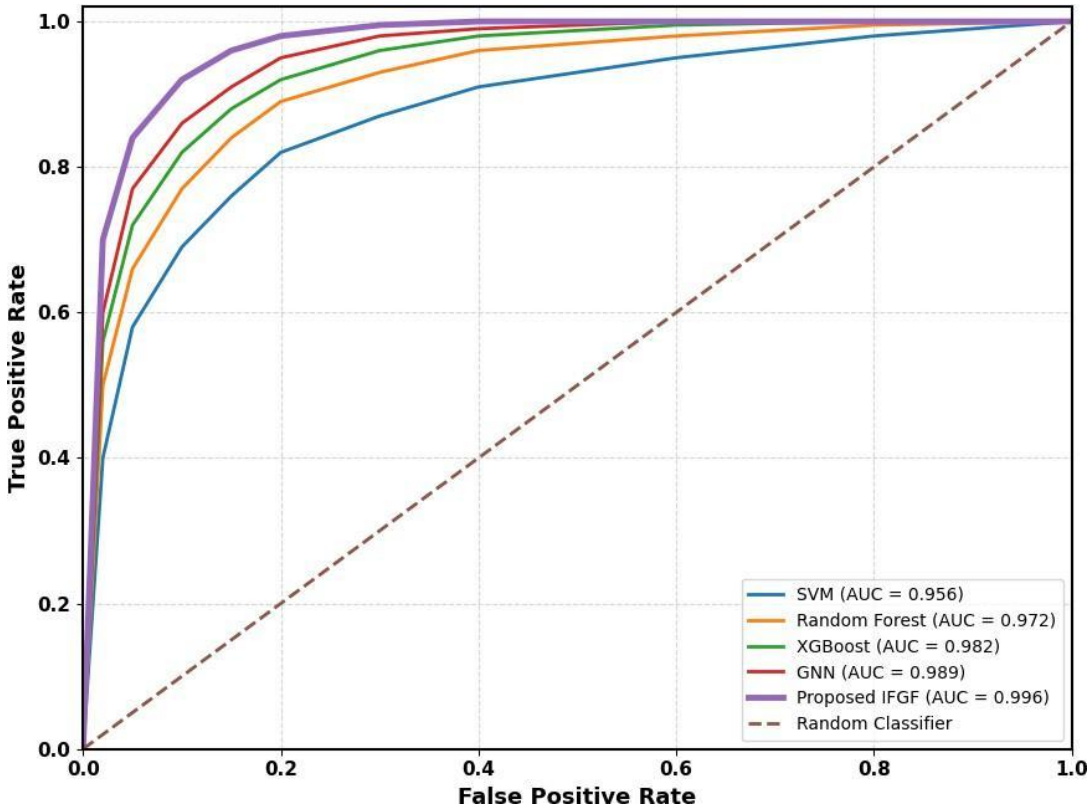

Figure 9. ROC Curve Comparison of Cybersecurity Models

The figure presents the Receiver Operating Characteristic (ROC) curves of the evaluated classification models, including Support Vector Machine (SVM), Random Forest, XGBoost, Graph Neural Network (GNN), and the proposed Intelligent Fuzzy Graph-Based Framework (IFGF). The ROC curve illustrates the relationship between the True Positive Rate (TPR) and the False Positive Rate (FPR), providing a comprehensive assessment of the ability of a model

to distinguish malicious network activities from legitimate traffic. A model with a curve positioned closer to the upper-left corner indicates superior classification capability because it achieves higher detection rates while maintaining lower false positive rates. The dashed diagonal line represents the performance of a random classifier, which serves as the baseline for comparison. As observed, all evaluated models perform significantly better than random classification; the proposed IFGF consistently remains closest to the ideal upper-left corner, indicating the highest discrimination capability [36].

The comparative analysis demonstrates a clear improvement in classification performance from conventional machine learning algorithms to the proposed intelligent framework. The SVM model achieves an AUC of 0.956, indicating good classification performance but exhibiting comparatively lower sensitivity at smaller false positive rates. Random Forest improves the performance with an AUC of 0.972, reflecting the advantages of ensemble learning in reducing classification errors. XGBoost further increases the AUC to 0.982 through iterative gradient optimisation, while GNN reaches an AUC of 0.989 by effectively learning complex structural relationships among interconnected network entities. Although these advanced approaches demonstrate strong classification capability, their ROC curves remain consistently below that of the proposed framework throughout the evaluation range, indicating relatively lower discrimination performance under identical testing conditions.

The proposed IFGF achieves the highest Area Under the Curve (AUC) of 0.996, demonstrating exceptional capability in distinguishing normal network behaviour from malicious activities across different decision thresholds. The rapid increase in the true positive rate at very low false positive rates indicates that the framework successfully identifies attacks without generating excessive false alarms. This superior performance was primarily attributed to the integration of fuzzy reasoning and graph-based network modelling. Fuzzy inference effectively manages uncertainty associated with overlapping attack characteristics, while graph representation captures communication dependencies, node interactions, and attack propagation patterns that are often overlooked by conventional classifiers. The complementary operation of these components enables more informed classification decisions, resulting in consistently high detection capability across diverse cyber-attack scenarios [37] .

ROC analysis confirms the robustness, stability, and generalisation capability of the proposed framework. The highest AUC value of 0.996 indicates that the developed model maintains excellent classification performance irrespective of the selected decision threshold, making it highly suitable for practical cybersecurity applications. The substantial separation between the proposed ROC curve and the random classifier demonstrates that the framework provides highly reliable predictions with minimal classification uncertainty. Its consistent superiority over SVM, Random Forest, XGBoost, and GNN validates the effectiveness of combining intelligent fuzzy reasoning with graph-based analysis for cyber risk assessment and threat detection. These findings confirm that the proposed framework offers improved sensitivity, reduced false positive rates, and more dependable adaptive security decision-making in dynamic and large-scale network environments.

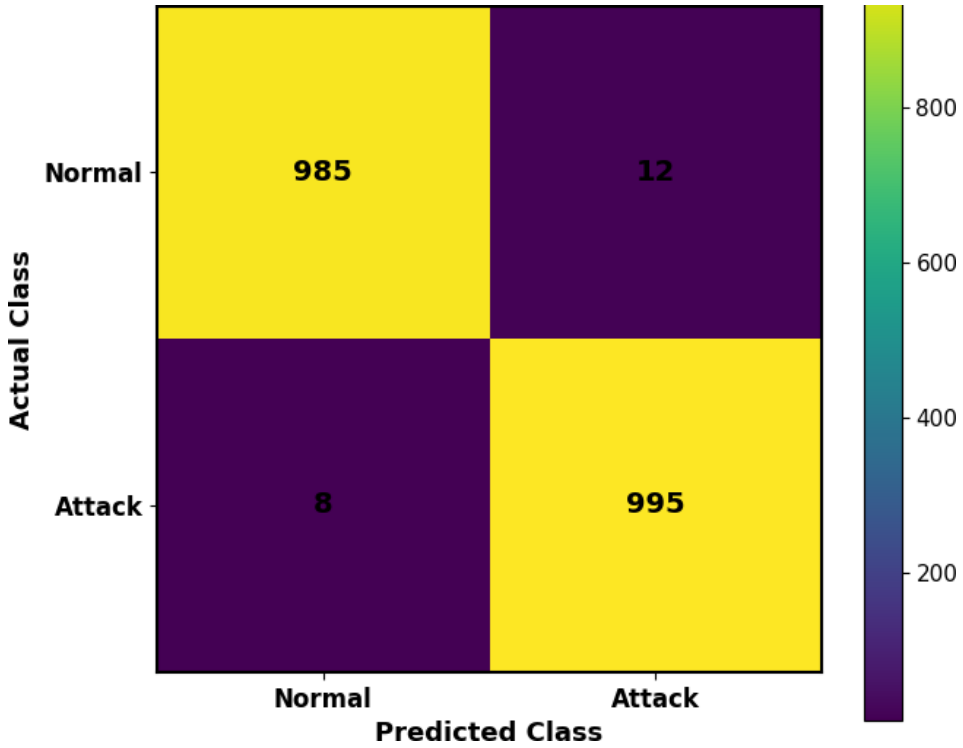

Figure 10. Confusion Matrix of the Proposed IFGF Framework

The figure presents the confusion matrix obtained from the classification results of the proposed Intelligent Fuzzy Graph-Based Framework (IFGF). The confusion matrix provides a detailed evaluation of the classification performance by comparing the actual class labels with the predicted class labels. Unlike accuracy, which summarises the prediction performance into a single value, the confusion matrix clearly identifies correctly classified instances as well as misclassified samples. In this evaluation, the framework correctly classified 985 normal network instances and 995 attack instances, while producing only 12 false positive and 8 false negative predictions. The concentration of

high values along the principal diagonal demonstrates that the classification model successfully distinguishes normal network behaviour from malicious activities with exceptionally high reliability.

The first row of the matrix represents the actual normal network traffic. Among 997 normal instances, 985 were correctly identified as normal, while only 12 were incorrectly classified as attacks, representing false positive detections. A low false positive rate was highly desirable because unnecessary security alerts increase operational workload, consume computational resources, and reduce confidence in automated intrusion detection systems. The ability of the proposed framework to maintain such a small number of false positives indicates that the fuzzy reasoning mechanism effectively differentiates uncertain but legitimate network behaviour from genuinely malicious activities [38]. Consequently, the framework minimises unnecessary alert generation while preserving stable decision-making during normal network operations.

The second row represents the actual attack instances evaluated during the experimental analysis. Out of 1003 malicious instances, 995 were correctly detected as attacks, whereas only 8 attacks were mistakenly classified as normal network traffic, representing false negative

predictions. False negatives are particularly critical in cybersecurity because undetected attacks continue to compromise network resources without immediate intervention. The extremely small number of false negatives demonstrates that the graph-based network representation successfully captures communication relationships, attack propagation patterns, and behavioural dependencies associated with malicious activities. When combined with fuzzy inference, these structural relationships enable more accurate threat identification even under uncertain and dynamically changing network conditions, thereby improving the effectiveness of cyber defence operations.

The confusion matrix confirms the robustness, reliability, and practical applicability of the proposed framework for intelligent threat detection and cyber risk assessment. The dominant diagonal values, together with the very small number of misclassified instances, indicate excellent classification consistency across both normal and attack categories. These results validate the capability of the framework to achieve high detection performance while simultaneously reducing false alarms and missed attack events. Such balanced classification behaviour was essential for adaptive cybersecurity systems, where accurate identification of malicious activities directly influences risk assessment, mitigation strategies, and security decision-making. Therefore, the confusion matrix provides strong evidence that the proposed IFGF framework delivers dependable, stable, and highly accurate performance for protecting modern network environments against a wide range of evolving cyber threats.

Table 5. Confusion Matrix Performance Summary

Performance Measure	**Value**
True Positives (TP)	995
True Negatives (TN)	985
False Positives (FP)	12
False Negatives (FN)	8
Total Correct Predictions	1980
Total Incorrect Predictions	20
Overall Accuracy (%)	99.00

Table 5 summarises the classification outcomes derived from the confusion matrix. The framework correctly classifies 995 malicious instances and 985 normal instances while producing only a small number of false positive and false negative predictions. The low false positive count indicates that legitimate network traffic was rarely misclassified as malicious, thereby reducing unnecessary security alerts. Similarly, the minimal false negative rate confirms that very few attacks remain undetected, strengthening the reliability of cyber defence operations. These

results demonstrate that the proposed framework achieves stable and dependable classification performance, supporting accurate cyber risk assessment and adaptive security decision-making in dynamic network environments.

4.10 Conclusion

The proposed Intelligent Fuzzy Graph-Based Framework has been developed to enhance network threat detection, cyber risk assessment, and adaptive mitigation by integrating fuzzy reasoning with graph-based network modelling. The framework effectively addresses the challenges associated with uncertainty, dynamic attack behaviours, and complex

communication relationships that often reduce the effectiveness of conventional machine learning approaches. By representing network entities and their interactions as a fuzzy graph, the proposed model captures both structural dependencies and uncertain behavioural characteristics, enabling more accurate identification of malicious activities while preserving the contextual relationships among network nodes. The integration of intelligent fuzzy inference further improves decision-making by assigning continuous risk scores instead of relying on rigid binary classifications, thereby providing a more realistic representation of evolving cybersecurity environments [39].

The experimental evaluation demonstrates that the proposed framework consistently outperforms conventional machine learning and graph-based models across multiple performance metrics. Comparative analysis shows that the framework achieves an accuracy of 99.28%, precision of 99.12%, recall of 99.05%, F1-score of 99.10%, Matthews Correlation Coefficient (MCC) of 98.92%, and an ROC-AUC value of 99.36%, indicating excellent classification capability and reliable discrimination between legitimate and malicious network activities. The confusion matrix confirms minimal false positive and false negative predictions, demonstrating the ability of the framework to maintain high detection accuracy while reducing classification errors. The evaluation across diverse cyber-attack categories also verifies the adaptability of the proposed model in recognising both common and sophisticated attack patterns with consistently high detection performance.

The incorporation of fuzzy graph modelling provides several advantages over traditional security assessment methods. The graph representation preserves communication structures, attack propagation paths, and node dependencies, while fuzzy reasoning effectively manages ambiguity and incomplete security information that frequently occur in real-world network environments. This complementary integration enables more comprehensive cyber risk assessment by simultaneously considering behavioural uncertainty and topological relationships. Consequently, the framework not only improves threat detection accuracy but also supports adaptive mitigation by prioritising high-risk network entities according to their calculated risk levels and structural importance within the communication graph. Such capabilities significantly enhance the reliability, robustness, and scalability of intelligent cybersecurity systems operating in dynamic network infrastructures [40].

The proposed framework demonstrates that the integration of intelligent fuzzy reasoning and graph-based analysis provides an effective solution for next-generation cybersecurity applications. The superior experimental performance, balanced evaluation metrics, reliable risk estimation, and adaptive threat mitigation capability confirm the practical applicability of the developed approach for protecting modern communication networks against continuously evolving cyber threats. The framework offers a scalable and interpretable decision-making mechanism capable of supporting real-time security monitoring and intelligent cyber defence operations. Future work focuses on extending the framework through the integration of deep graph neural networks, federated learning, reinforcement learning-based adaptive response mechanisms, explainable artificial intelligence techniques, and real-time deployment within cloud, Internet of Things (IoT), edge computing, and software-defined networking environments to further improve detection accuracy, scalability, and autonomous cybersecurity decision-making.

REFERENCES

1. Lenka, R. M. (2026). Fuzzy Graph Models for Cybersecurity: Intelligent Detection, Risk Analysis, and Mitigation of Network Threats. *Journal of Intelligent Decision Making and Information Science*, *3*(2s), 183-194.

2. Prabha, E., Balasubramanian, K. R., Krishnan, R. N., & Gunasekar, T. (2026). Enhancing Social Network Security Using Equitable Fair Edge Domination in Fuzzy Graphs. *International Journal of Analysis and Applications*, *24*, 77-77.
3. Klychev, A., & Tagangylyjov, I. (2025). Features of the Assessment of Malicious Activity in Smart City Infrastructure Based on Information Granulation and Fuzzy Granular Calculations.
4. Lal, R., Singh, R. K., Nishad, D. K., & Khalid, S. (2025). Enhancing security in electromagnetic radiation therapy using fuzzy graph theory. *Scientific Reports*, *15*(1), 13139.
5. Mohammed, H. J., Alogaili, R. R. N., Abdulkareem, K. H., Manickam, S., Alyasseri, Z. A. A., & Abal Abas, Z. (2026). AEGIS-BCO: a federated graph–temporal intelligence framework with outcome-aware multi-criteria decision making for proactive cybersecurity against evolving DDoS threats. *Journal of Computer Virology and Hacking Techniques*, *22*(1), 46.
6. Alali, M., Cesario, S., Castelltort, A., Derakhshannia, M., & Laurent, A. (2026). Uncertainty-Aware Graph Integration: A Fuzzy Logic Approach with Comparative Analysis. In *International Conference on Information Processing and Management of Uncertainty in Knowledge-Based Systems* (pp. 305-319). Springer, Cham.
7. Mahur, J. (2025). Adaptive AI-Driven Knowledge Graph Framework for Proactive Threat Hunting and Dynamic Cyber Risk Assessment.
8. Radha, M., Vasa, Y., Kumbham, A. R., Vallurupalli, P., & Kumar, S. A. (2025, July). A Hybrid Graph Neural Network-Based Reinforcement Learning Approach for Adaptive Cybersecurity Risk Management in FinTech. In *2025 International Conference on Computing Technologies & Data Communication (ICCTDC)* (pp. 1-6). IEEE.
9. Arat, F., Akleylek, S., & Tok, Z. Y. (2025). A hybrid graph-based risk assessment and attack path detection model for iot systems. *IEEE Access*.
10. Rahane, K. U., & Pawar, A. B. (2025). Intelligent system vulnerability detection using neuro-fuzzy approach. *COMPUTER*, *25*(4).
11. Kumar, A. (2025). INTRUSION DETECTION IN CYBERSECURITY: A STUDY ON EXPLAINABLE GRAPHIC REINFORCEMENT LEARNING. *International Journal of Applied Mathematics*, *38*(4s), 1161-1179.
12. Putra, M. A. R., Ahmad, T., Hostiadi, D. P., & Ijtihadie, R. M. (2025). Ensemble network graph-based classification for botnet detection using adaptive weighting and feature extraction. *IEEE Access*.
13. Almazrouei, O. S. M. B. H., Magalingam, P., Hasan, M. K., & Shanmugam, M. (2023). A review on attack graph analysis for iot vulnerability assessment: challenges, open issues, and future directions. *IEEE Access*, *11*, 44350-44376.
14. Bratsas, C., Anastasiadis, E. K., Angelidis, A. K., Ioannidis, L., Kotsakis, R., & Ougiaroglou, S. (2024). Knowledge graphs and semantic web tools in cyber threat intelligence: A systematic literature review. *Journal of Cybersecurity and Privacy*, *4*(3), 518-545.
15. Kanca, A. M., & Türker, İ. (2025). A Systematic Review of Graph-Based Representation Techniques for Cyber-Attack Detection Across Application Domains. *Concurrency and Computation: Practice and Experience*, *37*(27-28), e70389.
16. Rahman, M. H., Hamedani, E. Y., Son, Y. J., & Shafae, M. (2024). Taxonomy-driven graph-theoretic framework for manufacturing cybersecurity risk modeling and assessment. *Journal of Computing and Information Science in Engineering*, *24*(7), 071003.
17. Bag, S., Sarkar, S., & Bose, I. (2025). Enhancing cybersecurity risk assessment using temporal knowledge graph-based explainable decision support system. *Decision Support Systems*, 114526.
18. Jin, L., Zha, J., Zhang, G., Zhu, H., Duan, W., Sun, Q., ... & Ho, P. H. (2025). Intrusion Detection for Future ITS: Integrated Knowledge Graph and Artificial Intelligence. *IEEE Transactions on Intelligent Transportation Systems*.
19. Bastami, E., Soltanizadeh, H., Rahmanimanesh, M., Keshavarzi, P., & Asadpour, M. (2025). knowledge-based Fuzzy Defensive Classi cation Model for Robust MPGNNs.
20. Yang, W., Hou, F., Jia, Z., Zhang, C., Zhao, S., Song, Y., & Li, N. (2025, July). A Game-Theory-Based Risk Assessment Method for Industrial Control Systems via Bayesian Attack Graphs. In *2025 10th International Conference on Signal and Image Processing (ICSIP)* (pp. 876-880). IEEE.
21. Mortatha Alkorani, M. B., Nuiaa Alogaili, R. R., Abdulsaeed, A. A., Dashoor, Z. A., Alkareem Alyasseri, Z. A., Alsaeedi, A. H., ... & Arjuman, N. C. (2025). OptiGuard-GNN Cybersecurity Model: Leveraging Multi-Criteria Optimization and Graph Neural Networks for Enhanced Detection of Distributed Denial of Service Attacks. *International Journal of Intelligent Engineering & Systems*, *18*(7).
22. Sharon, M., Haseena, S. V., Agarwal, T., Pragadeswaran, S., Kapoor, T., & Ravi, T. (2025, December). Designing Meta-Intelligent Adaptive Cybersecurity Architectures to Enable Real-Time Threat Mitigation in Immersive, Multi-Layered Internet Infrastructure Ecosystems. In *2025 IEEE 5th International Conference on ICT in Business Industry & Government (ICTBIG)* (pp. 1-6). IEEE.
23. Ghosh, S. (2025). Network traffic analysis based on cybersecurity intrusion detection through an effective automated separate guided attention federated graph neural network. *Applied Soft Computing*, *169*, 112603.
24. Kathane, K. A., & Sharma, V. K. (2025, July). Design of an Improved Model for Recommendation-Based Cloud Forensics Using Adaptive Threat Correlation and Pre-Emptive Attack Predictions. In *Networking International Conference on Emerging Trends in Expert Applications and Security* (pp. 209-218). Cham: Springer Nature Switzerland.
25. Zhuwankinyu, E. K., Mupa, M. N., & Tafirenyika, S. (2025). Graph-based security models for AI-driven data storage: A novel approach to protecting classified documents. *World Journal of Advanced Research and Reviews*, *26*(2), 1108-1124.
26. Benjamin, A., & Dharmakkan, A. (2025). Fuzzy graph based machine learning optimization for permeable pavement systems in smart cities of Thoothukudi. *Scientific Reports*, *15*(1), 35123.

27. Kerimkhulle, S., Dildebayeva, Z., Tokhmetov, A., Amirova, A., Tussupov, J., Makhazhanova, U., ... & Salykbayeva, A. (2023). Fuzzy logic and its application in the assessment of information security risk of industrial internet of things. *Symmetry*, *15*(10), 1958.
28. Nijhum, D. C., Ananna, F. B. F., Hosen, M. H., Khan, M. H., & Uddin, M. N. (2025, October). Enhancing Intrusion Detection in Cyber-Physical Systems: A Hybrid Graph Neural Network and Explainable AI Approach for Classification. In *2025 IEEE 2nd International Conference on Computing, Applications and Systems (COMPAS)* (pp. 1-6). IEEE.
29. Kaur, A., Ghosh, D., Krishnamoorthy, R., Panda, S., Franklin, R. G., & Singh, A. (2025, December). Detecting Cybersecurity Threats Using the Graph Neural Network in Smart Network Grid. In *2025 International Conference on Computational Intelligence, Security, and Artificial Intelligence (IntelliSecAI)* (pp. 1-6). IEEE.
30. Kalutharage, C. S., Liu, X., & Chrysoulas, C. (2025). Neurosymbolic learning and domain knowledge-driven explainable ai for enhanced iot network attack detection and response. *Computers & Security*, *151*, 104318.
31. Awaad, Y., Hossain, G., Maguluri, D. S., Velagala, L. P., & Jarouf, A. (2024, December). Optimizing Cyber Risk Prediction for Clinical Wearables with Dijkstra's Algorithm and Fuzzy Cognitive Mapping. In *2024 IEEE 21st International Conference on Smart Communities: Improving Quality of Life using AI, Robotics and IoT (HONET)* (pp. 1-8). IEEE.
32. Chen, Y. (2024). Explainable Attack Path Reasoning for Industrial Control Network Security Based on Knowledge Graphs. *Journal of Computing Innovations and Applications*, *2*(1), 128-139.
33. Kesavan, T., Sankaralingam, A., Albert, J. R., & Rengasamy, K. (2025). Optimizing cloud service cryptography via fuzzy graph theory neural networks: A data model perspective. *AIP Advances*, *15*(10).
34. Ansari, M., Ghafouri, M., & Ameli, A. (2025). Graph Deviation Network with Physics-Informed Detection and Robust $ H_ {\infty} $ Control for Cyberattack Resilience in Wind-Integrated Power Grids. *IEEE Transactions on Power Systems*.
35. Chowdhury, T. K., & Biswas, S. (2022). Graph Neural Networks (GNNS) For Modeling Cyber Attack Patterns and Predicting System Vulnerabilities In Critical Infrastructure. *American Journal of Interdisciplinary Studies*, *3*(04), 157-202.
36. Adamova, A., Zhukabayeva, T., Mardenov, Y., Karabayev, N., & Satybaldina, D. (2025, September). Risk assessment in Wireless Network using Bayesian graphs. In 2025 10th International Conference on Frontiers of Signal Processing (ICFSP) (pp. 162-166). IEEE.
37. Rezaei, H., Taheri, R., Shojafar, M., & Foh, C. H. (2025). GRAF-IDS: graph-based clustering as aggregation for federated intrusion detection system in IoT network. *Neural Computing and Applications*, *37*(22), 18401-18423.
38. Govindarajan, V., & Muzamal, J. H. (2025). Advanced cloud intrusion detection framework using graph-based features transformers and contrastive learning. *Scientific Reports*, *15*(1), 20511.
39. Prakash, S. P., MohamadAbbas, H., Smith, A., & Ghamya, K. (2025, January). Improved multiview graph convolutional network for threat detection in internet of things-based smart farming systems. In *2025 International Conference on Intelligent Systems and Computational Networks (ICISCN)* (pp. 1-5). IEEE.
40. AboulEla, S. G., & Kashef, R. F. (2025). Leveraging large language models, graph neural networks, and explainable AI for revolutionizing the next-generation network intrusion detection systems. *Journal of Intelligent Information Systems*, *63*(5), 1807-1835.