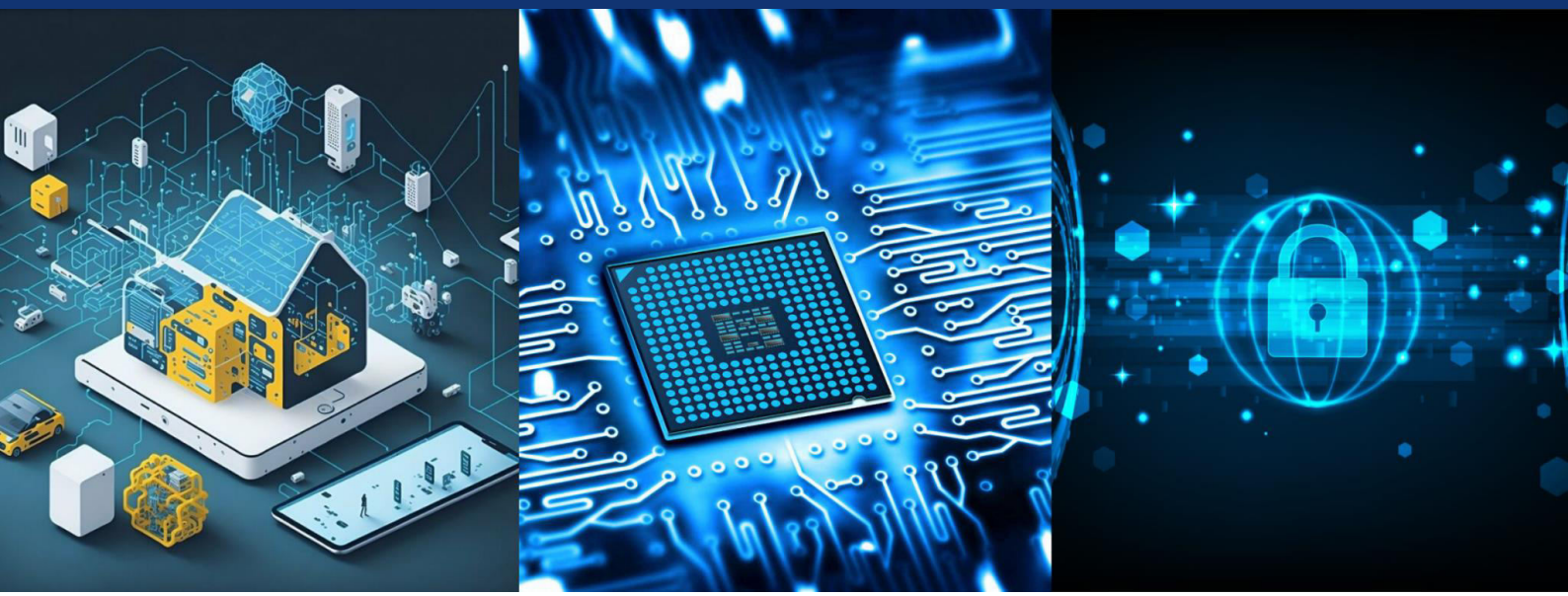
IJIRCCE

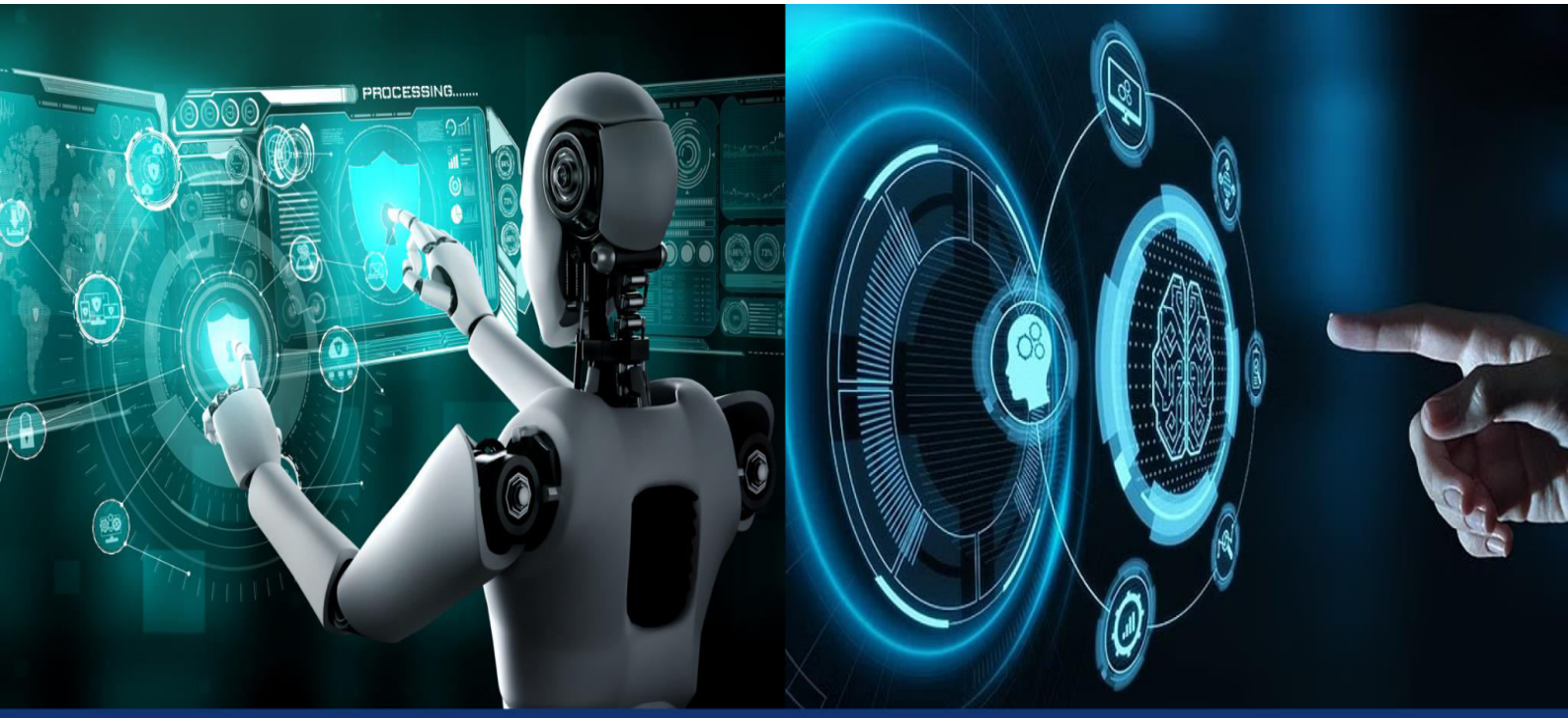
ISSN(O): 2320-9801

ISSN(P): 2320-9798



International Journal of Innovative Research in Computer and Communication Engineering

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 9.927

Volume 14, Issue 7, July 2026

© 2026 IJIRCCE | Volume 14, Issue 7, July 2026 DOI: 10.15680/IJIRCCE.2026.1407030

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Detecting Malicious Nodes Using Game Theory and Reinforcement Learning in Software-Defined Networks

K V Lakshmi Priya, Dr. M. Dhanalakshmi

Post Graduate Student, Department of Computer Science and Engineering, Computer Networks and Information Security, Jawaharlal Nehru Technological University, Hyderabad, India

Professor, Department of Computer Science and Engineering, Jawaharlal Nehru Technological University, Hyderabad, India

ABSTRACT: Software-Defined Networking (SDN) has become a widely adopted networking paradigm due to its centralized management and enhanced flexibility. However, the centralized architecture of SDN makes it susceptible to security threats such as malicious nodes and botnet attacks, which can negatively impact network performance, availability, and reliability. Conventional intrusion detection techniques often depend on predefined signatures and static rules, limiting their ability to detect sophisticated and emerging cyber threats. To overcome these limitations, this study presents a Mafia Game-Based Malicious Node Detection Framework that utilizes role-based modeling, where network entities are represented as roles including Godfather, Mafia, Detective, Doctor, and Townie for effective behavioral analysis and trust assessment.

The proposed framework integrates belief-based evaluation mechanisms with Reinforcement Learning (RL) to detect, prioritize, and classify malicious nodes within the SDN environment. By continuously learning from network interactions and previous outcomes, the RL agent enhances the adaptability and accuracy of the detection process. The performance of the framework is assessed using standard evaluation metrics such as Accuracy, Precision, Recall, F1-Score, True Positive Rate (TPR), and True Negative Rate (TNR). Experimental findings indicate that the proposed method effectively identifies malicious activities and strengthens overall network security. The framework offers an intelligent, adaptive, and scalable approach for safeguarding modern Software-Defined Networks.

KEYWORDS: Software-Defined Networking (SDN), Malicious Node Detection, Game Theory, Botnet Detection, Intrusion Detection System (IDS), Network Security.

I. INTRODUCTION

Software-Defined Networking (SDN) has emerged as a modern networking approach that simplifies network management by separating the control plane from the data plane. This architecture enables centralized control, improved flexibility, and efficient resource management, making SDN widely adopted in cloud computing, data centers, enterprise networks, and other large-scale communication environments. The ability to dynamically configure and monitor network operations has made SDN an important technology for supporting the growing demands of modern digital infrastructure.

Although SDN offers several advantages, its centralized nature also introduces significant security concerns. Malicious nodes, compromised hosts, and botnet-based attacks can exploit network vulnerabilities, disrupt normal communication, and reduce overall network performance. These attacks often imitate legitimate network behavior, making them difficult to detect using traditional intrusion detection systems. Most existing security solutions rely on predefined signatures or fixed rules, which limits their ability to identify new and evolving threats in dynamic network environments.

To address these challenges, this paper proposes a Mafia Game-Based Malicious Node Detection Framework that combines Game Theory and Reinforcement Learning for intelligent threat detection in Software-Defined Networks. The proposed system models network entities using Mafia game roles such as Godfather, Mafia, Detective, Doctor, Proof, and Townie to analyze trust relationships and behavioral patterns. Belief functions are used to evaluate node activities

© 2026 IJIRCCE | Volume 14, Issue 7, July 2026 DOI: 10.15680/IJIRCCE.2026.1407030

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

and rank suspicious nodes, while a Reinforcement Learning agent continuously improves detection decisions based on previous interactions and outcomes. Experimental results demonstrate that the proposed framework effectively detects malicious nodes and enhances the security, reliability, and resilience of SDN environments.

II. RELATED WORK

Software-Defined Networking (SDN) has become a popular networking architecture because of its centralized control and flexible management capabilities. However, the increasing use of SDN has also raised concerns regarding network security, particularly malicious node attacks, botnet activities, and unauthorized intrusions. To address these issues, researchers have proposed several detection techniques based on machine learning, deep learning, and SDN traffic analysis. These approaches focus on identifying abnormal network behavior and improving attack detection accuracy. Although many of these methods have shown promising results, most of them rely heavily on traffic patterns and historical data, making it difficult to detect sophisticated and continuously evolving threats.

Recent studies have explored the application of Game Theory and Reinforcement Learning to enhance cybersecurity in SDN environments. Game-theoretic models help analyze the strategic interactions between attackers and defenders, while Reinforcement Learning enables systems to learn from network behavior and adapt their detection strategies over time. Despite these advancements, many existing solutions lack an effective mechanism for evaluating trust relationships among network nodes and accurately identifying malicious entities. To overcome these limitations, the proposed framework integrates Mafia game-based role modeling, belief function analysis, node ranking strategies, and Reinforcement Learning. This combination provides an intelligent and adaptive approach for detecting malicious nodes and strengthening security in Software-Defined Networks.

III. PROPOSED ALGORITHM

A. *System Architecture:*

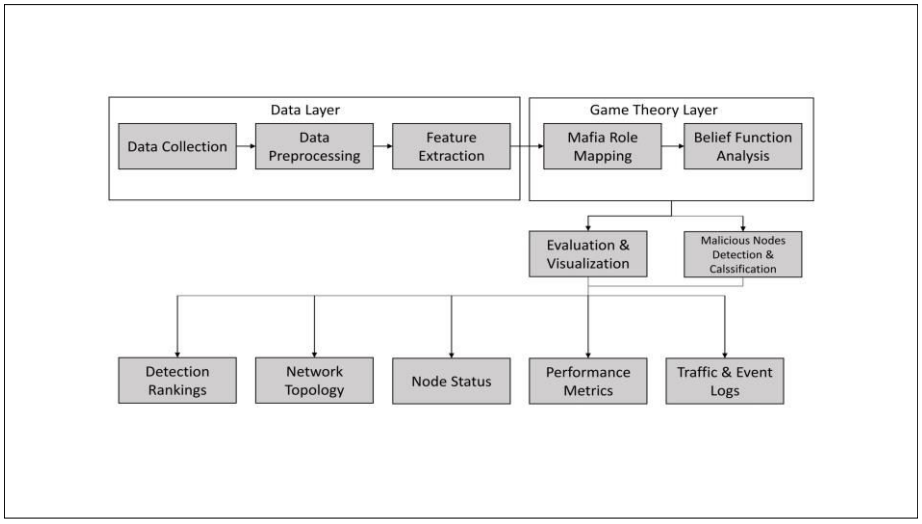


Fig. 1. Proposed System Architecture

B. *Design Considerations:*

- The malicious node detection model is developed and evaluated using Software-Defined Network (SDN) traffic and node behavior data.
- The dataset contains both legitimate and malicious node activities, including botnet behavior and compromised network entities.
- Data preprocessing is performed to remove missing values, duplicate records, and irrelevant attributes that may affect detection performance.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

- Behavioral features, trust indicators, and network interaction patterns are extracted to improve malicious node classification accuracy.
- Belief Function Analysis is employed to evaluate trust relationships and identify suspicious node behavior.
- Linear Ranking Strategy is used to prioritize nodes according to their likelihood of being malicious..
- Reinforcement Learning is integrated to continuously learn from network interactions and improve detection decisions over time.
- The framework is designed to provide real-time monitoring, malicious node detection, and visualization through an interactive Streamlit dashboard.

C. *Description of the Proposed Algorithm:*

The proposed framework aims to accurately identify malicious nodes in Software-Defined Networks using a combination of Game Theory, Belief Function Analysis, and Reinforcement Learning. The detection process consists of five major stages.

Step 1: Data Collection and Preprocessing:

Network traffic information and node activity records are collected from the SDN environment. Missing values, duplicate records, and irrelevant attributes are removed to improve data quality.

Let,

$D = \{x_1, x_2, x_3, ..., x_n\}$

where D represents the preprocessed network dataset containing n node activity records.

Step 2: Mafia Role Mapping:

Network entities are modeled using Mafia game roles to represent different behaviors within the network.

Role = {Godfather, Cultafia, Mafia, Detective, Doctor, Proof, Townie} Eq. (1)

This role-based representation helps analyze relationships among network nodes and supports strategic decision-making.

Step 3: Belief Function Analysis:

The system computes belief values based on node behavior, communication patterns, and trust indicators.

$\text{Belief Score} = B(\text{Node}_i)$ Eq. (2)

where $B(\text{Node}_i)$ represents the trust score assigned to node i.

Nodes exhibiting abnormal behavior receive lower trust scores and are marked as suspicious.

Step 4: Node Ranking and Reinforcement Learning:

The framework ranks nodes according to their belief scores and behavioral characteristics.

$\text{Rank}(\text{Node}_i) = f(\text{Belief Score, Behavior Metrics})$ Eq. (3)

A Reinforcement Learning agent continuously learns from previous detection outcomes and updates its decision policy to improve future detection accuracy.

Step5: Malicious Node Detection:

Based on ranking results and learned policies, the system classifies nodes as either legitimate or malicious.

$\text{Detection Status} = RL(\text{Node}_i)$ Eq. (4)

If Detection Status = 0 → Legitimate Node

If Detection Status = 1 → Malicious Node

The detected malicious nodes are displayed through the monitoring dashboard along with trust scores, rankings, and performance metrics. This adaptive approach improves detection accuracy, strengthens network security, and enhances the resilience of Software-Defined Networks against evolving cyber threats.

IV. PSEUDO CODE

Step 1: Load the SDN dataset containing both legitimate and malicious node activity records.

Step 2: Perform data preprocessing by:

• Removing missing and duplicate values.

• Eliminating irrelevant features.

• Handling inconsistent records.

• Normalizing selected features for improved analysis.

Step 3: Separate the dataset into input features (X) and target labels (Y).

Step 4: Split the dataset into training and testing datasets.

Step 5: Extract behavioral features and trust indicators required for malicious node detection.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Step 6: Assign Mafia game roles to network entities:
• Godfather
• Cultafia
• Mafia
• Detective
• Doctor
• Proof
• Townie
Step 7: Compute belief scores based on node behavior, communication patterns, and trust relationships.
Step 8: Apply a linear ranking strategy to rank nodes according to their level of suspicion.
Step 9: Initialize the Reinforcement Learning (RL) agent with suitable learning parameters.
Step 10: Train the RL agent using network interactions and historical detection outcomes.
Step 11: Evaluate node behavior using belief scores, rankings, and RL policies.
Step 12: Classify network nodes.
IF Node Status = Legitimate
    Display "Normal Network Node"
    Continue Monitoring
ELSE
    Display "Malicious Node Detected"
    Proceed to Security Analysis
Step 13: Identify the malicious node category.
IF Behavior corresponds to Botnet Activity
    Node Type ← Botnet Node
ELSE IF Behavior corresponds to Compromised Host
    Node Type ← Compromised Node
ELSE
    Node Type ← Suspicious Node
Step 14: Generate appropriate security actions such as:
• Node Isolation
• Traffic Blocking
• Access Restriction
• Trust Score Reduction
• Security Alert Generation
Step 15: Calculate performance metrics such as:
• Accuracy
• Precision
• Recall
• F1-Score
• True Positive Rate (TPR)
• True Negative Rate (TNR)
Step 16: Display node rankings, detection results, security alerts, and performance metrics on the Streamlit dashboard.
Step 17: Store detection results for future analysis and model improvement.
Step 18: Continue monitoring network activities for new malicious behavior.
Step 19: Update RL policy based on new observations and feedback.
Step 20: End.

V. SIMULATION RESULTS

The proposed Mafia Game-Based Malicious Node Detection Framework was implemented using Python and evaluated using Software-Defined Network (SDN) datasets containing both legitimate and malicious node activities. The collected data was preprocessed and analyzed using belief-based behavioral analysis, node ranking mechanisms, and Reinforcement Learning techniques. The framework was trained and tested to accurately distinguish malicious nodes from legitimate network entities. Performance evaluation was carried out using standard metrics such as Accuracy, Precision, Recall, F1-Score, True Positive Rate (TPR), and True Negative Rate (TNR). Experimental results indicate that

© 2026 IJIRCCE | Volume 14, Issue 7, July 2026 DOI: 10.15680/IJIRCCE.2026.1407030

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

the proposed framework achieved high detection accuracy while maintaining low false positive and false negative rates, demonstrating its effectiveness in identifying malicious nodes and botnet-related activities within SDN environments. In addition to malicious node detection, the proposed framework integrates Mafia game-based role mapping and Reinforcement Learning to improve adaptability and decision-making. The system continuously evaluates node behavior, computes trust scores, and ranks nodes according to their likelihood of malicious activity. Once a malicious node is detected, appropriate security actions such as node isolation, traffic blocking, access restriction, and alert generation are initiated to protect network resources. The Streamlit-based dashboard provides interactive visualization of network topology, node status, trust scores, detection results, and performance metrics. The overall results demonstrate that the proposed framework enhances network security, improves detection reliability, and provides an intelligent solution for protecting Software-Defined Networks from evolving cyber threats.

A. Evaluation and Interpretation of System Interfaces:

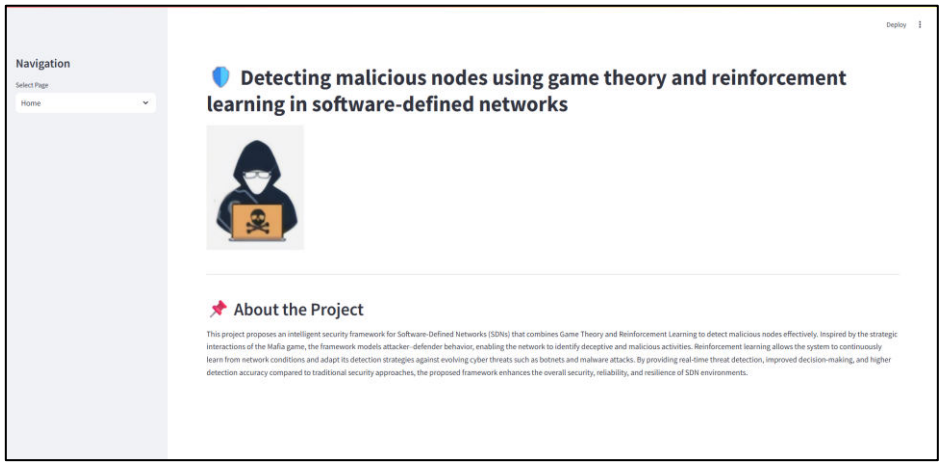


Fig.2. Home Page

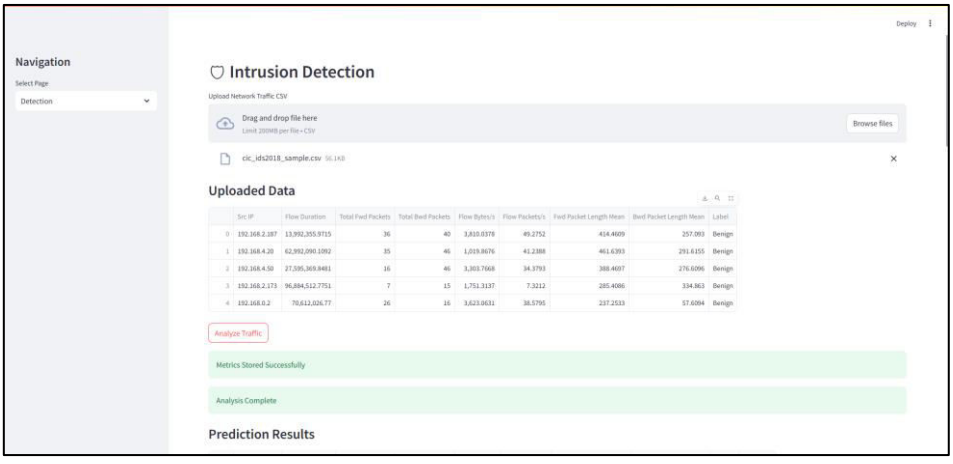


Fig.3. Dashboard After Dataset Upload

© 2026 IJIRCCE | Volume 14, Issue 7, July 2026 DOI: 10.15680/IJIRCCE.2026.1407030

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

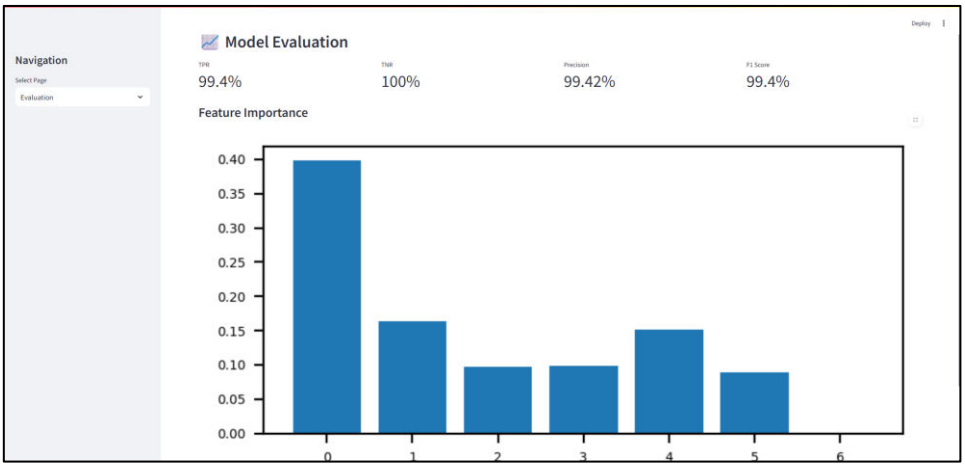


Fig.5. Performance Evaluation Results

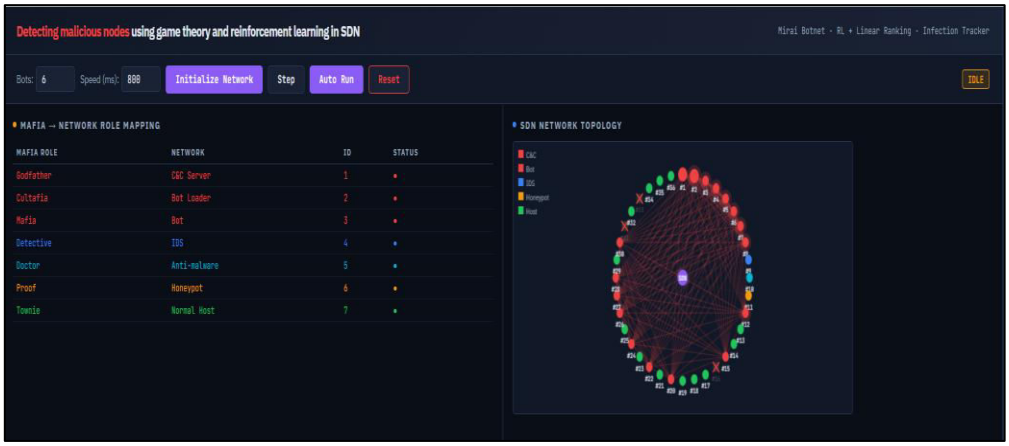


Fig.6. Live Server Mafia Role Mapping and SDN Network Topology

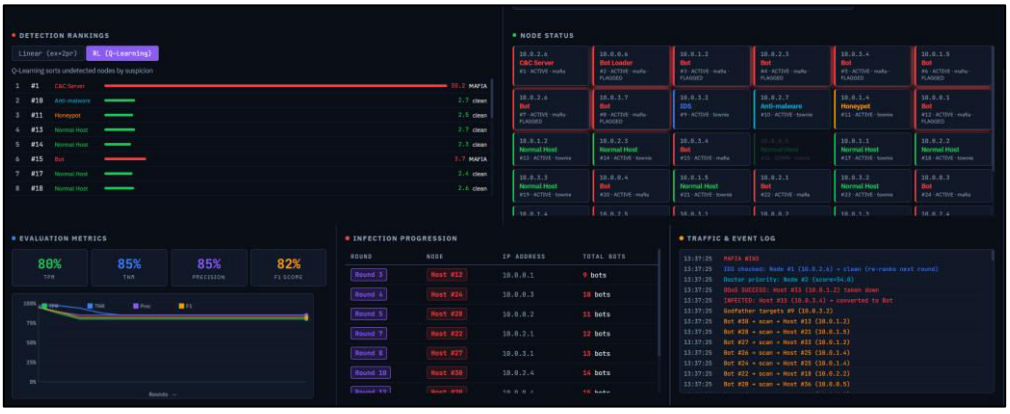


Fig.7. Detection Rankings and Network Monitoring Dashboard

D. Metrics for Evaluation:

The performance of the proposed Mafia Game-Based Malicious Node Detection Framework is evaluated using standard classification metrics such as Accuracy, Precision, Recall, F1-Score, True Positive Rate (TPR), and True Negative Rate

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

(TNR). These metrics help measure the effectiveness of the proposed framework in distinguishing malicious nodes from legitimate network entities within the Software-Defined Network environment.

Let:

TP = True Positives (correctly identified malicious nodes)

TN = True Negatives (correctly identified legitimate nodes)

FP = False Positives (legitimate nodes incorrectly classified as malicious)

FN = False Negatives (malicious nodes incorrectly classified as legitimate)

True Positive Rate (TPR): Measures the proportion of malicious nodes correctly identified by the system.

$$TPR = \frac{TP}{TP+FN} \quad \text{Eq. 5}$$

Precision:

Proportion of true positive predictions among all positive predictions.

$$\text{Precision} = \frac{TP}{TP+FP} \quad \text{eq. (6)}$$

True Negative Rate (TNR):

Measures the proportion of legitimate nodes correctly classified by the system.

$$TNR = \frac{TN}{TN+FP} \quad \text{eq. (7)}$$

F1-Score:

The F1-Score is the harmonic mean of Precision and Recall and provides a balanced evaluation of the classifier's performance.

$$\text{F1Score} = 2 \times \frac{Precision \times Recall}{Precision + Recall} \quad \text{eq. (8)}$$

VI. CONCLUSION AND FUTURE WORK

The suggested Mafia Game-Based Malicious Node Detection Framework uses reinforcement learning, game theory, and belief-based analysis to successfully identify malicious nodes in software-defined networks. Through continual learning, the framework rates suspicious entities, assesses node activity, and enhances detection judgments. High detection accuracy and dependable performance in differentiating malicious nodes from authorized network users are demonstrated by experimental findings. In order to further increase detection accuracy and scalability, future work will concentrate on combining sophisticated Deep Reinforcement Learning algorithms, Graph Neural Networks (GNNs), and real-time SDN controller deployment. For improved cybersecurity protection, the framework can also be expanded to accommodate cloud environments, IoT networks, and large-scale dispersed network infrastructures.

REFERENCES

1. N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, and J. Turner, "OpenFlow: Enabling Innovation in Campus Networks," ACM SIGCOMM Computer Communication Review, vol. 38, no. 2, pp. 69–74, 2008.
2. A. Javadpour, M. S. Movahedi, and M. M. Ahmadi, "Detecting Malicious Nodes Using Game Theory and Reinforcement Learning in Software-Defined Networks," Scientific Reports, vol. 15, no. 1, pp. 1–25, 2025.
3. R. S. Sutton and A. G. Barto, Reinforcement Learning: An Introduction, 2nd ed., Cambridge, MA, USA: MIT Press, 2018.
4. V. Mnih, K. Kavukcuoglu, D. Silver, A. Graves, I. Antonoglou, D. Wierstra, and M. Riedmiller, "Playing Atari with Deep Reinforcement Learning," arXiv:1312.5602, 2013.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

5. R. S. Sutton, A. G. Barto, "Temporal-Difference Learning," Machine Learning, vol. 8, no. 3–4, pp. 279–292, 1992.
6. R. Agrawal, B. Bhushan, H. Sharma, A. A. Hameed, and A. Jamil, "Advancing Intrusion Detection in Software-Defined Networks Using Deep Reinforcement Learning and Graph Convolutional Networks," Proceedings of SATC 2025, pp. 1–8, 2025.
7. R. Kanimozhi and P. S. Ramesh, "Deep Reinforcement Learning-Based Intrusion Detection Scheme for Software-Defined Networking," Scientific Reports, vol. 15, 2025.
8. F. Razvan and C. Mitica, "Enhancing Network Security Through Integration of Game Theory in Software-Defined Networking Framework," International Journal of Information Security, vol. 24, no. 2, pp. 145–159, 2025.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details