iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** V **Month of publication:** May 2026

DOI: https://doi.org/10.22214/ijraset.2026.81886

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue V May 2026- Available at www.ijraset.com

Explainable AI-Based Intrusion Detection System Using Rule-Based Anomaly Detection and Honeypot Mechanism Implementation

Amal Murali, Dharvish K.S, Fasil Shah T.S, Sreedil V.J, Mahshiya V.M
Dept. of Computer Science &Engg Universal Engineering College Thrissur, Kerala

Abstract: ***Modernnetworkenvironmentsareincreasinglyvul-nerable to cyber threats such as unauthorized access, brute force attacks, and abnormal traffic behavior. Traditional intrusion detectionsystemsoftenrelyoncomplexmachinelearningmodels that require large training datasets and lack transparency in decision-making.***
To address these limitations, this paper presents an Explain-able AI-Based Intrusion Detection System (IDS) that combines real-time network monitoring with rule-based anomaly detection and a honeypot mechanism. The system captures live network packets using TShark and performs network scanning using Nmap to identify open ports and services. Instead of relying on machine learning models, the system uses predefined rules such as abnormal packet size, high request frequency, and repeated login attempts to detect suspicious activities.
Additionally, a honeypot module is implemented as a fakelogin interface to capture attacker behavior and record details such as IP address and login attempts. An Explainable AI component provides human-readable explanations for detected anomalies, improving transparency and trust in the system. The systemisdeployedthroughaweb-baseddashboardforreal-timemonitoring,alertgeneration,andloganalysis.Experimental evaluation shows that the system effectively detects common intrusion patterns with low computational overhead, making it suitable for real-time security applications.
Index Terms—Intrusion Detection System, Explainable Ar-tificial Intelligence, Rule-Based Anomaly Detection, Network Security, TShark, Nmap, Honeypot, Network Traffic Analysis, Cybersecurity, Real-Time Monitoring

I. INTRODUCTION

With the rapid growth of internet-connected systems, cy-bersecurity has become a critical concern in modern network environments. Networks are continuously exposed to threats suchasunauthorizedaccess,bruteforceattacks,portscanning, andabnormaltrafficbehavior.Traditionalsecuritymechanisms like firewalls are not sufficient to detect sophisticated attacks, which makes intrusion detection systems (IDS) essential.

Many modern IDS solutions rely on machine learning and deep learning techniques. While these approaches can achieve high detection accuracy, they require large training datasets, highcomputationalresources,andoftenbehaveasblack-boxsystems.Thislackoftransparencymakesitdifficult for administrators to understand why a particular activity is classified as malicious.

To overcome these limitations, this work proposes an Ex-plainable AI-Based Intrusion Detection System using rule-based anomaly detection. The system focuses on real-time packet monitoring using TShark and network scanning using Nmap. Instead of relying on trained models, predefined rules are used to detect suspicious patterns such as abnormal packet sizes, repeated requests, and unusual traffic behavior.

Inaddition,ahoneypotmoduleisintegratedintothesystem to simulate a fake login interface. This allows the system to capture attacker interactions and analyze intrusion behavior. An Explainable AI module provides clear explanations for detected anomalies, improving system transparency.

The proposed system aims to provide a lightweight, real-time, and interpretable intrusion detection mechanism suitable for academic and practical environments.

II. RELATED WORKS

Our project draws on and combines several major advance-ments in network intrusion detection, rule-based anomaly detection, honeypot systems, and explainable artificial intel-ligence in cybersecurity.

A. *IntrusionDetectionSystems*

Traditional Intrusion Detection Systems (IDS) rely on signature-basedmethods,whichareeffectiveforknownat- tacks but fail to detect unknown or zero-day threats [**?**]. To overcome this limitation, anomaly-based detection systems have been introduced, which identify deviations from normal networkbehavior.Toolssuchaspacketanalyzersandnetwork monitoring systems play a key role in capturing real-time traffic data for analysis. Modern IDS solutions focus on improving real-time detection while maintaining low compu-tational overhead.

B. *Rule-BasedAnomalyDetection*

Rule-based detection techniques are widely used in net-work security due to their simplicity and efficiency. These systems define predefined thresholds such as packet size, trafficfrequency,andconnectionpatternstoidentifyabnormal behavior. Unlikemachinelearningmodels,rule-basedsystems do not require training datasets and provide faster decision-making. Several studies have demonstrated that rule-based approaches are effective for detecting brute force attacks, abnormal traffic spikes, and unauthorized access attempts in real-time environments [**?**], [**?**].

C. *Honeypot-BasedSecuritySystems*

Honeypotsaredecoysystemsdesignedtoattractattack-ers and study their behavior. They provide valuable insights intoattackpatterns,includingloginattempts,IPtracking, and intrusion techniques. Research shows that integrating honeypots with IDS enhances the detection capability by capturing attacker interactions that may not be visible through normal monitoring [**?**]. Modern honeypot systems are often implemented as fake login interfaces or vulnerable services to simulate real-world attack scenarios.

D. *ExplainableAIinCybersecurity*

With the increasing use of intelligent systems in cyberse-curity, explainability has become an important requirement. Explainable Artificial Intelligence (XAI) techniques aim to provide human-understandable reasons for system decisions. In intrusion detection, XAI helps administrators understand why certain traffic is classified as suspicious, improving trust and usability [**?**]. Instead of relying on black-box models, explainable systems provide clear insights such as identifying brute force attempts or abnormal traffic behavior.

E. *PriorWorkandMotivation*

Existing research shows that intrusion detection systems either focus on complex machine learning models or basic rule-based detection without transparency. While machine learning-based systems offer high accuracy, they lack inter-pretability and require large datasets. On the other hand, rule-based systems are efficient but often lack detailed explanation capabilities.

Our system bridges this gap by combining rule-based anomaly detection with a honeypot mechanism and an Ex-plainable AI module. This approach provides real-time detec-tion, captures attacker behavior, and offers clear explanations fordetectedintrusions,makingitsuitableforpracticaldeploy-ment in network security environments.

III. SYSTEM ARCHITECTURE

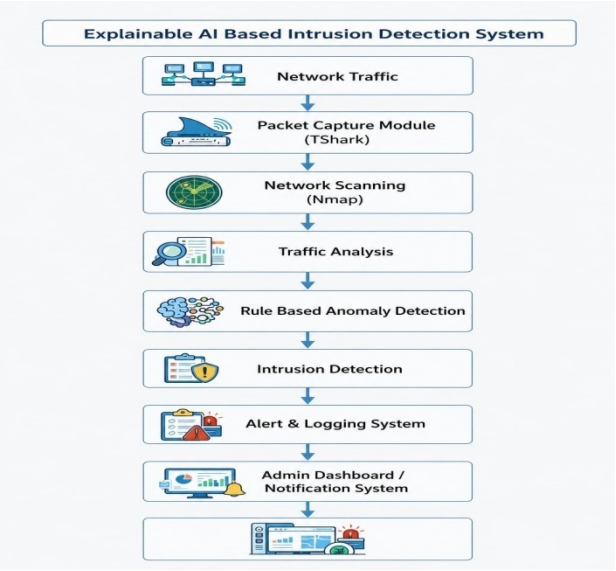


Fig. 1.System Architecture of the Explainable AI-Based Intrusion DetectionSystem

Thesystemisdesignedasamodulararchitectureconsisting ofmultiplecomponentsthatworktogethertomonitor,analyze, and detect network intrusions.

A. PacketCaptureModule(TShark)

The system captures real-time network packets using TShark,whichisthecommand-lineversionofWireshark. It extracts essential packet information such as source IP, destination IP, packet size, and protocol details.

B. NetworkScanningModule(Nmap)

Nmap is used to scan the network and identify open ports and active services. Open ports are potential entry points for attackers, making them important for intrusion detection.

C. TrafficAnalysisandRule-BasedDetection

Capturedpacketdataisanalyzedusingpredefinedrules instead of machine learning models. The system checks for:

- Abnormalpacketsizes
- Highfrequencyofrequests
- Repeatedloginattempts

If any rule condition is violated, the traffic is classified as suspicious.

D. HoneypotModule

A fake login interface is implemented to attract attackers. When an attacker attempts to access the system, their details such as IP address and login attempts are recorded.

E. ExplainableAIModule

The system provides explanations for detected anomalies. For example, it identifies whether the intrusion is due to brute force attempts or abnormal traffic patterns.

F. AlertandLoggingSystem

When suspicious activity is detected, alerts are generated and logs are stored for further analysis.

G. AdminDashboard

A web-based interface is used to display real-time traffic, alerts, and logs, allowing administrators to monitor system activity.

IV. EXPERIMENTAL SETUP & EVALUATION

To evaluate the performance of the proposed intrusion detection system, a series of experiments were conducted in a controllednetworkenvironment.Thesystemwasdeployedon a standard computing setup with moderate processing capa-bility, running the backend locally using Python and FastAPI. Networktrafficwasgeneratedusingnormalbrowsingactivities as well as simulated intrusionscenarios such as repeated login attempts and high-frequency packet transmission.

A. LatencyAnalysis

Since real-time monitoring is a critical requirement for intrusion detection systems, we measured the system response time across multiple traffic events. The evaluation was per-formed over 50 different network interactions, including both normal and suspicious activities. Table I shows the average time taken by each module in the system.

TABLEI
AVERAGEPROCESSINGTIMEPERNETWORKEVENT

ProcessingModule	MeanTime(ms)	Percentage
PacketCapture(TShark)	120	18.5%
NetworkScanning(Nmap)	210	32.3%
TrafficAnalysis	140	21.5%
Rule-BasedDetection	110	16.9%
Alert&Logging	70	10.8%
TotalSystemTime	650ms	100%

V. IMPLEMENTATION DETAILS

A. BackendImplementation

The backend is implemented using Python and FastAPI. It handles packet capture, rule evaluation, and alert generation.

B. PacketCaptureusingTShark

TShark is used to continuously capture network packets. The captured data is parsed to extract relevant features suchas IP addresses and packet size.

C. NetworkScanningusingNmap

Nmap scans the network periodically to detect open ports and services. This helps identify vulnerable points in the system.

D. Rule-BasedDetectionEngine

The detection engine uses predefined rules to identify anomalies.Theserulesarebasedonnetworkbehaviorpatterns and do not require training data.

E. HoneypotImplementation

A fake login page is developed to capture attacker interac-tions. All login attempts are logged and analyzed.

F. ExplainableAIIntegration

The system generates explanations for detected anomalies, making it easier for administrators to understand the reason behind alerts.

G. FrontendDashboard

A web-based interface is used to display captured packets, detected anomalies, and alerts in real time.

The total processing time remains under one second, allow-ing the system to respond quickly to potential threats. Among all modules, network scanning contributes the highest latency due to port scanning operations, while rule-based detection remains computationally efficient.

H. DetectionPerformance

Toevaluatedetectioncapability,thesystemwastestedwith a mix of normal traffic and simulated attack scenarios such as brute force login attempts and abnormal packet transmission. Detectionperformancewasassessedusingstandardevaluation metrics such as accuracy, precision, recall, and F1-score.

TABLEII
INTRUSION DETECTIONPERFORMANCEMETRICS

Metric	Value (%)	Description
Accuracy	84.6	Correctclassificationofnormalandsuspicioustraffic
Precision	81.3	Correctidentificationofmaliciousactivities
Recall	78.9	Detectionrateofactualintrusions
F1-score	80.0	Balancebetweenprecisionandrecall

The results indicate that the system is capable of effectively detecting suspicious activities with consistent performance. Therule-basedapproachensuresfastdetectionwithoutrequir-ing training data.

I. HoneypotAnalysis

The honeypot module was evaluated by simulating unau-thorized access attempts through a fake login interface. The system successfully captured attacker details such as IP ad-dresses and login attempts. These interactions provided valu-able insights into intrusion behavior and attack patterns.

J. ExplainableAIEvaluation

The Explainable AI module was assessed based on its ability to generate understandable explanations for detected anomalies. The system successfully identified reasons such as repeated login attempts, abnormal packet size, and unusual trafficfrequency.Thisimprovessystemtransparencyandhelps administrators make informed decisions.

Overall, the experimental results demonstrate that the pro-posed system provides efficient real-time intrusion detection with low computational overhead while maintaining clear interpretability.

VI. CONCLUSION AND FUTURE WORK

The proposed Explainable AI-Based Intrusion Detection System demonstrates an effective approach to enhancing network security using real-time monitoring and rule-based anomaly detection. By integrating tools such as TShark for packet capture and Nmap for network scanning, the system is capable of identifying suspicious activities such as abnormal traffic patterns, repeated login attempts, and unauthorized access attempts.

Unlike traditional machine learning-based systems, the pro-posedapproachdoesnotrelyonlargetrainingdatasetsorcom-plex models. Instead, it uses predefined rules for fast and ef-ficient detection, making it suitable for real-time applications. The integration of a honeypot module further strengthens the system by capturing attacker behavior, including IP addresses and login attempts, which provides valuable insights into intrusion patterns. Additionally, the Explainable AI module enhances transparency by providing clear and understandable explanations for detected anomalies, improving trust and us-ability for system administrators.

The system provides a lightweight and scalable framework that can be easily deployed in small to medium network environments.Theuseofaweb-baseddashboardenablesreal-time monitoring, alert generation, and log analysis, allowing administrators to respond quickly to potential threats.

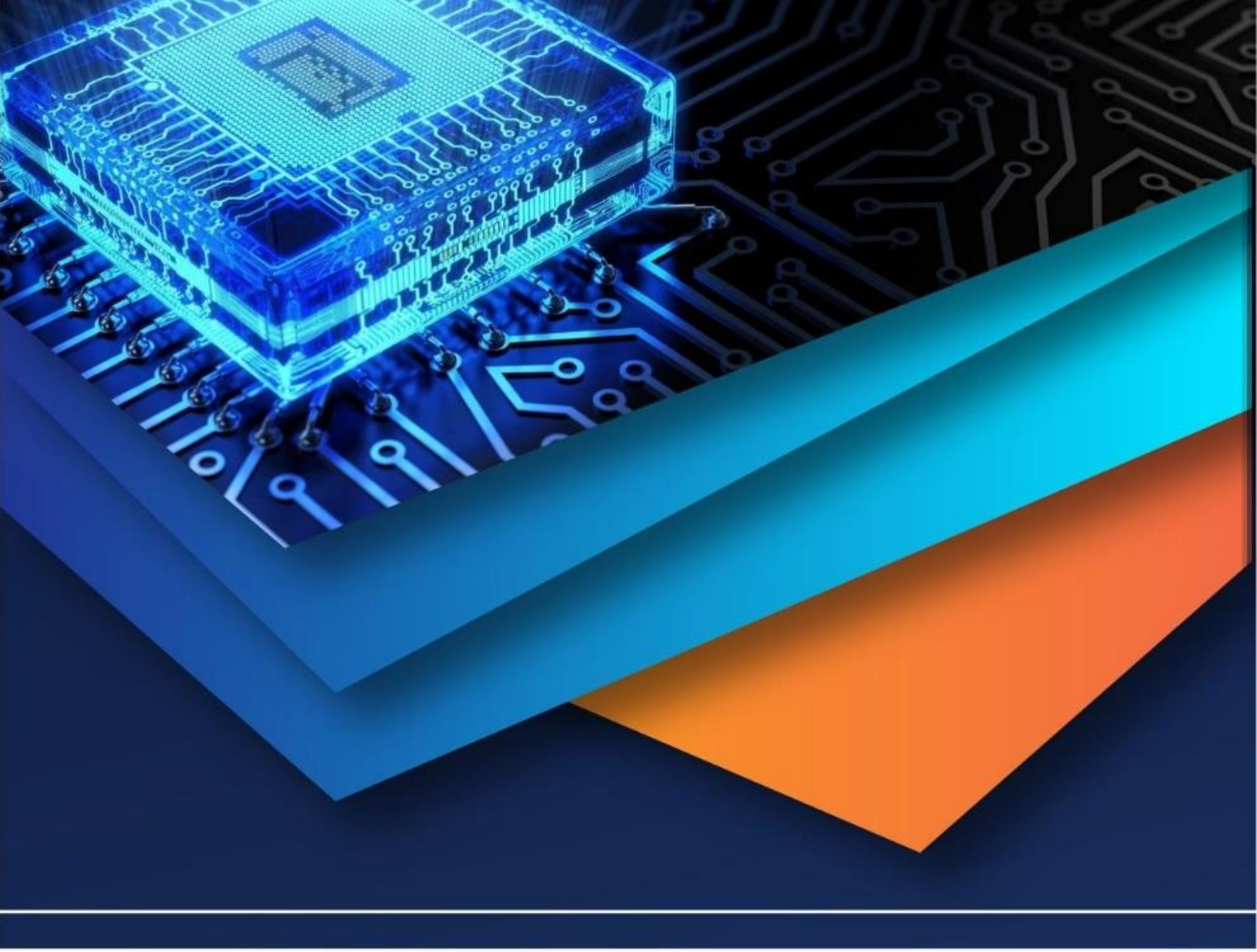
Infuturework,thesystemcanbeenhancedbyincorporating adaptive rule mechanisms to automatically adjust detection thresholds based on changing network conditions. Additional improvements may include integrating automated response systemssuchasIPblockingandfirewallconfiguration,aswell as extending the honeypot module to simulate more complex attack scenarios. Further enhancements in the Explainable AI modulecanprovidemoredetailedinsightsintoattackpatterns, improving decision-making capabilities. The system can also be extended for deployment in large-scale enterprise networks and cloud environments.

VII. ACKNOWLEDGMENT

We would like to thank the Department of Computer Sci-ence and Engineering at Universal Engineering College for their continued guidance, support, and the resources provided throughout the development of this project.

REFERENCES

[1] Yang,Z.,Liu,X.,Li,T.,Wu,D.,Wang,J.,&Zhao,Y.(2022).Asystematic literature review of methods and datasets for anomaly-basednetwork intrusion detection. Computers & Security, 116, 102675.
[2] Sowmya,T.,&Anita,E.M.(2023).Acomprehensivereviewofintrusiondetection systems. Measurement: Sensors, 28, 100827.
[3] Khraisat, A., Gondal, I., Vamplew, P., &Kamruzzaman, J. (2019). Surveyof intrusion detection systems: techniques, datasets and challenges.Cybersecurity, 2(1), 1-22.
[4] Ring, M., Wunderlich, S., Scheuring, D., Landes, D., &Hotho, A.(2019). A survey of network-based intrusion detection data sets. Com-puters& Security, 86, 147-167.
[5] Almseidin,M.,Alzubi,M.,Kovacs,S.,&Alkasassbeh,M.(2018). Evaluation of intrusion detection approaches. arXiv preprintarXiv:1801.02330.
[6] Yang, Z., et al. (2022). Anomaly-based intrusion detection techniquesfor network security. Computers & Security.
[7] Wali, S., & Khan, I. (2021). Explainable AI for intrusion detectionsystems. arXiv preprint arXiv:2112.09177.
[8] Lundberg,S.M.,&Lee,S.-I.(2017).Aunifiedapproachtointerpretingmodelpredictions.AdvancesinNeuralInformationProcessingSystems,30.
[9] Aldweesh, A., Derhab, A., & Emam, A. Z. (2020). Survey on anomaly-based intrusion detection systems. Knowledge-Based Systems, 189,105124.
[10] Sharafaldin, I., Lashkari, A. H., & Ghorbani, A. A. (2019). Developingrealistic DDoS attack dataset and taxonomy. ICCST.
[11] Al-Jarrah, O., et al. (2020). Comparative study of intrusion detectionapproaches. Journal of Intelligent & Fuzzy Systems.
[12] Joshi,M.,etal.(2024).Intrusiondetectionsystemsfornetworksecurity.Nanotechnology Perceptions.
[13] Nizam, A., et al. (2025). Comparative study on intrusion detectionsystems. IJERT.
[14] Sauka,K.,etal.(2022).Explainableintrusiondetectionsystems.Ap-plied Sciences.
[15] Jiang,H.,etal.(2023).Secureloggingandblockchain-basedsecuritysystems. IEEE Transactions.
[16] Madry,A.,etal.(2017).Securitychallengesinadversarialenviron-ments. arXiv.
[17] Goodfellow,I.J.,etal.(2014).Understandingadversarialattacks.arXiv.
[18] Lo,W.W.,etal.(2022).Networkbehavioranalysisforintrusiondetection. arXiv.
[19] Nakıp, M., &Gelenbe, E. (2023). Online anomaly detection in networksystems. arXiv.
[20] Caville,E.,etal.(2023).Anomalydetectionmethodsfornetworkintrusion detection. Knowledge-Based Systems.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY