© January 2025 | IJIRT | Volume 11 Issue 8 | ISSN: 2349-6002

A High-Performance Network Intrusion Detection System – IntruAlert

Likith.G[1], Kushaal.G. P[2], Gaurav Dhull[3], Ms.Raesa Razeen[4]
[1,2,3,4]*School of Computer Science and Engineering, Presidency University,BangaloreKarnataka 560064, India*

***Abstract*—In today's rapidly evolving digital landscape, protecting network infrastructure from unauthorised access and cyber threats is of paramount importance. IntruAlert is an advanced Network Intrusion Detection System (NIDS) engineered to proactively monitor, detect, and mitigate network threats in real-time. By integrating cutting-edge technologies like machine learning, signature-based detection, and anomaly detection algorithms, IntruAlert delivers comprehensive protection against both known and emerging cyberattacks.**

The system persistently analyses network traffic to detect irregular patterns that may signify intrusions. It features an extensive threat signature database and employs heuristic methods to identify zero-day vulnerabilities. IntruAlert's modular design ensures seamless integration into existing network infrastructures, offering scalability and adaptability to cater to various organisational needs.

I. INTRODUCTION

In an era of advanced digital communication and interconnected systems, organisations are increasingly vulnerable to a diverse range of cyber threats. These threats include malware, ransomware, phishing attacks, and advanced persistent threats (APTs). Traditional security measures, primarily focused on perimeter defence, are no longer sufficient to counter these sophisticated attacks.

IntruAlert, a sophisticated NIDS, addresses the growing complexity of cyberattacks by adopting a proactive approach. Unlike conventional security measures, it continuously monitors network traffic to detect and respond to suspicious activities. Combining signature-based analysis, which compares traffic with known threat signatures, and anomaly-based methods, which flag unusual behaviour, IntruAlert provides a comprehensive security solution against both known and unknown threats.

This introduction to IntruAlert highlights the system's significance in safeguarding organizational networks from increasingly sophisticated cyber threats. By offering real-time monitoring, intelligent detection, and actionable insights, IntruAlert serves as a critical tool in maintaining the integrity, confidentiality, and availability of network resources in a digitally connected world.

II. CHALLENGES

1. Evolving Threat Landscape

Cybercriminals constantly devise new methods to bypass security measures, such as polymorphic malware, encrypted attacks, and APTs. Keeping IntruAlert's detection algorithms updated is an ongoing challenge.

2. High False Positive and False Negative Rates

Striking a balance between sensitivity and specificity is critical. Excessive sensitivity leads to numerous false alarms, overwhelming administrators, while insufficient sensitivity may allow threats to go undetected.

3. Zero-Day Attacks

Identifying zero-day vulnerabilities which exploit previously unknown security flaws is difficult. This necessitates sophisticated anomaly-based and heuristic detection methods.

4. Performance and Scalability

Processing massive amounts of data in real-time without impacting network performance requires high optimisation. IntruAlert must efficiently handle modern network speeds and traffic loads.

5. Encrypted Traffic Analysis

With widespread adoption of encrypted communications (e.g., HTTPS, VPNs), detecting malicious activities within encrypted data is challenging. Balancing security and user privacy during encrypted traffic analysis is crucial.

6. Integration with Existing Systems

Organisations often have complex IT environments. Ensuring seamless integration of IntruAlert with existing security tools (e.g., firewalls, SIEM systems, endpoint protection) is a significant undertaking.

7. Machine Learning Limitations

While machine learning improves detection accuracy, it introduces challenges like data quality, model interpretability, and susceptibility to adversarial attacks. Maintaining reliable and adaptive learning models is essential.

8. Ease of Integration

IntruAlert can seamlessly integrate with existing security solutions such as firewalls, endpoint protection, and Security Information and Event Management (SIEM) systems, enabling a unified approach to cybersecurity.

III. ADVANTAGES

1. Real-Time Threat Detection

IntruAlert continuously monitors network traffic, enabling instant detection of potential threats and swift incident response.

2. Comprehensive Coverage

By combining signature-based and anomaly-based detection, IntruAlert effectively identifies a wide spectrum of threats, including known malware, zero-day exploits, and insider threats.

3. Reduced Data Breach Risk

Early detection and mitigation of intrusions safeguard sensitive data, ensuring confidentiality, integrity, and availability.

4. Adaptive Learning Capabilities

Leveraging machine learning, IntruAlert continuously refines its detection algorithms, adapting to emerging threats and reducing false positives and negatives over time.

5. Early Zero-Day Exploit Detection

Through heuristic and anomaly-based analysis, IntruAlert can identify novel attack patterns, enabling the detection of zero-day vulnerabilities before widespread exploitation.

6. Scalability and Flexibility

IntruAlert's modular architecture makes it suitable for organisations of all sizes, from small businesses to large enterprises, and adaptable to diverse IT environments.

C. Problem Statement

In today’s interconected digital world, organisations face a persistent and growing threat landscape, with cyberattacks like malware, ransomware, phishing, and APTs becoming more sophisticated and frequent. Traditional security measures, such as firewalls and antivirus software, are no longer adequate to detect and prevent these complex and stealthy attacks.

The primary challenge lies in real-time monitoring of network traffic to detect malicious activities while minimising false positives and negatives. The rapid adoption of encrypted communications, zero-day vulnerabilities, and insider threats complicates detection further. Additionally, organisations struggle with scalability, as modern networks demand solutions that can process high volumes of data without causing latency or performance bottlenecks.

Additionally, the lack of integration with existing security tools, the need for skilled cybersecurity professionals, and compliance with strict legal and regulatory requirements further complicate the deployment and effectiveness of intrusion detection systems.

IV. SYSTEM DESIGN ARCHITECTURE

Network Traffic Observing

- IntruAlert catches parcels from the organization utilizing instruments like bundle sniffers (e.g., Wireshark, tcpdump) or incorporation with Range ports and organization taps.

Preprocessing Layer

- Parcel Investigation
- Crude information is parsed into significant components, for example, IP addresses, ports, conventions, and payloads.

Identification Motor

Signature-Based Identification

- Matches network traffic against a predefined data set of known assault marks (e.g., Grunt or Suricata rule sets).

Peculiarity Based Discovery

- Uses factual techniques and AI models to recognize deviations from laid out baselines.

Direction and Alarming Layer Danger Scoring

- Every potential interruption is doled out a seriousness score in view of elements like certainty level and danger influence.

Constant Cautions

- Cautions are shipped off heads by means of email, SMS, or a dashboard with itemized logs and
- proposals for moderation.

Reporting and Logging Layer

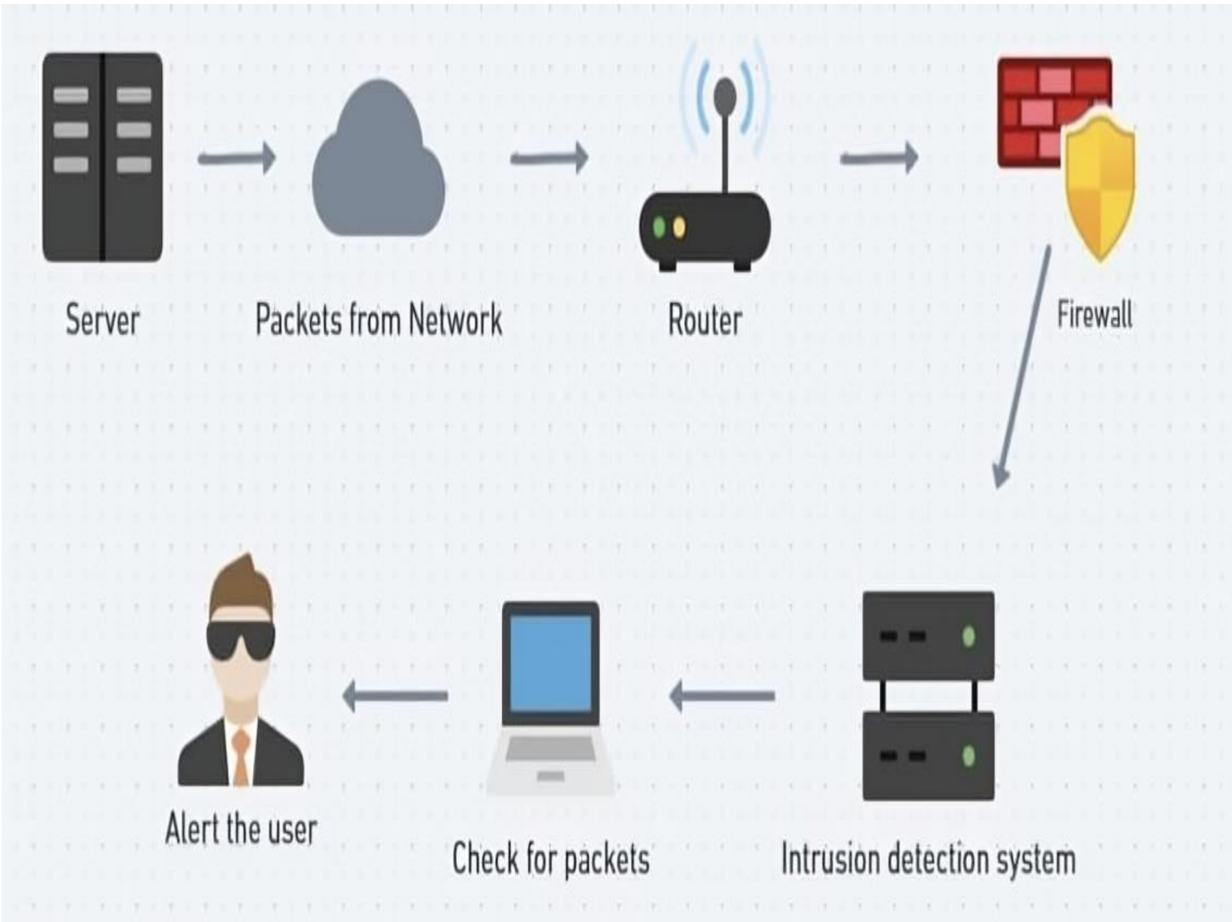
- Visualization:

Provides dashboards and graphs for traffic trends, threat detection statistics, and system performance.

- Detailed Logs:

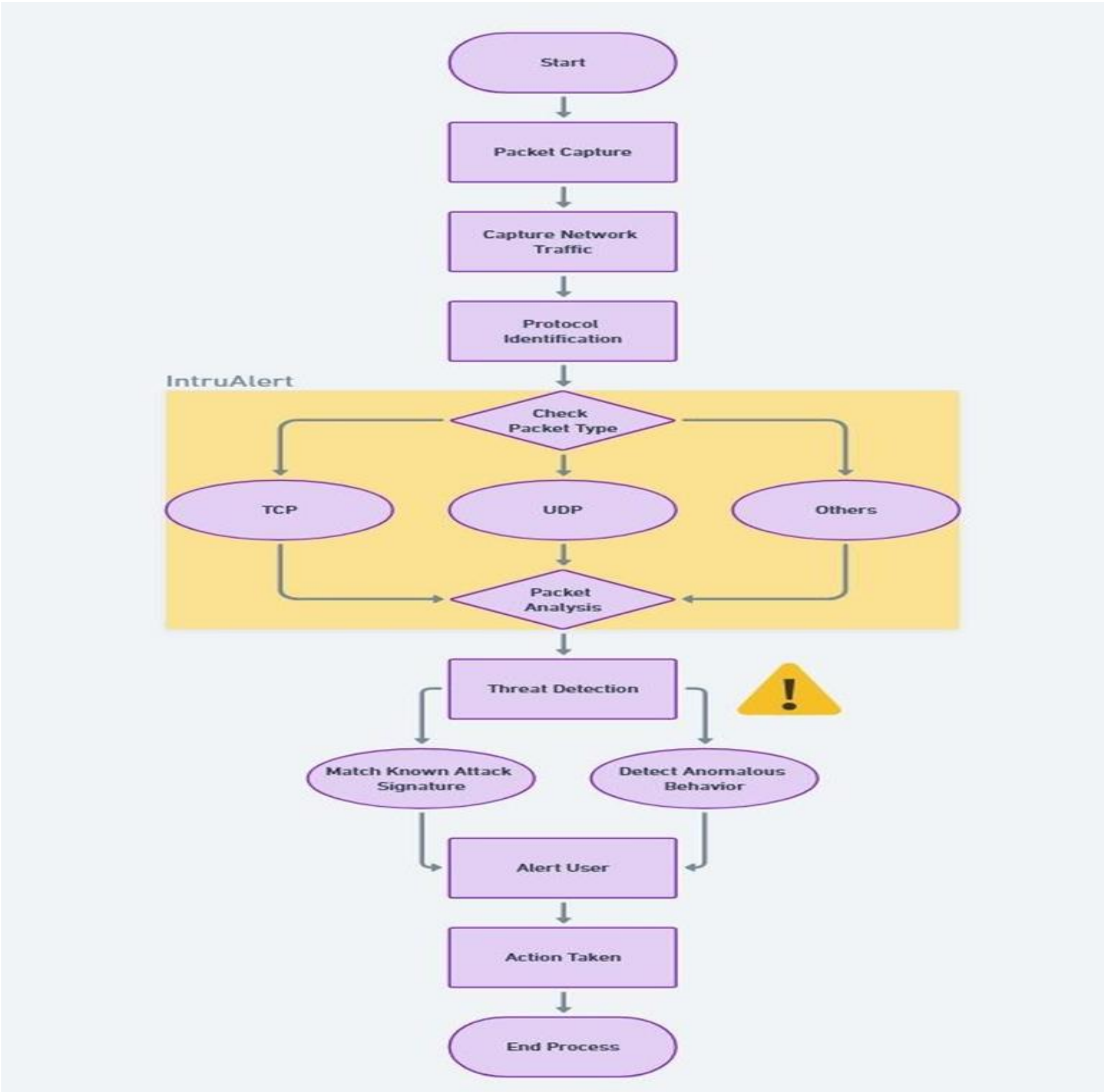
Logs every detected event for forensic analysis and compliance with regulations.

V. BLOCK DIAGRAM



- Server
  The starting point where data originates or is accessed. It generates or processes network packets.
- Packets from Network
  Network traffic consisting of data packets is sent over the network.
- Router
  Directs the flow of packets to their intended destination within or outside the network.
- Firewall
  Acts as the first layer of security, filtering packets based on predefined rules to block unauthorized access.
- Intrusion Detection System (IDS)
  Analyzes the packets allowed by the firewall to detect potential malicious activity or security breaches.
- Check for Packet
- the system monitors packet content and traffic patterns to determine if any anomalies or intrusions exist.
- Alert the User
  If an intrusion or abnormal activity is detected, the IDS sends an alert to the user or administrator for further action.

VI. SYSTEM DESIGN AND ARCHITECTURE



This flowchart represents the operational workflow of IntruAlert for detecting and mitigating network threats. It begins with packet capture and traffic analysis, followed by protocol identification and packet type classification (TCP, UDP, or others). The packets are analyzed to detect threats by matching known attack signatures or identifying anomalous behavior. Upon detecting a threat, the system alerts the user and initiates appropriate actions to mitigate the attack, concluding the processs.

VII. Methodology

A. Hand- Grounded Discovery Algorithms

These algorithms calculate on predefined patterns of known pitfalls, similar as malware autographs or attack actions.

B. Aho- Corasick Algorithm

- Used formulti-pattern string matching in network packets.
- Effective in searching for multiple attack

autographs contemporaneously.

C. Boyer- Moore Algorithm

- Optimized for fast pattern matching by skipping gratuitous comparisons.
- Useful for detecting known malware autographs in network business.

D. Anomaly- Grounded Discovery Algorithms

- These algorithms descry diversions from normal network geste
- and are effective for relating unknown or zero-day attacks.

E. K- Means Clustering

- Groups network business into clusters to separate between normal and abnormal
- Suitable for unsupervised literacy during birth creation.
- star element Analysis (PCA)
- Reduces the dimensionality of data to identify significant features for anomaly discovery.
- Highlights outliers in network business.

F. insulation timber

- A tree- grounded algorithm specifically designed to descry anomalies.
- Isolates abnormal business patterns by recursively partitioning the dataset.
- Autoencoders (Deep Learning)
- Neural networks trained to compress and reconstruct normal business patterns.
- Anomalies are flagged when reconstruction error exceeds a predefined threshold.

G. Machine Learning Algorithms

- Machine literacy models help classify business as vicious or benign grounded on training data.

H. Random Forest

- A robust ensemble learning algorithm combining multiple decision trees.
- Used for classifying business grounded on features like protocol type, packet size, and duration.

I. Support Vector Machine (SVM)

- Effective in high- dimensional spaces, SVM is used to classify business as normal or anomalous.
- Useful for double andmulti-class bracket tasks.

J. Naïve Bayes

- A probabilistic algorithm grounded on Bayes' theorem.
- Effective for detecting specific attack types, similar as spam or phishing.
- grade Boosting Algorithms (e.g., XGBoost, LightGBM)
- employed for high- delicacy bracket tasks in intrusion discovery.
- Handles large datasets and identifies subtle attack patterns.

K. Hybrid Algorithms

IntruAlert often combines multiple algorithms to maximize detection accuracy and reduce false positives.

L. Ensemble Models

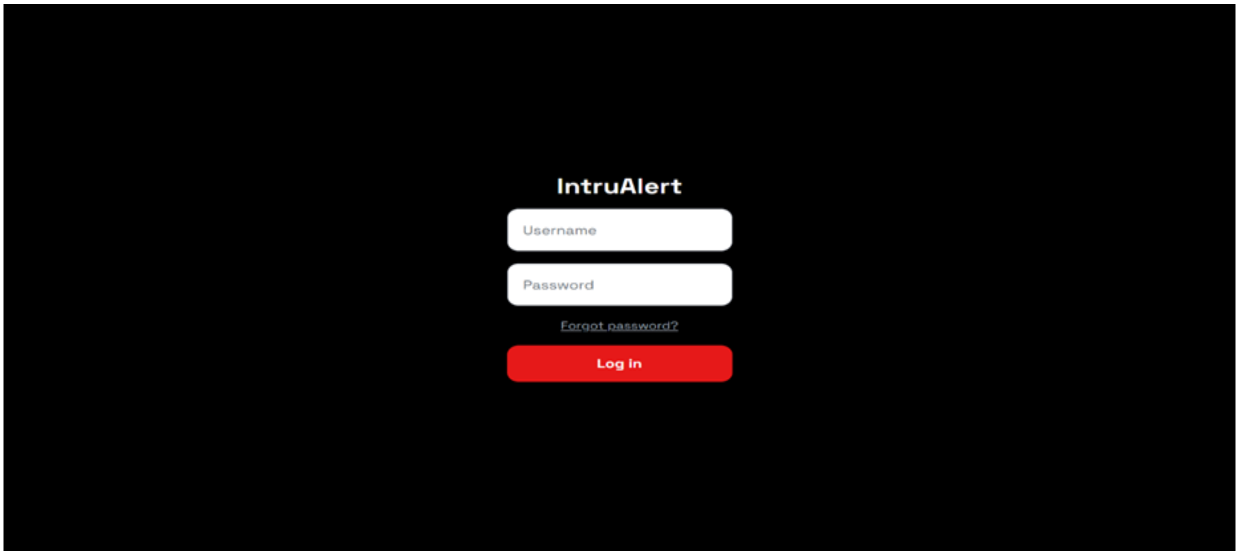
- Combines outputs from multiple machine learning models (e.g., Random Forest + SVM).
- Improves robustness and accuracy in detecting diverse attack patterns.

M. Hybrid Detection Systems

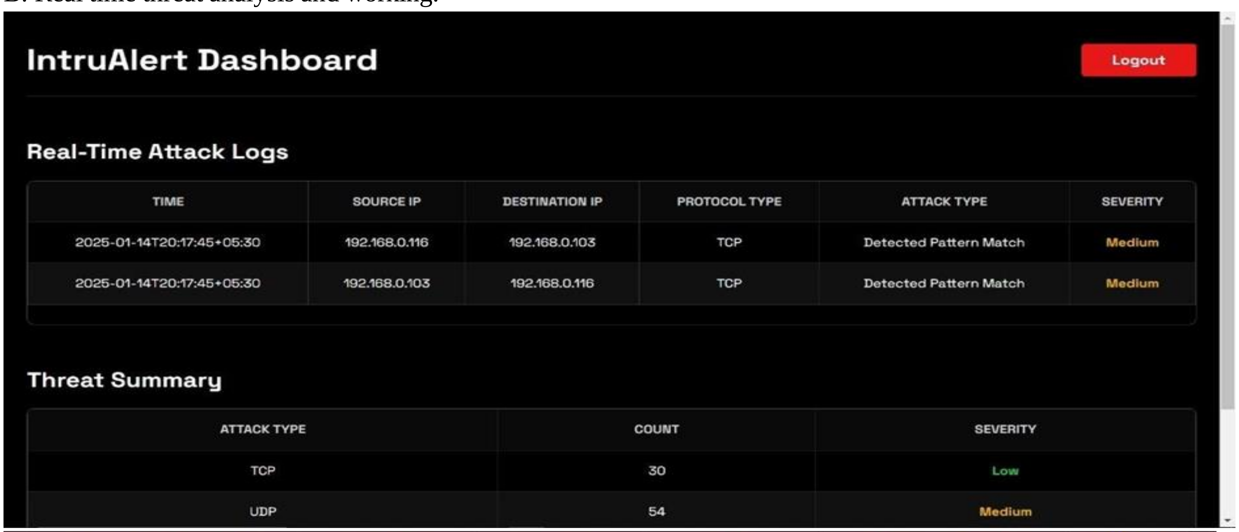
- Combines signature-based and anomaly-based approaches.
- Uses signature detection for known threats and anomaly detection for zero-day attacks.

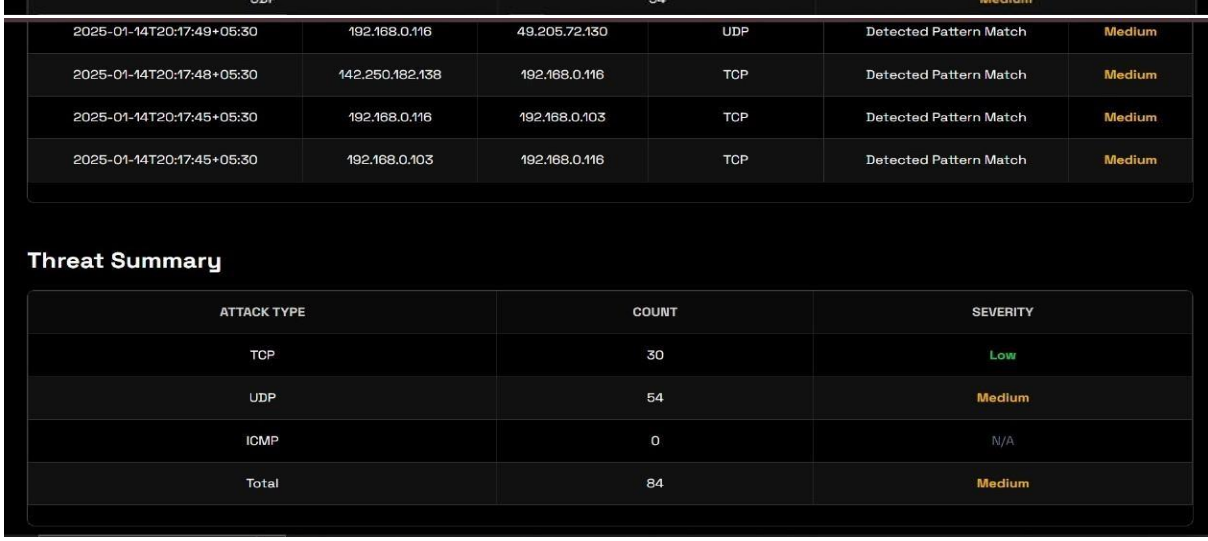
VIII. Results

A. Login page



B. Real time threat analysis and working.





- The IntruAlert dashboard captures and analyzes real-time network traffic to identify potential security threats. The provided screenshots showcase its detection capabilities:
- Real-Time Attack Logs

  Displays details of detected threats, including the timestamp, source IP, destination IP, protocol type (e.g., TCP or UDP), attack classification (e.g., detected pattern matches), and severity levels (e.g., Medium). This helps in pinpointing the origin and nature of malicious activities within the network.
- Threat Summary

  Summarizes detected attack types, their occurrence counts, and associated severity levels. For example, the dashboard reports TCP-based attacks with 30 instances (Medium severity) and UDP- based attacks with 54 instances (Low severity).
- How It Works:

  IntruAlert uses network packet analysis and pattern matching to identify malicious traffic. It continuously monitors incoming and outgoing data, analyzes protocol behavior, and compares traffic against known threat signatures. Upon detecting abnormal or malicious patterns, it logs the details and assigns a severity rating, helping administrators take immediate action to safeguard the network. This system is crucial for real-time threat detection and response.

IX. Conclusion

As cyber threats become increasingly sophisticated, the need for an intelligent, reliable, and scalable intrusion detection system has never been greater. IntruAlert provides a comprehensive solution through real-time monitoring, detection, and mitigation of network threats.

By integrating signature-based detection for known threats, anomaly detection for zero-day vulnerabilities, and machine learning for adaptive threat recognition, IntruAlert offers a multi-layered defence tailored for modern network environments. Its modular design ensures compatibility with existing infrastructures, while advanced algorithms enhance detection accuracy and minimise false positives.

IntruAlert also addresses critical challenges such as encrypted traffic analysis, regulatory compliance, and scalability for large networks. Its ability to provide actionable insights and automate threat mitigation empowers organisations to respond swiftly to potential breaches, reducing the risk of data loss and operational downtime.

Moreover, IntruAlert's integration with existing security frameworks ensures seamless deployment, reducing the complexity of implementation and operational overhead. Its adaptive learning mechanisms continuously refine detection models, making it resilient to emerging attack patterns and zero-day vulnerabilities. By automating routine monitoring tasks and generating actionable alerts, IntruAlert enables IT teams to focus on strategic security initiatives rather than reactive firefighting. Ultimately, IntruAlert not only enhances the organization's ability to prevent and respond to cyber threats but also strengthens its reputation as a trusted, secure entity in the digital landscape, paving the way for sustainable growth and innovation.

In conclusion, IntruAlert represents a significant advancement in network security. By combining cutting-edge technologies, adaptive learning capabilities, and user-friendly interfaces, it serves as a robust shield against the ever-evolving cyber threat landscape. With IntruAlert, organizations can strengthen their security posture, ensure data integrity, and maintain the trust of stakeholders in an increasingly digital world.

References

[1] Ahmad, Z., Khan, A. S., Shiang, C. W., Abdullah, J., & Ahmad, F. (2021). Network Intrusion Detection System: A systematic study of Machine Learning and Deep Learning approaches. International Journal of Communication Systems. Retrieved from https://onlinelibrary.wiley.com/doi/full/10.1002/ett.4150

[2] Forrest, S., Hofmeyr, S. A., Somayaji, A., & Longstaff, T. A. (1996). A Sense of Self for Unix Processes. Proceedings of the 1996 IEEE Symposium on Security and Privacy. Retrieved from https://dl.acm.org/doi/abs/10.1145/319709.319712

[3] McHugh, J. (2001). A Survey of Intrusion

Detection Techniques. ACM Computing Surveys. Retrieved from https://ieeexplore.ieee.org/abstract/document/4667434

[4] Thottan, M., & Ji, C. (2003). A Review of Anomaly Detection Techniques in Network Intrusion Detection Systems. Computer Networks. Retrieved from https://www.sciencedirect.com/science/article/pii/S1877050916311127

[5] Liao, K., Zhao, D., Cardenas, A., & Xu, S. (2013). Anomaly-Based Network Intrusion Detection: Techniques, Systems and Challenges. Journal of Computer Science and Technology. Retrieved from https://ieeexplore.ieee.org/abstract/document/4492545

[6] Agrawal, S., & Agrawal, J. (2015). Review on Anomaly Based Network Intrusion Detection System. International Conference on Computer Communication and Informatics (ICCCI). Retrieved from https://ieeexplore.ieee.org/abstract/document/8284655

[7] Kim, Y., Kim, J., & Kim, H. (2020). Real-Time Network Intrusion Detection System Based on Deep Learning. International Conference on Artificial Intelligence in Information and Communication (ICAIIC). Retrieved from https://www.sciencedirect.com/science/article/pii/S1877050921011078

[8] El-Bakry, H. M., & Mastorakis, N. (2010). A Real-Time Intrusion Detection Algorithm for Network Security. International Journal of Computer Science and Network Security. Retrieved from https://ieeexplore.ieee.org/abstract/document/283931

[9] Singh, S., Estan, C., Varghese, G., & Savage, S. (2004). A Real-Time Intrusion Detection System for High-Speed Networks. Symposium on Networked Systems Design and Implementation. Retrieved from https://ieeexplore.ieee.org/abstract/document/9040718

[10] Heady, R., Luger, G., Maccabe, A., & Servilla, M. (1990). The Architecture of a Network Level Intrusion Detection System. Technical Report. Retrieved from https://digitalcommons.aaru.edu.jo/cgi/viewcontent.cgi?article=1127&context=isl