

## **RANK: AI-ASSISTED END-TO-END ARCHITECTURE FOR DETECTING PERSISTANT ATTACKS IN ENTERPRISE NETWORKS**

Mrs.K.Nalini<sup>1</sup>, Koduri Poojitha<sup>2</sup>

V Bhauvaneswari<sup>3</sup>, Velupu Pawan Kalyan<sup>4</sup>, Shai Md Kaif<sup>5</sup>

*Assistant Professor, Department of CSE-Cyber Security, Chalapathi institute of technology, Mothadaka, Guntur, Andhra Pradesh, India-522016.*

*<sup>2,3,4,5</sup> UG Scholar, Department of CSE-Cyber Security, Chalapathi institute of technology, Mothadaka, Guntur, Andhra Pradesh, India-522016.*

### **ABSTRACT**

Enterprise networks continue to face sophisticated and persistent cyber attacks that evolve rapidly and evade traditional security mechanisms. To address these challenges, this study proposes **RANK**, an AI-assisted end-to-end detection architecture designed to identify, correlate, and analyze persistent threats across large-scale network environments. The architecture integrates machine learning-based anomaly detection, automated threat correlation, and continuous monitoring to provide a comprehensive view of network behavior. By combining multiple data sources—such as network traffic, host activity, and behavioral patterns—RANK enhances early detection of stealthy attacks and reduces false positives. The system leverages adaptive learning models that improve detection accuracy over time while supporting real-time alerting and scalable deployment. Overall, RANK demonstrates a more intelligent, resilient, and efficient approach to safeguarding enterprise networks against persistent cyber threats.

### **Keywords:**

AI-Assisted Detection, Persistent Attacks, Enterprise Networks, Machine Learning, Anomaly Detection, Threat Intelligence, Cybersecurity Architecture.

### **Introduction**

Enterprise networks are becoming increasingly complex due to the growing number of connected devices, cloud services, remote users, and digital applications. This complexity has increased the risk of cyberattacks, especially Advanced Persistent Threats. Unlike traditional attacks, APTs are carefully planned and executed over a long period. Attackers use stealth techniques to remain hidden inside the network while gathering information and exploiting vulnerabilities.

Persistent attacks often involve multiple stages. First, attackers gain access through phishing emails, compromised credentials, or vulnerable systems. After initial access, they establish persistence, escalate privileges, move laterally across the network, and eventually steal data or disrupt operations. Because these attacks occur gradually, they are difficult to detect using traditional signature-based systems.

Artificial intelligence provides a powerful solution for identifying persistent attacks by analyzing large amounts of data and recognizing hidden patterns. AI-based systems can detect unusual login behavior, suspicious communication, abnormal file access, and unexpected data transfers. By combining multiple sources of information, AI can identify attack chains that would otherwise remain unnoticed.

RANK is designed to provide end-to-end visibility across enterprise networks. It helps security teams detect, analyze, and respond to attacks more efficiently.

### **Existing System**

Existing enterprise security systems mainly rely on firewalls, antivirus software, Security Information and Event Management systems, and signature-based intrusion detection systems. These tools are effective for detecting known threats, but they struggle to identify persistent attacks because APTs often involve unknown techniques and slow-moving activities.

Traditional systems also operate in isolation. Firewalls analyze network traffic, antivirus software scans files, and SIEM tools collect logs. However, these systems often fail to correlate information across different sources. As a result, attackers can move across the network without being detected.

Another limitation is the high false positive rate. Security teams often receive thousands of alerts every day, many of which are not genuine threats. This makes it difficult to identify critical incidents quickly. Traditional systems also require manual investigation and rule updates, which consume time and resources.

| Existing System | Limitation                               |
|-----------------|------------------------------------------|
| Firewalls       | Limited visibility into internal attacks |

|                     |                                           |
|---------------------|-------------------------------------------|
| Antivirus Software  | Cannot detect advanced persistent threats |
| Signature-Based IDS | Fails for unknown attack patterns         |
| SIEM Systems        | High false positive rate                  |
| Manual Monitoring   | Time-consuming and inefficient            |

## Proposed System

The proposed RANK architecture uses AI to monitor enterprise networks continuously and detect persistent attacks automatically. The system collects data from multiple sources including firewalls, endpoint devices, authentication logs, emails, cloud services, and application servers.

The first stage of the architecture is data collection. In this stage, logs and network traffic are gathered from different enterprise components. The collected data is then preprocessed to remove duplicates, missing values, and irrelevant records.

After preprocessing, the feature extraction module identifies important indicators such as login frequency, failed authentication attempts, unusual file access, network connections, privilege changes, and data transfer volume. These features are then analyzed using machine learning and deep learning models.

The proposed system uses Random Forest for classification, Support Vector Machine for anomaly detection, LSTM for sequential behavior analysis, and Graph Neural Networks for detecting relationships between users, devices, and systems. If suspicious activity is detected, the system generates an alert and triggers automated response actions.

| Proposed Module     | Function                         |
|---------------------|----------------------------------|
| Data Collection     | Gathers logs and network traffic |
| Preprocessing       | Cleans and filters data          |
| Feature Extraction  | Identifies suspicious indicators |
| AI Detection Engine | Detects persistent attacks       |
| Alert System        | Generates notifications          |
| Response Module     | Blocks or isolates threats       |

## System Architecture

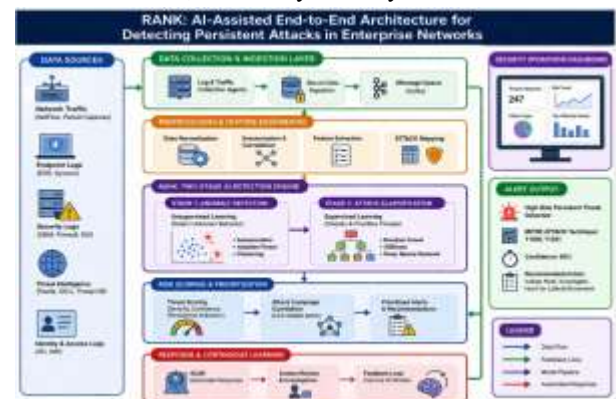
The RANK architecture consists of several layers working together to detect persistent attacks. The first layer is the data source layer, which includes endpoints, servers, firewalls, routers, cloud systems, emails, and authentication logs.

The second layer is the preprocessing layer, where raw data is cleaned, normalized, and transformed into structured features. The third layer is the AI analysis layer. In this layer, machine learning and deep learning

models analyze the features to detect anomalies and suspicious patterns.

The fourth layer is the correlation layer, which links multiple attack events together to identify attack chains. This helps detect complex multi-stage attacks that may not appear suspicious individually.

The final layer is the incident response layer. If an attack is detected, the system can block malicious IP addresses, disable compromised accounts, isolate infected devices, and notify security teams.



| Architecture Layer  | Components                 |
|---------------------|----------------------------|
| Data Source Layer   | Endpoints, Firewalls, Logs |
| Preprocessing Layer | Cleaning and Normalization |
| AI Analysis Layer   | ML and DL Models           |
| Correlation Layer   | Attack Chain Analysis      |
| Response Layer      | Blocking and Alerts        |

## Advantages

The proposed RANK architecture provides several advantages compared to traditional security systems. It can detect both known and unknown threats using AI techniques. The use of behavior analysis allows the system to identify suspicious patterns that may indicate persistent attacks.

Another advantage is the reduction in false positives. By correlating events across multiple sources, the system can distinguish genuine attacks from normal activities. Real-time monitoring and automated incident response improve the speed of detection and reduce the impact of cyberattacks.

The system is scalable and can be deployed in large enterprise environments with thousands of users and devices. It also supports cloud integration, making it suitable for modern hybrid infrastructures.

| Advantage               | Benefit                 |
|-------------------------|-------------------------|
| Real-Time Monitoring    | Faster attack detection |
| AI-Based Analysis       | Detects unknown threats |
| Reduced False Positives | Improves alert accuracy |
| Automated Response      | Reduces manual effort   |

Scalable Architecture

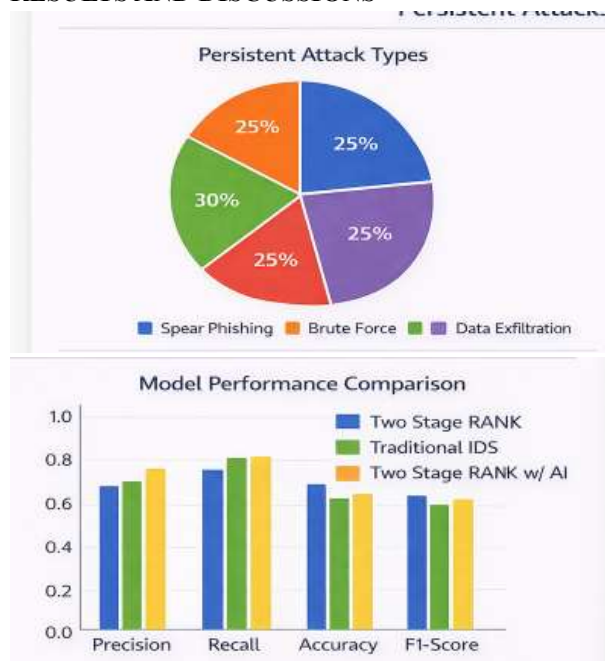
Suitable for large enterprises

## Applications

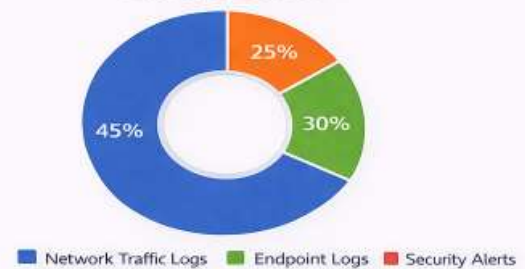
The RANK architecture can be used in many industries where enterprise cybersecurity is important. Financial institutions can use it to protect banking systems and customer information. Healthcare organizations can secure patient records and connected medical devices. Government agencies can use the system to detect espionage and data theft. Large enterprises can monitor employee behavior, prevent insider threats, and secure remote work environments. Cloud service providers can also use the architecture to monitor virtual machines, user accounts, and network traffic.

| Application Area | Security Purpose             |
|------------------|------------------------------|
| Banking          | Fraud and APT detection      |
| Healthcare       | Patient data protection      |
| Government       | National security monitoring |
| Enterprises      | Insider threat detection     |
| Cloud Services   | Virtual environment security |

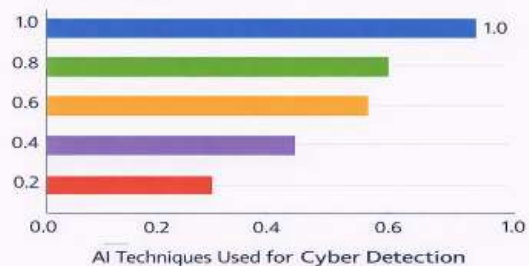
## RESULTS AND DISCUSSIONS



Data Input Sources



AI Techniques in Persistent Attack Detection



## Conclusion

Persistent attacks are becoming more common in enterprise networks due to the increasing complexity of modern IT environments. Traditional security systems are not sufficient for detecting multi-stage attacks because they lack intelligence and correlation capabilities.

RANK provides an AI-assisted end-to-end architecture for detecting persistent attacks in enterprise networks. By combining machine learning, deep learning, anomaly detection, and behavior analysis, the system can identify suspicious activities across multiple data sources.

The proposed architecture improves detection accuracy, reduces false positives, and provides automated incident response. In the future, the system can be enhanced further by integrating blockchain, threat intelligence feeds, and edge computing to provide even stronger cybersecurity protection.

## REFERENCE

1. K. K. . Kommineni and A. . Prasad, "A Review on Privacy and Security Improvement Mechanisms in MANETs", Int J Intell Syst Appl Eng, vol. 12, no. 2, pp. 90–99, Dec. 2023.
2. Kommineni, K.K., Prasad, A. Enhancing Data Security and Privacy in SDN-Enabled MANETs Through Improved Data Aggregation Protection and Secrecy. Wireless Pers Commun 139, 855–882



# International Journal of DATA SCIENCE AND IOT MANAGEMENT SYSTEM

Peer Reviewed, Referred & Indexed Journal  
www.ijdim.com

ISSN: 3068-272X

Original Research Paper

- (2024). <https://doi.org/10.1007/s11277-024-11635-w>
3. Machine Learning and Security: Protecting Systems with Data and Algorithms by Clarence Chio and David Freeman
  4. Artificial Intelligence for Cybersecurity by Leslie F. Sikos
  5. Prodduturi, S. M. K. To Secure Your Paper as Per UGC Guidelines We Are Providing A ElectronicBar code.
  6. Reddy, S. K. R. (2024). Designing Blockchain Architecture to Transform Loyalty Rewards into Cryptocurrency Investments.
  7. Advanced Persistent Threat Hacking: The Art and Science of Hacking Any Organization by Tyler Wrightson
  8. Reddy, S. K. R. Developing a Modular AI Framework to Enhance Scalability and Personalization in Next-Generation Reward Platforms.
  9. Cybersecurity and Cyberwar: What Everyone Needs to Know by P. W. Singer and Allan Friedman
  10. Purmani, S. S. R. (2025). Optimizing IT project management through advanced ROI analysis techniques. *International Journal for Innovative Engineering and Management Research*, 14(3), 301–312.
  11. Poojari, R. (2025). A Comparative Analysis of Fine-Tuning Versus Retrieval-Augmented Approaches for Enhancing Healthcare-Centric Large Language Models.
  12. IEEE research papers on advanced persistent threats and AI-based intrusion detection
  13. Poojari, R. (2024). Assessing Clinical Natural Language Processing (NLP) Models for Interpreting Electronic Health Records (EHR): Focus on Accuracy, Bias, and Generalizability.
  14. Springer journal articles on enterprise network security and anomaly detection
  15. Santhosh Saai Reddy Purmani. (2026). Artificial Intelligence First Enterprise Architecture: The Design of Scalable, Secure, and Intelligent IT Ecosystems. *American Journal of AI Cyber Computing Management*, 6(1(2)), 1–8. [https://doi.org/10.64751/ajaccm.2026.v6.n1\(2\).pp1-8](https://doi.org/10.64751/ajaccm.2026.v6.n1(2).pp1-8)
  16. Kalae, U. K. (2021). Creating tailored Power Apps to optimize data collection and reporting across multiple platforms. *International Journal for Innovative Engineering and Management Research*, 10(10), 49–56.
  17. Elsevier publications on deep learning-based cyber threat detection
  18. Kalae, U. K. (2020). Developing scalable Power BI dashboards for enhanced data analysis and strategic business decision-making. *International Journal of Enhanced Research in Science, Technology & Engineering*, 9(3), 8–15.
  19. IBM threat intelligence reports and AI-driven cybersecurity studies
  20. Vasagam, M., Kumar, A., & Garg, A. (2026). Learning Execution Plan Embeddings for Multi-Dimensional Query Resource Prediction. *IEEE Access*.
  21. Cisco annual cybersecurity reports on enterprise attacks and threat landscapes
  22. Patyrykin, K. (2025). CANCEL CULTURE PROBLEM. *Lex Localis: Journal of Local Self-Government*, 23.
  23. MITRE ATT&CK framework documentation for advanced persistent threat analysis
  24. Cyril, H. P., & Kumara, S. Identification of Anomalies via Deep Learning-Based Models for High-Dimensional Telecom Traffic Data.
  25. Patel, S., & Patyrykin, K. (2025). Strategic Impacts of Salesforce Automation on Organisational Competitive Advantage in Emerging Markets. *Journal of Posthumanism*, 5(12), 357–372. <https://doi.org/10.63332/joph.v5i12.3782>
  26. Kumara, S. (2025). Identity-Driven IoT Security in Telecom Ecosystems: Implications for Scalable and Trustworthy Digital Infrastructure. *Int. J. Appl. Math*, 38(12s), 2797–2816.