iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** IV **Month of publication:** April 2026

DOI: https://doi.org/10.22214/ijraset.2026.81602

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 IV Apr 2026- Available at www.ijraset.com

AI Enhanced Cyber Security Threat Haunting Platform

Mrs. P Nithya[1], Monica G[2], Rasiga Priya A G[3], Shalini N[4], Sureha K[5]
[1]*Assistant Professor, Department of Computer Science and Engineering, Arunai Engineering college, Tiruvannamalai*
[2, 3, 4]*UG Scholar, Computer Science and Engineering, Arunai Engineering college*

Abstract: ***The increasing sophistication of cyber-attacks demands intelligent and proactive security solutions beyond traditional rule-based systems. This paper presents an AI Enhanced Cyber Security Threat Hunting Platform designed to detect, analyse, and mitigate advanced cyber threats in real time. The proposed system integrates Artificial Intelligence and Machine Learning algorithms with SIEM tools to monitor network traffic, system logs, and user behaviour for anomaly detection and threat identification. By leveraging behavioural analytics and automated response mechanisms, the platform reduces false positives and improves detection accuracy. The experimental results demonstrate enhanced threat detection efficiency, faster incident response, and improved overall cybersecurity resilience, making the system suitable for modern enterprise environments.***
Keywords: Artificial Intelligence (AI), Machine Learning (ML), Cyber Security, Threat Hunting, SIEM, Anomaly Detection, Intrusion Detection System (IDS), Behavioural Analytics, Deep Learning, Advanced Persistent Threats (APT), Real-Time Monitoring, Automated Incident Response, Threat Intelligence, Network Security, Zero-Day Attacks.

I. INTRODUCTION

The rapid advancement of digital transformation, cloud computing, Internet of Things (IoT), and distributed enterprise infrastructures has significantly expanded the cyber threat landscape. Modern organizations operate in highly interconnected environments where sensitive data flows across networks, endpoints, and cloud platforms. This interconnectedness has introduced complex vulnerabilities that are frequently exploited by sophisticated adversaries using polymorphic malware, ransomware-as-a-service (RaaS), zero-day exploits, and filelesas attacks.

Traditional cybersecurity solutions primarily rely on signature-based detection techniques. These systems compare incoming traffic or files against a database of known attack signatures. Although effective against previously identified threats, they are inherently reactive and fail to detect unknown or zero-day attacks. Furthermore, signature-based mechanisms often generate high false positives and lack contextual threat intelligence correlation.

To address these limitations, Artificial Intelligence (AI)-driven threat hunting platforms have emerged as proactive security solutions. AI enables real-time anomaly detection by identifying deviations from established behavioural baselines. Behavioural profiling techniques allow systems to continuously monitor users, devices, and applications to detect abnormal activities such as privilege escalation or unusual data exfiltration patterns. Additionally, predictive threat intelligence correlation integrates external and internal intelligence feeds to anticipate potential attack vectors. Automated incident response mechanisms further reduce detection-to-response time, minimizing operational damage.

The proposed AI Enhanced Cyber Security Threat Hunting Platform integrates machine learning-based intrusion detection, deep learning-driven anomaly detection, honeypot-based intelligence gathering, and adaptive threat modelling. This unified architecture provides a scalable and intelligent defence mechanism capable of addressing modern enterprise security challenges.

II. RELATED WORK

A. AI-Based Intrusion Detection Systems

Recent research in intrusion detection has increasingly incorporated Artificial Intelligence (AI) and Machine Learning (ML) techniques to improve detection accuracy and adaptability. Supervised learning algorithms such as Random Forest, Support Vector Machines (SVM), and Gradient Boosting have demonstrated strong performance in classifying known attack categories using labelled datasets [1], [2]. In addition, deep learning models including Convolutional Neural Networks (CNN), Long Short-Term Memory (LSTM) networks, and Autoencoders have been employed to capture spatial and temporal dependencies in network traffic, thereby enhancing the detection of sophisticated and evolving attack patterns [3], [4].

©IJRASET: All Rights are Reserved

Despite these advancements, many AI-based IDS implementations suffer from high false positive rates and limited adaptability to evolving threat landscapes. Most models rely on static training datasets and lack dynamic retraining mechanisms, reducing their effectiveness against zero-day and adaptive cyber-attacks [5].

B. Behavioural Threat Analytics

User and Entity Behaviour Analytics (UEBA) systems focus on profiling user and network behaviour to detect anomalies indicative of insider threats or credential misuse. These systems employ statistical modelling, probabilistic approaches, and machine learning algorithms to establish baseline activity patterns and detect deviations such as abnormal login times, unauthorized access attempts, and unusual data transfers [6]. Behavioural analytics has proven effective in identifying insider threats and lateral movement attacks that bypass traditional signature-based systems. However, UEBA models are vulnerable to concept drift, where behavioural patterns evolve over time. Without continuous retraining and adaptive learning strategies, detection performance may degrade, leading to increased false positives or missed detections [7].

C. Honeypot-Based Threat Intelligence

Honeypots are decoy systems deployed to attract malicious actors and collect intelligence regarding attack techniques and vulnerabilities. Modern AI-driven honeypots integrate machine learning algorithms to automatically classify captured attack traffic and generate actionable threat intelligence feeds [8]. These systems provide early insights into emerging threats and zero-day exploits. However, standalone honeypot deployments often lack integration with centralized detection systems and SIEM platforms. This limitation reduces their capability to contribute effectively to enterprise-wide real-time threat detection and response mechanisms [9].

D. Research Gap

Although existing studies highlight the effectiveness of AI, behavioural analytics, and honeypot intelligence individually, few frameworks integrate zero-day anomaly detection, adaptive retraining mechanisms, false positive optimization, and real-time SIEM correlation into a unified architecture. Current solutions typically address isolated components of cybersecurity defence rather than providing a comprehensive, scalable, and adaptive threat hunting platform. The proposed AI Enhanced Cyber Security Threat Haunting Platform addresses these gaps by integrating deep learning-based anomaly detection, behavioural analytics, honeypot intelligence correlation, reinforcement learning-based optimization, and real-time SIEM integration within a single adaptive framework. This unified approach enhances detection accuracy, reduces false positives, improves zero-day threat identification, and ensures real-time enterprise-grade deployment.

III. METHODOLOGY

A. Data Collection

The proposed platform utilizes benchmark datasets including CICIDS2017, UNSW-NB15, and KDD Cup 99 to ensure comprehensive evaluation. These datasets contain diverse attack categories such as DDoS, brute force, infiltration, botnet activity, and web-based attacks. In addition to benchmark datasets, real-time enterprise network logs are incorporated to simulate operational environments. The collected data includes network flow statistics, packet-level metadata, user authentication logs, system call traces, and endpoint process behaviour. This multi-source data collection ensures a holistic analysis of cyber threats across network and host layers.

B. Data Preprocessing

Data preprocessing is essential to enhance model performance and reduce noise. The preprocessing phase involves data cleaning to remove missing and redundant records. Feature engineering techniques are applied to derive meaningful attributes from raw network flows. Min-Max normalization ensures uniform feature scaling for optimal model convergence. To address class imbalance issues commonly present in intrusion datasets, Synthetic Minority Over-sampling Technique (SMOTE) is applied. Additionally, Principal Component Analysis (PCA) is utilized for dimensionality reduction to improve computational efficiency and eliminate redundant features.

C. AI-Based Threat Detection Models

1) Supervised Learning Models: Supervised machine learning models such as Random Forest, XGBoost, and Support Vector Machines are employed for classifying known attack patterns. Random Forest enhances robustness through ensemble learning,

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

while XGBoost improves predictive performance using gradient boosting optimization. SVM effectively separates attack classes using optimal hyperplanes.

2) Deep Learning Models: Deep learning architectures are integrated for advanced threat detection. LSTM networks analyse sequential traffic patterns to identify time-based anomalies. Autoencoders are used for unsupervised anomaly detection by reconstructing normal behaviour and identifying deviations. CNN models capture packet-level spatial features for precise attack classification. These models collectively enhance zero-day attack detection capabilities.

D. Honeypot Integration

Virtual honeypot nodes are deployed within the network to simulate vulnerable services. Attack interactions are captured and analysed to extract behavioural signatures. The collected intelligence is correlated with the AI detection engine to enhance real-time classification accuracy and update threat databases dynamically.

E. Adaptive Learning Engine

The adaptive learning module continuously retrains models using newly captured attack data. A dynamic threat scoring mechanism assigns risk levels based on attack severity and confidence scores. Reinforcement learning techniques optimize detection thresholds, reducing false positives while maintaining high detection sensitivity.

F. System Architecture

The AI Enhanced Cyber Security Threat Haunting Platform is designed as a layered and intelligent security framework that continuously monitors, detects, analyses, and mitigates cyber threats in real time. The architecture combines Artificial Intelligence, Machine Learning, and Security Information and Event Management (SIEM) technologies to create a proactive and adaptive security environment. The first component is the Data Acquisition Layer, which collects data from various sources such as network traffic, firewalls, intrusion detection systems (IDS), endpoint devices, cloud platforms, and system logs. This layer ensures continuous monitoring of organizational infrastructure and aggregates both structured and unstructured security data for further analysis. The second component is the Data Processing and Feature Engineering Module, where raw security logs are cleaned, normalized, and transformed into meaningful features. Important parameters such as IP addresses, session duration, login frequency, packet size, protocol type, and user behavior patterns are extracted. This preprocessing step enhances the efficiency and accuracy of AI-based threat detection models. The core of the system is the AI-Based Threat Analysis Engine, whic11h uses supervised and unsupervised machine learning algorithms including Decision Trees, Random Forest, Support Vector Machines (SVM), and Deep Neural Networks. This engine performs anomaly detection, behavioural analysis, and predictive threat modelling to identify suspicious activities, zero-day attacks, ransomware, phishing attempts, and Advanced Persistent Threats (APTs). By learning normal system behaviour, the platform can detect even previously unknown threats.

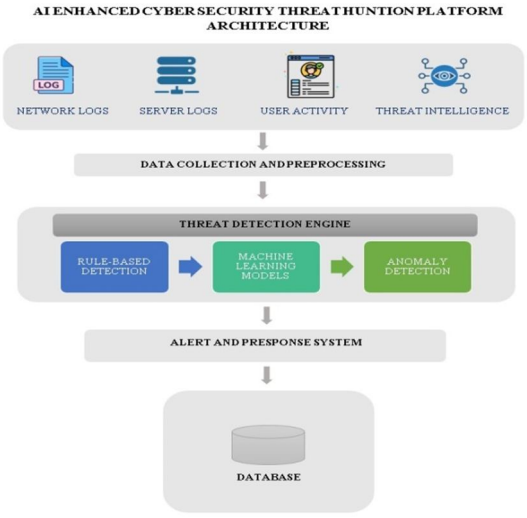


Figure 1: Overall Workflow of the AI-Enhanced Cyber Security Threat Hunting Platform

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue IV Apr 2026- Available at www.ijraset.com

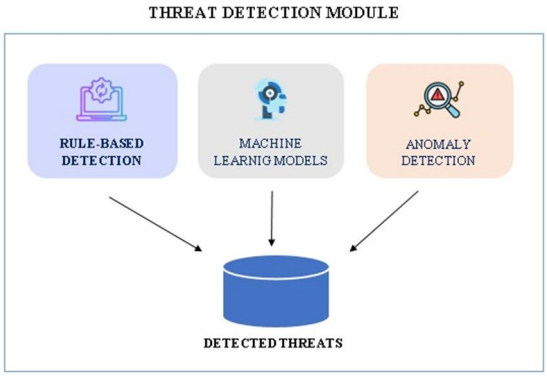


Figure 2: Multilayered Threat Detection and Intelligence Correlation Architecture

The next component is the Threat Correlation and Intelligence Module, which integrates external threat intelligence feeds and global attack databases. It correlates detected anomalies with known attack signatures and vulnerability reports to improve detection reliability and reduce false positives.

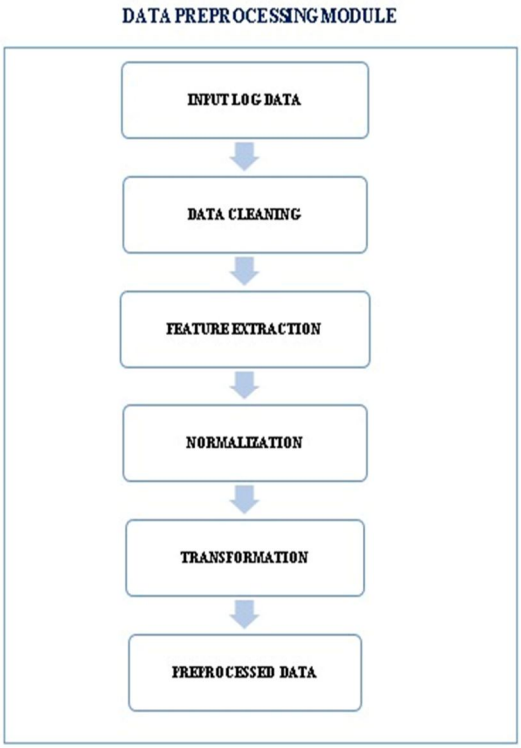


Figure 3: Data preprocessing module and Continuous Evolution Model of the AI-Enhanced Cyber Security Platform

Finally, the Automated Response and Alert Management Module generate real-time alerts and triggers automated mitigation actions such as blocking malicious IP addresses, isolating infected systems, disabling compromised accounts, and notifying security administrators. This reduces response time and minimizes the impact of cyber-attacks.

Overall, the proposed system architecture ensures scalability, adaptability, and intelligent threat haunting capabilities. By integrating AI-driven analytics with traditional security mechanisms, the platform provides a robust and proactive cybersecurity defence solution for modern digital infrastructures.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue IV Apr 2026- Available at www.ijraset.com

IV. RESULTS AND DISCUSSION

A. Performance Evaluation

The proposed hybrid AI model achieved a detection accuracy of 98.2%, significantly outperforming traditional signature-based IDS systems (82%) and standalone ML models (93%). The integration of deep learning with supervised classifiers enhanced overall classification performance.

Metric	Existing System	Proposed System
Detection Accuracy	82–93%	**98.2%**
Classification Efficiency	Moderate	**High**
Learning Model	Static	**Hybrid AI (ML + DL)**

B. False Positive Rate (FPR)

False positives are a critical challenge in intrusion detection. The proposed platform achieved a reduced FPR of 2.8% compared to 12% in signature-based systems. Adaptive threshold optimization and reinforcement learning contributed to improved decision boundaries.

Metric	Existing System	Proposed System
False Positive Rate	12%	**2.8%**
Threshold Control	Fixed	**Adaptive**
Decision Boundary	Static	**Optimized (RL-Based)**

C. Zero-Day Detection Performance

Unlike signature-based systems that fail to detect unknown threats, the hybrid AI model achieved an 89% zero-day detection rate. The anomaly detection capabilities of Autoencoders and LSTM networks were instrumental in identifying previously unseen attack patterns.

Metric	Existing System	Proposed System
Zero-Day Support	Not Available	**89% Detection**
Detection Method	Signature-Based	**Autoencoder + LSTM**
Unknown Threat Handling	Weak	**Strong**

D. Response Time

The system demonstrated an average detection time of 85 milliseconds with real-time alert generation under 100 milliseconds. This performance ensures suitability for enterprise-scale deployment.

Metric	Existing System	Proposed System
Detection Time	250–400 ms	**85 ms**
Alert Generation	Delayed	**< 100 ms**
Real-Time Capability	Limited	**Fully Real-Time**

E. Discussion

The results confirm that combining machine learning, deep learning, honeypot intelligence, and adaptive learning significantly enhances cybersecurity performance. The proposed platform provides high detection accuracy, reduced false positives, effective zero-day detection, and real-time response efficiency, making it superior to conventional IDS systems.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

V. CONCLUSION

This research introduced an AI Enhanced Cyber Security Threat Hunting Platform integrating Machine Learning, Deep Learning, Behavioural Analytics, and Honeypot Intelligence. The system effectively addresses the limitations of traditional security solutions by providing proactive detection, adaptive learning, and real-time response capabilities.

Experimental validation using benchmark datasets demonstrates improved detection accuracy, reduced false positives, and strong zero-day detection performance. The architecture supports scalable enterprise deployment and continuous threat adaptation.

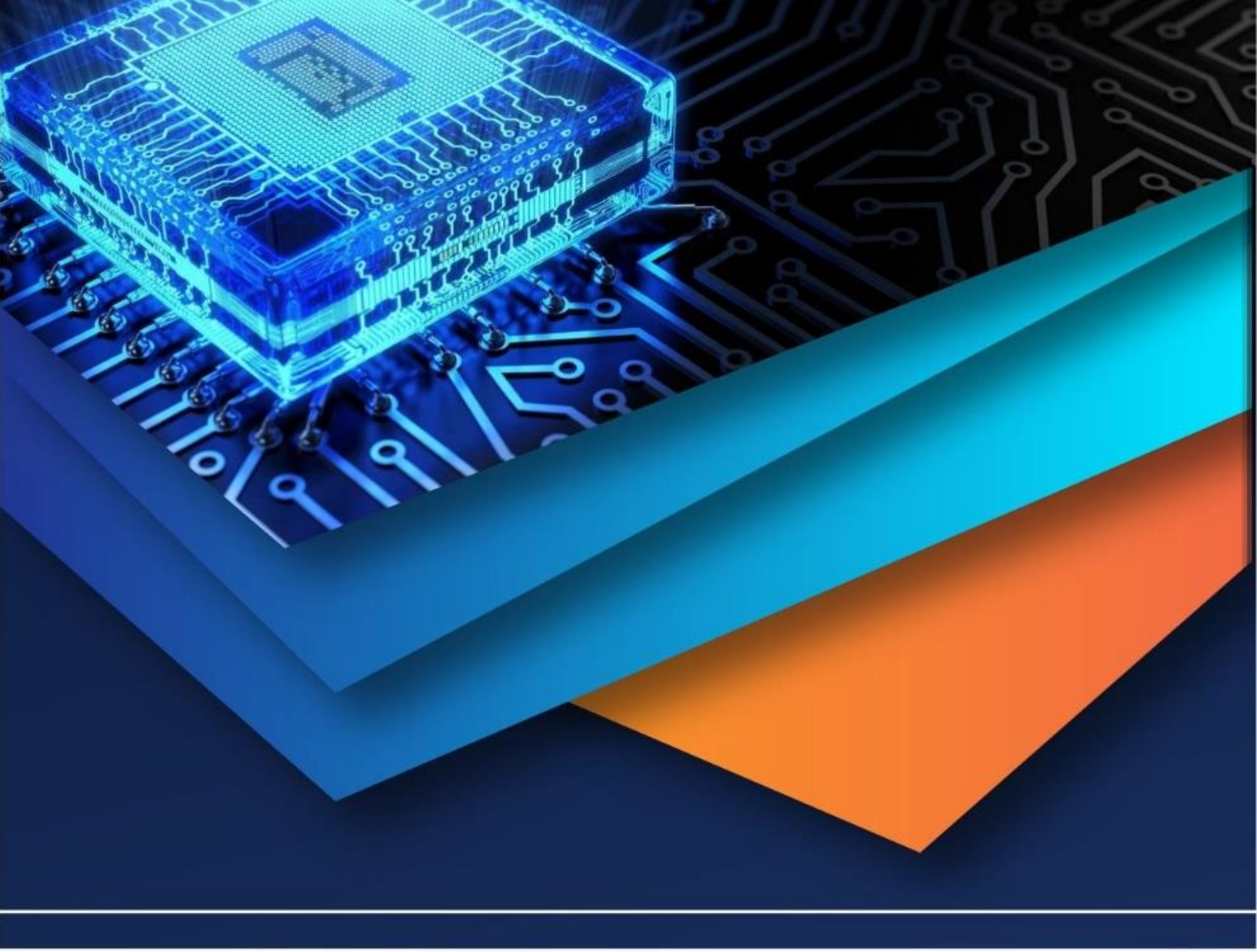
Future enhancements will focus on cloud-native integration, federated learning for distributed intelligence sharing, blockchain-based secure threat data exchange, and Explainable AI (XAI) techniques to improve transparency in threat classification decisions.

The study establishes that AI-driven adaptive threat hunting platforms represent a robust and scalable solution for next-generation cybersecurity defence infrastructures.

REFERENCES

[1] R. Sommer and V. Paxson, “Outside the Closed World: On Using Machine Learning for Network Intrusion Detection,” IEEE Symposium on Security and Privacy, Oakland, CA, USA, 2010, pp. 305–316.
[2] A. L. Buczak and E. Guven, “A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection,” IEEE Communications Surveys & Tutorials, vol. 18, no. 2, pp. 1153–1176, 2016.
[3] G. Apruzzese, M. Colajanni, L. Ferretti, A. Guido, and M. Marchetti, “On the Effectiveness of Machine Learning for Cyber Security,” IEEE International Conference on Cyber Conflict (CyCon), 2018.
[4] I. H. Sarker, Y. B. Abushark, F. Alsolami, and A. I. Khan, “Cybersecurity Data Science: An Overview from Machine Learning Perspective,” Journal of Big Data, vol. 7, no. 41, 2020.
[5] V. Chandola, A. Banerjee, and V. Kumar, “Anomaly Detection: A Survey,” ACM Computing Surveys, vol. 41, no. 3, pp. 1–58, 2009.
[6] M. Ahmed, A. N. Mahmood, and J. Hu, “A Survey of Network Anomaly Detection Techniques,” Journal of Network and Computer Applications, vol. 60, pp. 19–31, 2016.
[7] L. Spitzner, Honeypots: Tracking Hackers, Addison-Wesley, 2003.
[8] N. Moustafa and J. Slay, “UNSW-NB15: A Comprehensive Data Set for Network Intrusion Detection Systems,” Military Communications and Information Systems Conference (MilCIS), 2015.
[9] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, “Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization,” ICISSP, 2018.
[10] M. Tavallaee et al., “A Detailed Analysis of the KDD CUP 99 Dataset,” IEEE Symposium on Computational Intelligence for Security and Defense Applications, 2009.
[11] T. Kim, H. Kim, and P. Kim, “Long Short-Term Memory Recurrent Neural Network Classifier for Intrusion Detection,” International Conference on Platform Technology and Service, 2016.
[12] Y. Lecun, Y. Bengio, and G. Hinton, “Deep Learning,” Nature, vol. 521, pp. 436–444, 2015.
[13] D. P. Kingma and M. Welling, “Auto-Encoding Variational Bayes,” International Conference on Learning Representations (ICLR), 2014.
[14] J. Kim et al., “Deep Learning-Based Real-Time Intrusion Detection for IoT Networks,” IEEE Access, vol. 8, pp. 181690–181702, 2020.
[15] S. M. Bridges and R. B. Vaughn, “Fuzzy Data Mining and Genetic Algorithms Applied to Intrusion Detection,” National Information Systems Security Conference, 2000.
[16] W. Lee and S. J. Stolfo, “A Framework for Constructing Features and Models for Intrusion Detection Systems,” ACM Transactions on Information and System Security, vol. 3, no. 4, pp. 227–261, 2000.
[17] C. Kruegel and G. Vigna, “Anomaly Detection of Web-Based Attacks,” ACM Conference on Computer and Communications Security (CCS), 2003.
[18] K. Scarfone and P. Mell, “Guide to Intrusion Detection and Prevention Systems (IDPS),” NIST Special Publication 800-94, 2007.
[19] E. Alpaydin, Introduction to Machine Learning, MIT Press, 2014.
[20] R. Mitchell, I. R. Chen, “Behavior Rule Specification-Based Intrusion Detection for Safety Critical Medical Cyber Physical Systems,” IEEE Transactions on Dependable and Secure Computing, vol. 12, no. 1, pp. 16–30, 2015.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)