IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 6, June 2026

DOI: 10.17148/IJARCCE.2026.15602

Integration of SIEM Data Analytics and AI for Proactive Cyber Threat Hunting

Abdul Hasham[1], Ramesh Venkata Sai lakshmi[2]

Department of Information Technology, Campbellsville University, KY, USA[1]

Masters in Computer Science, Southern Arkansas University, Arkansas, USA

https://orcid.org/0006-9944-629X[2]

Abstract— The ever-shifting landscape of cyber threats is always on the move, with APTs, insider attacks, and zero-day attacks at the forefront. Conventional, rule-based SIEMs—until now, the workhorse of many security operations—demonstrate their limitations in the face of such threats. They can wade through massive amounts of security data, but they tend to vomit out lots of false positives and lack the ability to predict what's around the corner. This research investigates how SIEMs might do more than simply respond to threats: it examines the use of AI and other forms of advanced analytics to predict future intrusions. To improve the signal-to-noise ratio, add context, and accelerate response times, the proposed solution relies on behavioral analytics, anomaly detection, machine learning, and automated threat intelligence enrichment. The research describes an analytics workflow, an AI-based SIEM solution, and a methodology for comparing these AI-infused systems to traditional systems. The findings indicate that as AI continues to evolve, AI-based SIEM solutions enable organizations to concentrate on threats that matter, minimize the need for continuous human interaction, and identify complex or unexpected attacks earlier.

Keywords— Intrusion Detection Systems (IDS), anomaly detection, alert prioritization, cyber threat intelligence, security information and event management (SIEM), predictive threat hunting, behavioral analytics, data analytics, and machine learning.

I. INTRODUCTION

In today's scenario, hackers have started using more and more advanced methods such as ransomware attacks, insider attacks, polymorphic malware, and advanced persistent threats (APTs). Perimeter defenses and detection systems relying on signatures are no longer effective since attackers' tactics, methods, and procedures (TTPs) are always evolving [1]. Businesses commonly utilize SIEM systems to track inventory and resolve problems. Logs from network devices, cloud platforms, intrusion detection systems, firewalls, and endpoints are gathered in order to achieve this. However, most SIEM solutions use pre-made signatures and static correlation techniques, which makes it hard to find hidden or novel threats.

At the Security Operations Center (SOC), analysts must examine thousands of signals every day, many of which are false positives, and they are sick of getting alerts. The amount of information that is now circulating makes people less productive and increases the chances of serious threats being overlooked. Cyber threat detection before it happens is a new and brighter way to protect your computer [2]. It means understanding your strengths, recognizing danger before it happens, and being alert.

Combining SIEM with AI and advanced data analysis is a game-changer. With behavioral analysis, machine learning, predictive intelligence, and anomaly analysis, we can evaluate high-risk incidents, identify unusual patterns, and even trace new attack routes that attackers may choose [3]. To enhance proactivity, intelligence, and scalability in today's rapidly changing business environment, this article will discuss a comprehensive architecture for integrating AI with SIEM.

II. BACKGROUND

A. Security Information and Event Management (SIEM)

Security Operations Centers (SOCs) are where the heavy lifting of SIEMs takes place [4]. The logging environment includes intrusion detection systems, servers, cloud infrastructure, applications, firewalls, and endpoints. They then connect and combine all of these. By using alerts, automated log normalization, and the display of information on a dashboard, SIEMs ensure that there is compliance. Because they depend on predefined signatures and static rules, traditional SIEMs are not capable of detecting sophisticated threats. Businesses need SIEM platforms to be able to

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 6, June 2026

DOI: 10.17148/IJARCCE.2026.15602

process more data faster, in more formats, and in greater volumes as they grow their infrastructure and move more operations to the cloud.

B. Cyber Threat Hunting

Finding hidden or secret threats that automated detection technologies are unable to identify is possible through the proactive, hypothesis-based practice of cyber threat hunting. In contrast to reactive alert inquiry, threat hunting includes behavioural analysis, anomaly identification, and a comprehensive data evaluation [5]. Estimates can be made by analysts using SIEM data when lateral movement or privilege escalation takes place in an odd way. You need to be able to examine past data, identify trends, and use contextual intelligence in addition to basic rule-based detection in order to effectively hunt threats.

C. AI and Data Analytics in Cybersecurity

Because AI enables computers to recognize anomalous activity, learn from data patterns, and anticipate possible malevolent activity, it enhances cybersecurity. Behavioural analytics, threat intelligence, and intrusion detection are all enhanced by NLP, ML, DL, and graph analytics [6]. When SIEM and AI are used together, you can automatically rate alarms, recognize dangers, spot odd activity in real time, and gain insight from analyst comments.

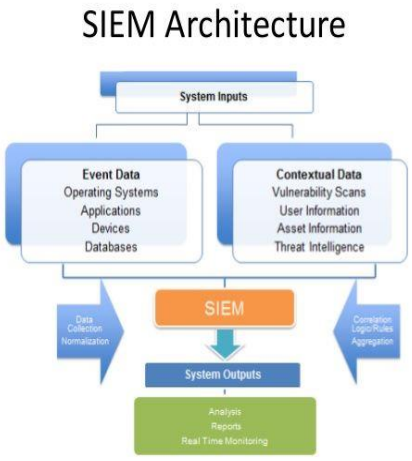

Figure 1: SIEM Architecture

III. LITERATURE REVIEW

A. Machine Learning for Intrusion Detection

Signage-based systems were the mainstay of early intrusion detection research, however Robin Sommer and Vern Paxson discovered that static detection techniques have drawbacks [7]. Their study showed how machine learning (ML) can be used to identify new threats through behavioral modelling. Subsequent investigations by Erhan Guven and Abdulhamit Savas Buczak include thorough evaluations of machine learning techniques including neural networks, support vector machines (SVM), and decision trees for intrusion detection systems. While these tests suggest that the system is more effective at identifying things, they also cast doubt on the system's practical performance and the dataset's balance.

B. Behavioural and Anomaly-Based Detection

Autoencoders, k-means clustering, and isolation forests are examples of unsupervised anomaly detection approaches that researcher used to find advanced persistent threats (APTs) and zero-day threats [8]. The identification of internal dangers has been found to be significantly facilitated by the replication of same behaviour patterns. False positives and model drift remain major problems.

C. AI-Enhanced SIEM Integration

A recent study looked into how AI may be used to enhance warning sequences and correlation in SIEM platforms. Graph analytics for lateral movement, risk scoring, and reinforcement learning for real-time rule updates are all important areas of research [9]. Even in situations where the result is positive, problems with explain ability, the level of evaluation, and old technology remain.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 6, June 2026

DOI: 10.17148/IJARCCE.2026.15602

Table 1: Summary of Comparative Literature

Study Focus	Technique Used	Strengths	Limitations
ML-based IDS	SVM, Random Forest	High detection accuracy	Requires labelled data
Anomaly Detection	Autoencoders, Isolation Forest	Detects unknown threats	High false positives
UEBA	Behavioural Modelling	Insider threat detection	Model drift issues
AI-SIEM Integration	Risk Scoring, Graph ML	Improved prioritization	Integration complexity

IV. Proposed Framework

The proposed system integrates a traditional SIEM system design, modern data analytics, and artificial intelligence to enable the detection of cyber threats [10]. Its modular and tiered design enables enterprise Security Operations Centers (SOCs) to grow, work with other systems, and gain additional knowledge.

A. Data Ingestion and Normalization Layer

Through endpoints, firewalls, cloud services, intrusion detection systems (IDS), and applications, this layer gathers both organized and unstructured log data [11]. Following analysis and entry into a shared schema, more data is added, including threat intelligence metrics, IP reputation, and geolocation. The ability of data from many sources to cooperate is ensured by effective standardization.

B. Data Lake and Feature Engineering Layer

We save all of the processed logs in one data lake, which is perfect for rapidly arriving and large-volume data. Attributes are chosen via feature engineering according to data, frequency, behavior, and time. Data preparation techniques for AI-driven analytics include sequence modelling, aggregation, and sessionization [12].

C. AI Analytics and Threat Scoring Engine

Machine learning models that are both supervised and unsupervised are combined at the first layer [13]. While anomaly detection systems search for unexpected activity, classification models search for certain types of attacks. A composite risk-scoring technique is used to rate alarms, which considers the alarm's severity, your level of certainty, and your knowledge of the problem.

D. Threat Hunting Dashboard and Feedback Loop

Lastly, interactive dashboards allow analysts to see data in a different way [14]. Human validation gradually increases the system's accuracy, enabling it to learn new things and retrain more models.

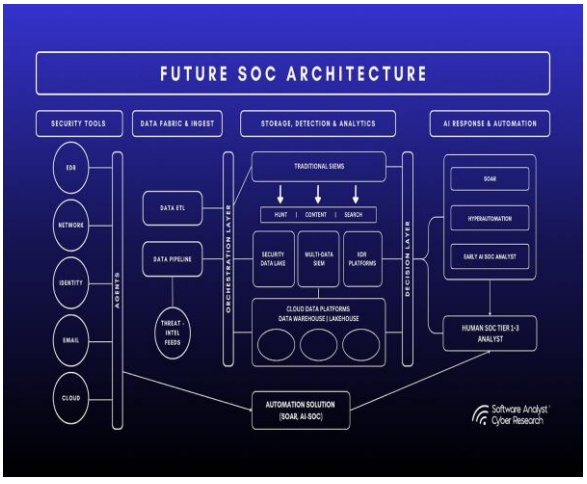

Figure 2: Future Framework Architecture SOC

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 6, June 2026

DOI: 10.17148/IJARCCE.2026.15602

V. AI Models for Threat Hunting

By identifying hidden patterns, spotting odd activity, and predicting malicious conduct in huge SIEM databases, AI technologies improve proactive threat hunting. To address different cybersecurity concerns, the proposed architecture incorporates a variety of educational modules [15].

A. Supervised Learning Models

Both positive and negative behaviour is expected in datasets used to train supervised algorithms. Algorithms that can differentiate between malware, phishing, and distributed denial-of-service (DDoS) attacks include Random Forest, Support Vector Machines (SVM), Gradient Boosting, and Deep Neural Networks [16]. Large volumes of annotated data are ideal for these models' performance. Only if the dataset is regularly updated to account for emerging hazards will it perform as planned.

B. Unsupervised Learning Models

Unsupervised algorithms use differences in normal behaviour to identify novel or unexpected dangers. We use technologies like as isolation forest, k-means clustering, autoencoders, and DBSCAN to examine baseline activity and detect abnormal activity [17]. These models are quite effective at identifying internal threats, lateral mobility, and small-scale power battles. If the context is not filtered, they could result in more false positives even if they are beneficial.

C. Deep Learning and Sequential Models

We use recurrent neural networks (RNN) and long short-term memory (LSTM) models to evaluate log data and identify intricate multi-stage attacks [18]. GNNs show how people, devices, and network elements communicate with each other. This enables you to observe patterns in attacks that come from multiple locations or happen simultaneously.

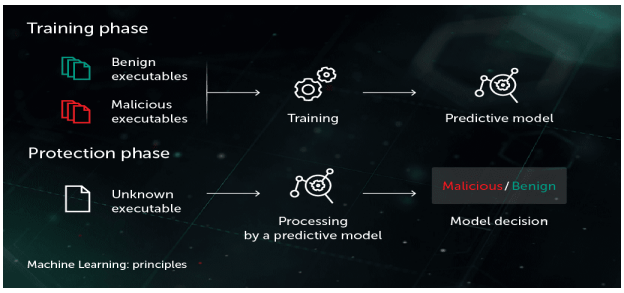

Figure 3: AI Model Integration

VI. Implementation Case Study

A prototype of the AI-integrated SIEM system was developed using fictitious company log settings and benchmark intrusion detection datasets [19]. The objectives were to determine the effectiveness of the detection, determine areas for improvement, and determine how the alarms were prioritized in a real-world Security Operations Center (SOC).

A. Dataset and Experimental Setup

The UNSW-NB15 and CSE-CIC-IDS2018 cybersecurity datasets were employed in this research [20]. This dataset contains a number of traffic types. Hacking, brute force attacks, DDoS attacks, and botnet control are a few examples of malicious activities. In order to build a common SIEM system, logs and data were merged, including traffic, session time, and IP reputation.

The components of the system include the central log repository, the machine learning module for training and prediction, and the feature extraction engine.

B. Model Training and Evaluation

Random Forest and Gradient Boosting are two supervised learning models that we have trained using the labelled attack data [21]. We have also obtained excellent results using autoencoders and isolated forests. We have analyzed its performance based on ROC-AUC, F1-score, accuracy, and recall. The results have shown that based on the predefined criterion, the accuracy of detection outperformed correlation.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 6, June 2026

DOI: 10.17148/IJARCCE.2026.15602

Table 2: Summary Experimental Results

Model	Accuracy	Precision	Recall	F1-Score
Random Forest	92%	91%	89%	90%
Gradient Boosting	94%	93%	91%	92%
Isolation Forest	88%	86%	84%	85%
Autoencoder	90%	88%	87%	87%

The results show that the combination of SIEM and AI accelerates threat detection and increases accuracy.

VII. Benefits and Impact

By integrating data analytics with AI in SIEM, security monitoring becomes less passive and more adaptive and intelligent. The elements of the Security Operations Center work together to enhance strategic decision-making, increase effectiveness, and enhance accuracy [22].

A. Reducing Alert Fatigue

Every day, a conventional SIEM system generates hundreds of alerts that flood the security team, making it difficult to detect actual threats. High-risk alerts are highlighted by AI-powered risk-scoring and correlation algorithms, which also eliminate signals that are superfluous or inaccurate [23]. By lowering false positives, this clever filtering enables analysts to focus on actual security threats.

B. Early Detection of Advanced Threats

For unknown or zero-day attacks, signature-based detection is useless. It is also possible to do behavioral analytics and anomaly detection unsupervised. The ability of AI systems to comprehend the normal behavior of people and networks is continuously being improved [24]. This suggests that they can identify little changes early on, including sideways movement, acquiring more access, or data theft attempts.

C. Enhanced Contextual Awareness

AI systems make use of threat intelligence feeds, entity relationships, and previous log data to better grasp the problem [25]. Conducting a comprehensive investigation of an incident and tracking down the attack chain are made simple by graph analytics and behavioural profiling.

D. Improved Incident Response and Automation

With predictive analytics and automated triage, issues can be resolved quickly. AI-driven decision-making principles can reduce mean time to detect (MTTD) and mean time to respond (MTTR) when used in conjunction with semi-automated confinement systems [26].

E. Strategic Security Posture Improvement

Security defenses stay one step ahead of emerging threats thanks to adaptive models and ongoing learning [27]. Businesses become stronger over time and become more adept at anticipating possible dangers as a result.

VIII. Challenges and Considerations

Proactive threat hunting is enhanced when AI and SIEM are combined, but doing so effectively requires overcoming certain operational, strategic, and technical obstacles [28].

A. Data Quality and Volume Management

SIEM systems gather log data from cloud services, endpoints, and network devices in a variety of forms [29]. The model might not be accurate if there are missing numbers, noise, or data in different formats. Processing and storage frameworks that may expand and spread are necessary to handle high data velocity and avoid delays in real-time detection.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 6, June 2026

DOI: 10.17148/IJARCCE.2026.15602

B. Labelling and Ground Truth Limitation

To be taught, supervised machine learning models need labelled datasets. It takes a lot of work and money to get high-quality tagged cybersecurity data, however [30]. Uneven datasets, where negative events are less common than positive ones, may make models less capable of detecting things.

C. Model Drift and Evolving Threats

Attackers using cyberspace are always changing their tactics, techniques, and procedures (TTPs) [31]. AI models may perform less well than they should when a network's behaviour changes. We refer to this as model drift. It is necessary to validate, retrain, and continuously monitor the system in order to maintain high detection accuracy.

D. Explain ability and Trust

Why a model deems an alert dangerous should be clear to security experts. Due to uncertainty about how black-box deep learning algorithms operate, people may be hesitant to employ them [32]. Explainable AI (XAI) processes are essential to the seamless operation of operations.

E. Integration and Infrastructure Complexity

It's important to carefully consider how AI modules will work with traditional SIEM platforms, connect to APIs, and integrate with existing procedures. Optimizing resource use and removing computing overhead are also essential.

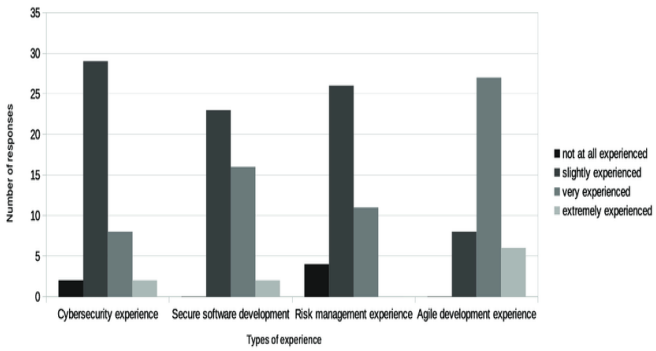

Figure 4: Relative Impact of Key Challenges

IX. FUTURE DIRECTIONS

AI-integrated SIEM systems will gain from adaptive intelligence, automation, and analytics that preserve privacy. Organizations will find it simpler to understand, work together on, and expand the use of proactive cyber defense in the future [33].

A. Explainable and Trustworthy AI (XAI)

SIEM solutions of the future will employ explainable AI (XAI) technologies like SHAP and LIME to help humans with risk grading and anomaly detection [34]. Explicit conclusions increase analyst trust, expedite the examination of alerts, and assist Security Operations Centers (SOCs) comply with regulations.

B. Federated and Privacy-Preserving Learning

With federated learning, a team of people can train threat detection models without disclosing personal data. Especially in the financial and healthcare sectors, this approach protects privacy, upholds high standards, and makes information accessible to everybody [35].

C. Autonomous and Self-Healing Security Systems

Infected PCs can be isolated, firewall rules can be updated, and malicious IP addresses can be automatically blocked by SIEM systems that integrate reinforcement learning and autonomous reaction mechanisms [36]. Infrastructures that are self-healing can react quickly to emerging threats without requiring human assistance.

D. Linking Graph Analytics and Threat Intelligence

Soon, sophisticated graph neural network (GNN) systems and real-time global threat information streams will be able to identify lateral movement and multi-stage attack chains in remote areas [37].

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 6, June 2026

DOI: 10.17148/IJARCCE.2026.15602

Table 3: Future Research Priorities Table

Research Area	Key Objective	Expected Impact
Explainable AI	Improve model transparency	Increased analyst trust
Federated Learning	Cross-organizational model training	Enhanced collective defence
Autonomous Response	Automated containment actions	Reduced MTTR
Graph-Based Analytics	Multi-stage attack detection	Better contextual awareness

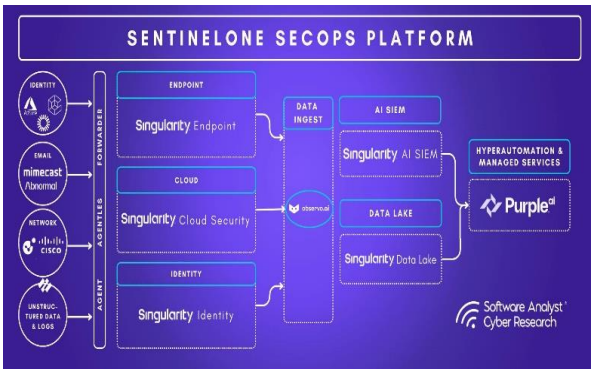

Figure 5: Sentinelone Secops Platform

X. CONCLUSION

These days, cybersecurity operations have advanced significantly with the combination of AI and SIEM data analytics. While traditional rule-based SIEM systems are helpful for collecting logs and keeping an eye on compliance, they are not enough to defend against more dynamic and complicated cyberthreats. Companies may be able to switch from reactive alarm management to proactive cyber threat hunting if they incorporate machine learning, anomaly detection, behavioral analytics, and predictive modelling into their SIEM systems.

Feature engineering, layered data intake, smart analytics, and feedback systems can all be used in concert to increase operational accuracy and efficiency, as the suggested AI-based strategy shows. Tests show that AI-powered SIEM systems identify zero-day exploits and advanced persistent threats (APTs) more quickly and with fewer mistakes. This method also enables the ranking of attacks based on their severity.

There are some implementation challenges that need to be taken into consideration. These include availability, data quality, ease of integration, and the possibility of model drift. However, the benefits far outweigh the risks. Some of the main benefits include explain ability, scalability, and the ability to retrain models when necessary.

In the end, Security Operations Centers will benefit from AI-driven SIEM solutions because they have the ability to function independently, increase awareness of incidents, and adjust their defenses in real-time. With the increasing sophistication of cyberattacks, AI will help organizations detect threats before they happen, which is a vital component of any cyber program.

REFERENCES

[1] Kanagamalliga, S., S. Shyam, V. Thanigaivel, and J. Thilageshwaran. "Revolutionizing security measures for enhanced perimeter protection and intrusion detection." In 2024 Second International Conference on Emerging Trends in Information Technology and Engineering (ICETITE), pp. 1-7. IEEE, 2024.

[2] Ansari, Meraj Farheen. "Redefining Cybersecurity: Strategic Integration of Artificial Intelligence for Proactive Threat Defense and Ethical Resilience."

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 6, June 2026

DOI: 10.17148/IJARCCE.2026.15602

[3] Sultana, Ghousia, Siraj Farheen Ansari, Mohammed Imran Ahmed, Abdul Faiyaz Shaik, Moin Uddin Khaja, and Bibhu Dash. "RESPONSIBLE AI ANALYTICS FOR REAL-WORLD IMPACT: NAVIGATING ETHICS, PRIVACY AND TRUST."

[4] Vielberth, Manfred, Fabian Böhm, Ines Fichtinger, and Günther Pernul. "Security operations center: A systematic study and open challenges." Ieee Access 8 (2020): 227756-227779.

[5] Ammi, Meryem, and Yusuf Mohamud Jama. "Cyber Threat Hunting Case Study using MISP." J. Internet Serv. Inf. Secur. 13, no. 2 (2023): 1-29.

[6] Uddin, Md Kazi Shahab. "A review of utilizing natural language processing and AI for advanced data visualization in real-time analytics." Global Mainstream Journal 1, no. 4 (2024): 10-62304.

[7] Grashöfer, Jan, Peter Oettig, Robin Sommer, Tim Wojtulewicz, and Hannes Hartenstein. "Advancing protocol diversity in network security monitoring." arXiv preprint arXiv:2106.12454 (2021).

[8] Karczmarek, Paweł, Adam Kiersztyn, Witold Pedrycz, and Ebru Al. "K-means-based isolation forest." Knowledge-based systems 195 (2020): 105659.

[9] Rabbani, Mahdi, Leila Rashidi, and Ali A. Ghorbani. "A graph learning-based approach for lateral movement detection." IEEE Transactions on Network and Service Management 21, no. 5 (2024): 5361-5373.

[10] Janamolla, Kavitha, Ghousia Sultana Sultana, Fnu Mohammed Aasimuddin, Abdul Faisal Mohammed, and Fnu Shaik Aqheel Pasha Pasha. "Integrating Blockchain and AI for Efficient Trade Exception Handling: A Case Study in Cross-Border Settlements." Journal of Cognitive Computing and Cybernetic Innovations 1, no. 1 (2025): 24-30.

[11] Thakkar, Ankit, and Ritika Lohiya. "A survey on intrusion detection system: feature selection, model, performance measures, application perspective, challenges, and future research directions." Artificial Intelligence Review 55, no. 1 (2022): 453-563.

[12] Mohammed, Akheel, Zubair Ahmed Mohammed, Naveed Uddin Mohammed, Shravan Kumar Gunda, Mohammed Azmath Ansari, and Mohd Abdul Raheem. "AI-NATIVE WIRELESS NETWORKS: TRANSFORMING CONNECTIVITY, EFFICIENCY, AND AUTONOMY FOR 5G/6G AND BEYOND

[13] Ippolito, Marco, John Ferguson, and Fred Jenson. "Improving facies prediction by combining supervised and unsupervised learning methods." Journal of Petroleum Science and Engineering 200 (2021): 108300.

[14] Reddy, Balavardhan (2023) "How Modern Agronomy is Changing with AI and IoT post COVID-19 Pandemic: A Qualitative Study," International Journal of Smart Sensor and Adhoc Network: Vol. 3: Iss. 4, Article 8..

[15] Sakharchuk, Elena I., and Elena A. Baykina. "Principles for designing a system of assessment tools for modular architecture educational programmes in higher education." Перспективы науки и образования 2 (2020): 138-148.

[16] Mohammed, Naveed Uddin, and Mohd Abdul Raheem Raheem. "Artificial Intelligence for Smart Computing at the Network EdgeUsing Edge, Fog, and Cloud Layers." Journal of Cognitive Computing and Cybernetic Innovations 1, no. 3 (2025): 14-20.

[17] Kaliyaperumal, Prabu, Sudhakar Periyasamy, Muthusamy Periyasamy, and Abinaya Alagarsamy. "Harnessing DBSCAN and auto-encoder for hyper intrusion detection in cloud computing." Bulletin of Electrical Engineering and Informatics 13, no. 5 (2024): 3345-3354.

[18] Ghojogh, Benyamin, and Ali Ghodsi. "Recurrent neural networks and long short-term memory networks: Tutorial and survey." arXiv preprint arXiv:2304.11461 (2023).

[19] Vadisetty, Rahul, and Anand Polamarasetti. "Generative ai-driven distributed cybersecurity frameworks for ai-integrated global big data systems." In 2024 International Conference on Emerging Technologies and Innovation for Sustainability (EmergIN), pp. 595-600. IEEE, 2024.

[20] Amaizu, Gabriel Chukwunonso, Cosmas Ifeanyi Nwakanma, Jae-Min Lee, and Dong-Seong Kim. "Investigating network intrusion detection datasets using machine learning." In 2020 International Conference on Information and Communication Technology Convergence (ICTC), pp. 1325-1328. IEEE, 2020.

[21] Callens, Aurélien, Denis Morichon, Stéphane Abadie, Matthias Delpey, and Benoit Liquet. "Using Random forest and Gradient boosting trees to improve wave forecast at a specific location." Applied Ocean Research 104 (2020): 102339.

[22] Mohammed, Abdul Khaleeq, Siraj Farheen Ansari, Mohammed Imran Ahmed, and Zubair Ahmed Mohammed. "Boosting Decision-Making with LLM-Powered Prompts in PowerBI."

[23] Fonkem, Beryl Ngum. "AI-Powered Risk Scoring Models for Real-Time Fraud Detection in Digital Banking Ecosystems." Journal of Computational Analysis and Applications 34, no. 11 (2025): 349-371.

[24] RAHEEM, MOHD ABDUL, and MOHAMMED AZMATH ANSARI. "INTELLIGENT AND TRUSTWORTHY 6G: AI-DRIVEN ARCHITECTURES, APPLICATIONS, AND SECURITY FRAMEWORKS.

[25] Chittoju, Siva Sai Ram, Sireesha Kolla, Mubashir Ali Ahmed, and Abdul Raheman Mohammed. "Synergistic Integration of Blockchain and Artificial Intelligence for Robust IoT and Critical Infrastructure Security."

[26] Kashif, Mohammed, Mohammed Aasimuddin, Mubashir Ali Ahmed, Laxmi Bhavani Cheekatimalla, Eraj Farheen Ansari, and Ahwan Mishra. "AI-DRIVEN CTI FOR BUSINESS: EMERGING THREATS, ATTACK STRATEGIES, AND DEFENSIVE MEASURES."

[27] Khader, Shuaib Abdul, Amir Ahmed Ansari, and Syed Sharik Ali. "Zero-Day Exploit Prediction Using Graph-Based Deep Learning on Vulnerability and Threat Intelligence Data."Nour, Boubakr, Makan Pourzandi, and Mourad Debbabi. "A survey on threat hunting in enterprise networks." IEEE communications surveys & tutorials 25, no. 4 (2023): 2299-2324.

DOI: 10.17148/IJARCCE.2026.15602

[28] Chittoju, S. R., and Siraj Farheen Ansari. "Blockchain's Evolution in Financial Services: Enhancing Security, Transparency, and Operational Efficiency." International Journal of Advanced Research in Computer and Communication Engineering 13, no. 12 (2024): 1-5.

[29] Braun, Tobias, Irdin Pekaric, and Giovanni Apruzzese. "Understanding the process of data labeling in cybersecurity." In Proceedings of the 39th ACM/SIGAPP Symposium on Applied Computing, pp. 1596-1605. 2024.

[30] Paschalides, Demetris, George Pallis, and Marios D. Dikaiakos. "FIMI Tactics, Techniques and Procedures." In Foreign Information Manipulation and Interference: Case Studies From the ATHENA Project, pp. 377-453. Cham: Springer Nature Switzerland, 2025.

[31] Khadri, Waheeduddin, Janamolla Kavitha Reddy, Abubakar Mohammed, and T. Kiruthiga. "The Smart Banking Automation for High Rated Financial Transactions using Deep Learning." In 2024 IEEE 3rd World Conference on Applied Intelligence and Computing (AIC), pp. 686-692. IEEE, 2024.

[32] Reddy, Balavardhan, and Amir Ahmed Ansari. "AI-ENHANCED NETWORK TRAFFIC ANALYSIS FOR PREVENTING FRAUD PAYMENT IN BANKS."KASHIF, MOHAMMED, ABDUL RAHMAN JIBRAN SYED, and MUBASHIR ALI AHMED. "ADVANCING ANOMALY AND FRAUD DETECTION IN BIG DATA WITH ARTIFICIAL INTELLIGENCE."

[33] Ahmed, Mohammed Imran, Abdul Raheman Mohammed, Srujan Kumar Ganta, Sireesha Kolla Kolla, and Mohammed Kashif . "AI-Driven Green Construction: Optimizing Energy Efficiency, Waste Management and Security for Sustainable Buildings." Journal of Cognitive Computing and Cybernetic Innovations 1, no. 1 (2025): 37-41.

[34] Al Siam, Abdullah, Md Maruf Hassan, Abdul Kadar Muhammad Masum, and Touhid Bhuiyan. "Automating Malware Detection and Response via Real-Time Threat Feed Integration with Wazuh SIEM." In 2025 IEEE 2nd International Conference on Computing, Applications and Systems (COMPAS), pp. 1-6. IEEE, 2025.

[35] Khader, Shuaib Abdul Khader, and Praveen Kumar Reddy Gouni Gouni. "Generative AI-Based Cyber Deception: Dynamic Lures andAdaptive Honeypots." Journal of Cognitive Computing and Cybernetic Innovations 1, no. 3 (2025): 44-52..

