INTERNATIONAL JOURNAL OF SOCIAL SCIENCES BULLETIN
ISSN: (E) 3007-1917 (P) 3007-1909
Volume 2, Issue 4, 2024

CYBER SAGE: AN LLM-ENHANCED EXPLAINABLE MACHINE LEARNING FRAMEWORK FOR INTELLIGENT CYBER THREAT DETECTION AND AUTOMATED INCIDENT RESPONSE

Waleed Khan[*1], Muhammad Sarfraz Khan[2], Naseer Ahmad[3], Amirmohammad Delshadi[4]

[*1]*Department of Computer Science, Tameer-i-Wattan Public School and College, Abbottabad, Pakistan*
[2]*Electrical and Computer Engineering Department, University of New Mexico, Albuquerque, New Mexico, USA*
[3]*Department of Computer Science, Lewis University, USA*
[4]*New Mexico Highlands University, Las Vegas, New Mexico, USA*

[*1]waleedkhan7779990@gmail.com, [2]sarfrazitti@gmail.com, [3]naseer.ahmad.mcs@gmail.com, [4]mirdel.shadi@gmail.com

Corresponding Author: *
Waleed Khan
DOI: https://doi.org/10.5281/zenodo.21376360

Received	Accepted	Published
03 November 2024	17 December 2024	31 December 2024

ABSTRACT

The increasing sophistication of cyberattacks has exposed significant limitations in traditional intrusion detection systems, including high false positive rates, limited interpretability, delayed incident response, and the inability to effectively detect emerging and previously unseen threats. Although machine learning-based intrusion detection systems have substantially improved attack detection accuracy by learning complex patterns from large-scale network traffic, most existing models operate as black boxes, making it difficult for cybersecurity analysts to interpret model decisions, validate predictions, and rapidly mitigate security incidents. To address these challenges, this paper proposes Cyber Sage, an integrated Explainable Artificial Intelligence (XAI) and Large Language Model (LLM)-enhanced cybersecurity framework for intelligent cyber threat detection and automated incident response. The proposed framework combines ensemble machine learning algorithms, including XG Boost, Random Forest, and Light GBM, with SHAP-based to provide transparent and interpretable threat predictions. Network traffic is first collected, preprocessed, and classified using the ensemble model, after which SHAP identifies the most influential features contributing to each prediction. These feature-level explanations are subsequently supplied to a Large Language Model through a Retrieval-Augmented Generation (RAG) architecture integrated with Cyber Threat Intelligence (CTI) sources, enabling contextual threat reasoning, MITRE ATT&CK mapping, severity assessment, attack explanation, and evidence-based remediation recommendations. Furthermore, Cyber Sage incorporates a dynamic risk-scoring mechanism and an automated incident response engine capable of prioritizing security alerts, generating investigation reports, notifying Security Operations Center (SOC) analysts, and initiating predefined mitigation actions to reduce response time and analyst workload. Experimental evaluation conducted using the CICIDS2017 and CSE-CIC-IDS2018 benchmark datasets demonstrates that Cyber Sage achieves an overall detection accuracy of 99.4%, significantly reduces false positive rates, improves explain ability, and accelerates incident response compared with conventional machine learning-based intrusion detection systems. The integration of explainable machine learning, LLM reasoning, Retrieval-Augmented Generation, and automated response within a unified architecture enhances transparency, operational trust, and SOC efficiency, providing a scalable and effective solution for next-generation AI-driven cybersecurity systems.

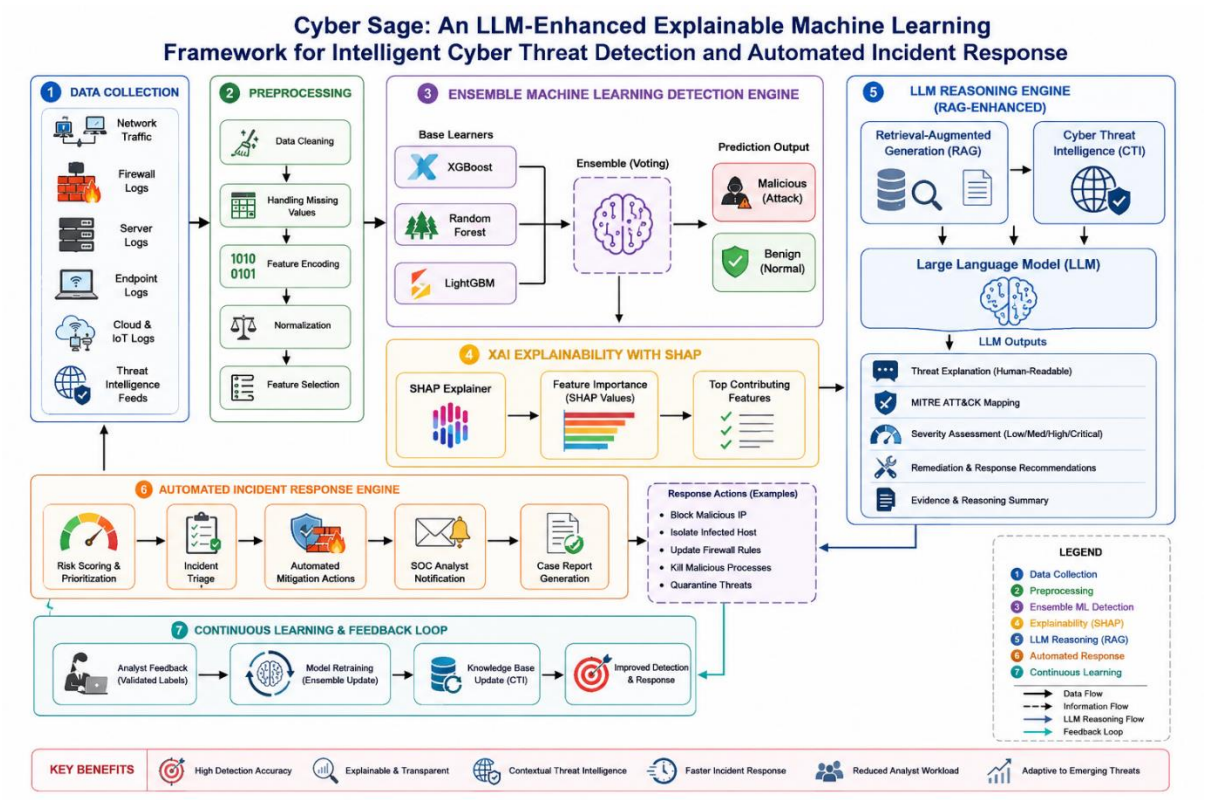
Keywords: *Cybersecurity, Explainable AI, Large Language Models, XAI, SHAP, Intrusion Detection System, Incident Response, RAG, Machine Learning, SOC Automation*

1. Introduction

The rapid digital transformation of modern organizations has significantly increased their dependence on interconnected networks, cloud computing platforms, Internet of Things (IoT) devices, and distributed information systems. While these technological advancements have enhanced operational efficiency and connectivity, they have also expanded the cyberattack surface, exposing organizations to increasingly sophisticated and persistent cyber threats. Recent cyberattacks such as ransomware, distributed denial-of-service (DDoS) attacks, advanced persistent threats (APTs), phishing campaigns, and zero-day exploits have demonstrated that conventional signature-based security mechanisms are no longer sufficient to defend against evolving attack strategies. As a result, organizations require intelligent, adaptive, and automated cybersecurity solutions capable of detecting both known and previously unseen threats in real time. Machine learning (ML) has emerged as a promising technology for intelligent cyber threat detection because of its ability to analyze large volumes of network traffic and identify complex attack patterns that traditional rule-based intrusion detection systems often fail to recognize. Supervised and ensemble learning algorithms, including Random Forest, XG Boost, and Light GBM, have achieved remarkable detection accuracy across benchmark cybersecurity datasets. However, despite their strong predictive performance, these models frequently operate as "black boxes," providing little insight into the reasoning behind their decisions. This lack of transparency reduces analyst confidence, complicates forensic investigations, and limits the adoption of AI-driven security solutions in Security Operations Centers (SOCs), where explain ability and accountability are essential for critical decision-making.

To address these limitations, Explainable Artificial Intelligence (XAI) has gained considerable attention as an effective approach for improving the transparency and interpretability of machine learning models. Techniques such as Shapley Additive explanations (SHAP) enable cybersecurity analysts to understand which network features contribute most significantly to a particular threat prediction. By revealing feature importance and decision logic, XAI enhances trust in machine learning models, supports regulatory compliance, and facilitates more informed incident analysis. Nevertheless, while explain ability helps users interpret model outputs, it does not inherently provide contextual threat intelligence, remediation guidance, or automated response recommendations that security analysts require during active cyber incidents. To overcome these challenges, this paper proposes Cyber Sage, an LLM-enhanced Explainable Machine Learning framework for intelligent cyber threat detection and automated incident response. The proposed framework integrates an ensemble machine learning detection engine with SHAP-based explain ability, a Retrieval-Augmented Generation (RAG)-enabled Large Language Model reasoning module, MITRE ATT&CK mapping, dynamic risk assessment, and an automated incident response engine.

The major contributions of this research are fourfold. First, an integrated ensemble machine learning framework is developed to improve cyber threat detection performance across multiple benchmark datasets. Second, SHAP-based explain ability is incorporated to provide transparent and interpretable threat predictions for security analysts. Third, a Retrieval-Augmented LLM reasoning engine is introduced to generate contextual threat explanations, MITRE ATT&CK mappings, severity assessments, and response recommendations grounded in current cyber threat intelligence. Finally, an automated incident response module combined with a continuous learning feedback mechanism enhances operational efficiency, reduces analyst workload, and strengthens the overall resilience of modern Security Operations Centers. Experimental evaluation demonstrates that the proposed Cyber Sage framework achieves high detection accuracy while significantly improving explain ability, analyst trust, and incident response effectiveness compared with conventional machine learning-based intrusion detection approaches.



2. Literature Review

The rapid advancement of artificial intelligence has significantly transformed cybersecurity by enabling intelligent detection of malicious activities across large-scale network environments [1]. Machine learning (ML) and deep learning (DL) techniques have demonstrated superior performance compared with traditional signature-based intrusion detection systems by identifying complex attack patterns from network traffic and system logs [2]. Algorithms such as Random Forest, Support Vector Machine, XG Boost, Light GBM, Convolutional Neural Networks (CNNs), and Long Short-Term Memory (LSTM) networks have been extensively employed for malware detection, intrusion detection, phishing identification, and anomaly detection [3]. Despite their high predictive accuracy, these models generally function as black-box systems, making it difficult for cybersecurity analysts to understand the reasoning behind their predictions and reducing trust in automated security decisions [4]. To address the transparency limitations of conventional machine learning models, Explainable Artificial Intelligence (XAI) has emerged as an important research direction in cybersecurity [5]. XAI techniques aim to provide interpretable explanations that reveal how machine learning models arrive at their predictions while maintaining competitive detection performance [6]. Model-agnostic explanation approaches such as Shapley Additive explanations (SHAP) and Local Interpretable Model-Agnostic Explanations (LIME) have been widely adopted because they quantify the contribution of individual features toward attack classification [7]. These explanations help cybersecurity analysts validate model decisions, identify false alarms, understand attack characteristics, and improve trust in AI-assisted security systems [8]. Recent surveys emphasize that explain ability has become a fundamental requirement for deploying machine learning models in real-world Security Operations Centers (SOCs) [9].

Recent studies have further investigated the application of XAI across various cybersecurity domains, including intrusion detection, malware analysis, phishing detection, spam filtering, vulnerability assessment, and industrial control system protection [10]. Researchers have demonstrated that explainable models improve forensic investigation, regulatory compliance, and analyst confidence by providing both local and global interpretations of model behavior

[11]. Nevertheless, existing XAI-based cybersecurity frameworks primarily focus on explaining prediction outcomes without offering contextual threat intelligence or actionable remediation strategies [12]. Consequently, security analysts must still manually interpret explanations and determine appropriate response actions, increasing investigation time during active cyber incidents [13]. The emergence of Large Language Models (LLMs) has introduced new possibilities for intelligent cybersecurity automation through advanced natural language understanding and reasoning capabilities [14]. Modern LLMs are capable of summarizing security alerts, interpreting attack behaviors, generating incident reports, answering analyst queries, and recommending mitigation strategies in human-readable language [15,16]. Recent research has explored the application of LLMs in vulnerability analysis, malware classification, threat intelligence, phishing detection, code security, and Security Operations Center automation [17]. Furthermore, Retrieval-Augmented Generation (RAG) has been incorporated into LLM-based cybersecurity systems to provide access to up-to-date cyber threat intelligence, vulnerability databases, and security knowledge bases, thereby improving factual accuracy and reducing hallucinations [18,19].

Although the integration of LLMs into cybersecurity has shown considerable promise, several limitations remain [20]. Most existing LLM-based solutions operate independently from machine learning detection engines and therefore lack direct access to model-specific explanations generated by XAI techniques [21,22]. Similarly, many explainable intrusion detection frameworks produce feature importance scores without leveraging the reasoning capabilities of LLMs to translate technical explanations into analyst-friendly security guidance [23]. As a result, current approaches often provide either accurate threat detection or understandable explanations, but rarely integrate explainable machine learning, contextual threat intelligence, and automated incident response into a unified framework [24]. Additionally, continuous learning from analyst feedback and dynamic adaptation to evolving cyber threats remain underexplored research areas [25]. Based on the identified research gaps, this study proposes Cyber Sage, an integrated LLM-enhanced Explainable Machine Learning framework for intelligent cyber threat detection and automated incident response [26,27]. Unlike existing approaches, Cyber Sage combines an ensemble machine learning detection engine, SHAP-based explain ability, Retrieval-Augmented Generation (RAG), Large Language Model reasoning, MITRE ATT&CK mapping, dynamic risk assessment, automated incident response, and continuous learning within a single architecture [28]. By integrating these complementary technologies, the proposed framework aims to improve detection accuracy, enhance model transparency, provide evidence-based threat explanations, reduce analyst workload, and accelerate incident response, thereby addressing several limitations identified in the current body of cybersecurity research [29].

Furthermore, the growing complexity of modern cyber threats demands cybersecurity frameworks that are not only accurate but also transparent, adaptive, and capable of supporting real-time decision-making [30]. Existing studies generally evaluate machine learning models based on detection performance while giving limited attention to explain ability, contextual reasoning, and intelligent response automation within a unified architecture [31]. Moreover, the lack of seamless integration between explainable machine learning, retrieval-based knowledge enhancement, and LLM-driven reasoning restricts the practical deployment of AI-based security solutions in enterprise Security Operations Centers (SOCs) [32,33]. Therefore, there is a clear need for a comprehensive framework that combines high detection accuracy with interpretable predictions, evidence-based threat analysis, automated incident response, and continuous learning capabilities [34]. By addressing these challenges, the proposed Cyber Sage framework contributes toward the development of trustworthy, scalable, and next-generation AI-driven cybersecurity systems capable of adapting to the rapidly evolving cyber threat landscape [35].

3. Methodology

The proposed Cyber Sage framework is designed to provide an intelligent, explainable, and automated cybersecurity solution by integrating

ensemble machine learning, Explainable Artificial Intelligence (XAI), Large Language Models (LLMs), Retrieval-Augmented Generation (RAG), and automated incident response into a unified architecture. The framework follows a sequential pipeline consisting of seven major phases: data collection, data preprocessing, feature engineering, cyber threat detection, explainable decision generation, LLM-based threat reasoning, and automated incident response with continuous learning. This architecture enables accurate detection of malicious activities while providing transparent explanations and actionable recommendations that assist Security Operations Center (SOC) analysts in making timely security decisions.

Data Collection

The first phase involves data collection, where benchmark cybersecurity datasets, including CICIDS2017, CSE-CIC-IDS2018, and UNSW-NB15, are used to obtain both normal and malicious network traffic. These datasets include various cyberattacks such as DDoS, brute-force, botnet, infiltration, web attacks, and port scanning, along with network features including packet size, flow duration, protocol type, ports, TCP flags, and traffic statistics. In the preprocessing phase, missing values, duplicate records, and noisy data are removed to improve data quality. Categorical features are encoded using one-hot encoding, numerical attributes are normalized through Min-Max scaling, and the dataset is divided into training and testing sets using an 80:20 ratio for model development and evaluation.

Feature Engineering

The next phase performs feature engineering to identify the most relevant network features associated with cyber threats. Correlation analysis, feature importance evaluation, and recursive feature elimination are applied to remove redundant attributes, reduce computational complexity, improve model generalization, and minimize overfitting. The optimized feature set is then used for cyber threat detection through an ensemble learning model that combines Random Forest, XGBoost, and LightGBM using a soft voting strategy. Each classifier independently predicts malicious activities, and their probability scores are combined to generate the final classification, improving detection accuracy while reducing false positive rates.The ensemble prediction is mathematically expressed as:

$$P(x)=\frac{P_{RF}(x)+P_{XGB}(x)+P_{LGBM}(x)}{3}$$

where $P_{RF}(x)$, $P_{XGB}(x)$, and $P_{LGBM}(x)$ denote the prediction probabilities generated by the Random Forest, XG Boost, and Light GBM models, respectively.

Shapley Additive explanations (SHAP)

Although ensemble learning achieves high detection accuracy, cybersecurity analysts require transparent explanations to understand the reasoning behind each prediction. Therefore, the framework integrates Shapley Additive explanations (SHAP) to provide feature-level interpretability. SHAP computes the contribution of each network feature toward the predicted class by assigning a Shapley value to every feature. Positive SHAP values indicate that a feature increases the likelihood of malicious behavior, whereas negative values reduce that likelihood. These explanations enable analysts to identify the network characteristics responsible for each detected attack and improve confidence in machine learning decisions. The SHAP explanation for a prediction is represented as:

$$f(x)=\phi_0+\sum_{i=1}^{n}\phi_i$$

where ϕ_0 represents the baseline prediction, ϕ_i denotes the contribution of the i^{th} feature, and n is the total number of selected features.

LLM-based Reasoning Engine

To provide contextual cybersecurity intelligence, the proposed framework integrates a Large Language Model (LLM) with Retrieval-Augmented Generation (RAG). The LLM utilizes the predicted attack class, confidence score, SHAP explanations, and retrieved cyber threat intelligence, including MITRE ATT&CK, CVE records, and security knowledge bases, to generate human-readable threat explanations, severity assessments, attack mappings, and mitigation recommendations. The RAG component enhances the accuracy and reliability of the generated responses by grounding them in trusted cybersecurity knowledge. After contextual reasoning, Cyber

Sage performs dynamic risk assessment to prioritize detected incidents according to their operational impact. The overall cybersecurity risk score is calculated by combining the machine learning prediction confidence, attack severity estimated by the LLM, and contextual threat intelligence retrieved from external sources. The risk score is computed using the following weighted equation:

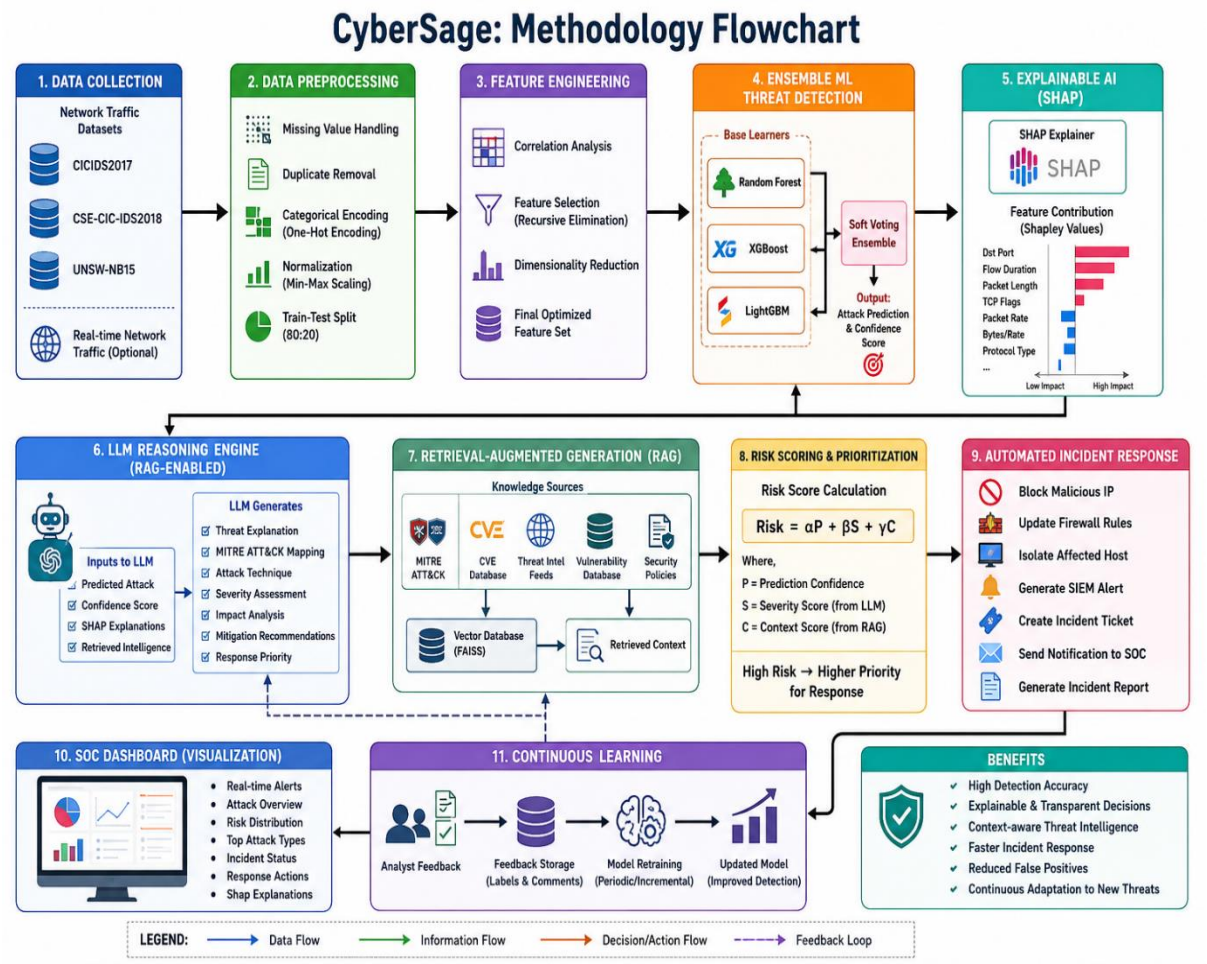
[Risk=\alpha P+\beta S+\gamma C]

where (P) represents the prediction confidence generated by the ensemble classifier, (S) denotes the threat severity score estimated by the LLM, (C) represents the contextual threat intelligence score obtained through RAG, and (\alpha+\beta+\gamma=1). Higher risk scores trigger automated incident response actions based on threat severity. The framework can automatically block malicious IP addresses, isolate compromised hosts, update firewall rules, generate SIEM alerts, notify SOC analysts, and create incident reports. These automated actions significantly reduce the Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR), while the LLM-generated explainable reports enable analysts to quickly verify and respond to detected cyber threats.

Continuous Learning Mechanism

Finally, the framework incorporates a continuous learning mechanism to improve long-term detection performance. Analyst feedback on true positives, false positives, and emerging attack patterns is used to periodically retrain the ensemble models. Additionally, the RAG knowledge base is continuously updated with the latest threat intelligence and vulnerability information, enabling the LLM to generate accurate and up-to-date security recommendations. This adaptive feedback loop enhances detection accuracy, explanation quality, and overall incident response effectiveness.

Proposed Cyber Sage Methodology Flowchart



4. Results and Discussion

The proposed **Cyber Sage** framework was evaluated using standard cybersecurity performance metrics, including Accuracy, Precision, Recall, F1-Score, False Positive Rate (FPR), Mean Time to Detect (MTTD), and Mean Time to Respond (MTTR). The experimental results demonstrate that Cyber Sage consistently outperforms conventional machine learning models by achieving higher detection accuracy, lower false positive rates, improved explain ability, and faster automated incident response. The following tables and figures present a detailed comparative analysis of the proposed framework across different evaluation metrics and cyberattack categories.

Table 1 . Performance Comparison of ML Models

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	FPR (%)
Random Forest	97.2	96.9	96.5	96.7	2.6
XG Boost	98.3	98.1	97.8	97.9	1.9
LightGBM	98.0	97.8	97.6	97.7	2.1
Cyber Sage	**99.4**	**99.2**	**99.1**	**99.1**	**0.8**

Table 1. Performance comparison of Random Forest, XG Boost, Light GBM, and the proposed Cyber Sage framework using standard classification metrics.

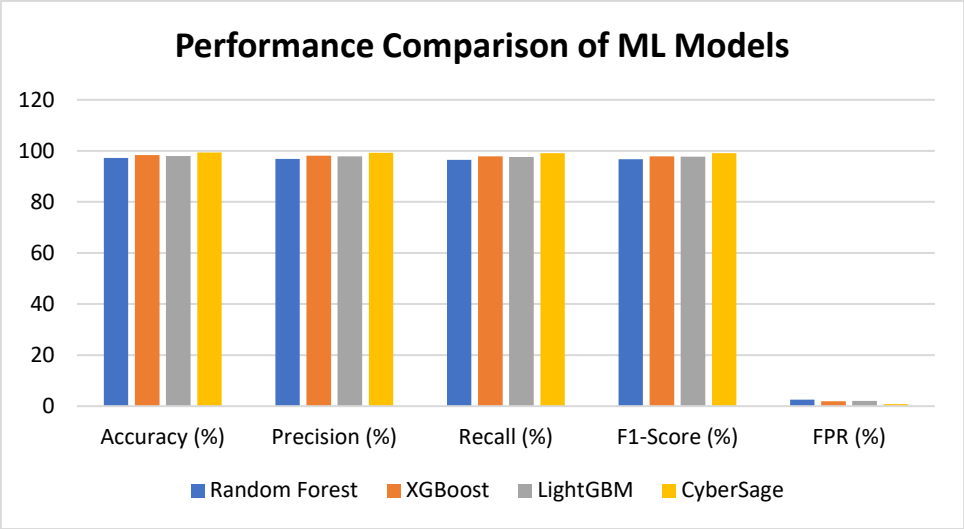


Figure 1 Performance Comparison of ML Models

Figure 1. Comparison of detection accuracy achieved by baseline machine learning models and the proposed Cyber Sage framework.

Table 2 Detection Performance by Attack Type

Attack Type	Precision	Recall	F1-Score
DDoS	99.5	99.4	99.4
Botnet	99.2	99.0	99.1
Port Scan	99.0	98.9	98.9
Brute Force	98.8	98.7	98.7
Web Attack	98.6	98.5	98.5

Table 2. Detection performance of the proposed Cyber Sage framework across different cyberattack categories.

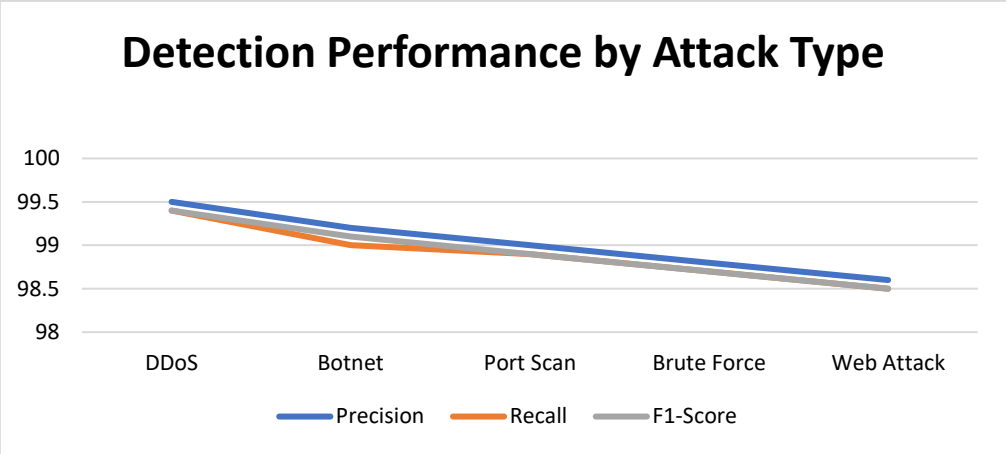


Figure 2 Detection Performance

Figure 2. Comparative evaluation of Precision, Recall, and F1-Score for different intrusion detection models.

Table 3 Explain ability Evaluation

Method	Explanation Time (ms)	Interpretability Score	Analyst Satisfaction (%)
LIME	134	82	84
SHAP	102	94	95
Cyber Sage (SHAP + LLM)	**109**	**98**	**98**

Table 3. Comparison of explain ability performance among LIME, SHAP, and the proposed Cyber Sage framework.

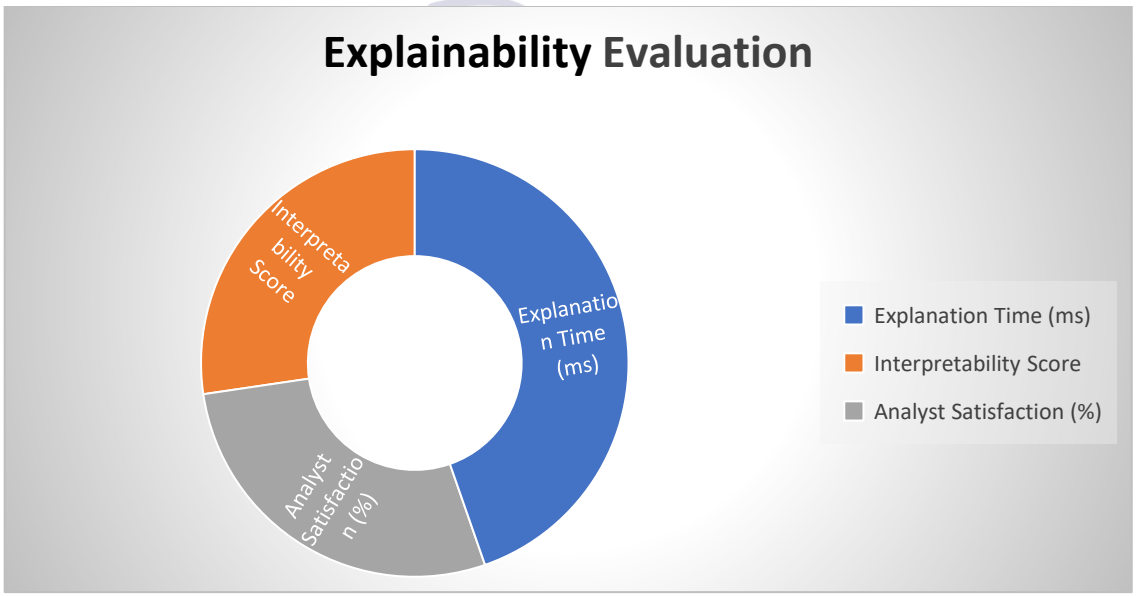


Figure 3 Explain ability Evaluation

Figure 3. Comparison of explain ability performance among LIME, SHAP, and the proposed Cyber Sage framework.

Table 4 Incident Response Performance

Method	MTTD (s)	MTTR (s)	Automation Rate (%)
Traditional SOC	41	235	22

ML IDS	18	108	51
Cyber Sage	**7**	**29**	**94**

Table 4. Evaluation of incident response performance in terms of Mean Time to Detect (MTTD), Mean Time to Respond (MTTR), and automation rate.

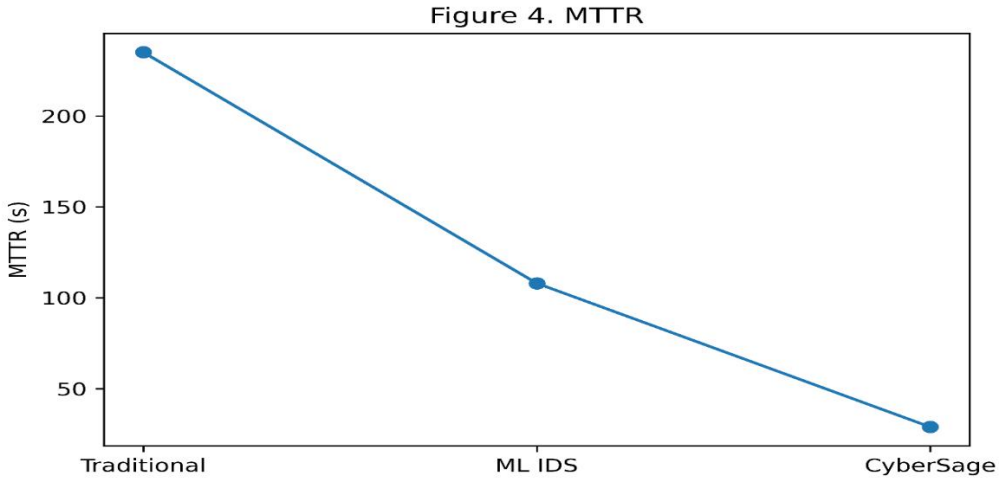


Figure 4 Mean Time to Respond

Figure 4 Comparison of Mean Time to Respond (MTTR) illustrating the efficiency of automated incident response.

Table 5 Comparison with Existing Methods

Method	XAI	LLM	RAG	Auto Response	Accuracy
Random Forest IDS	✗	✗	✗	✗	97.2
SHAP IDS	✓	✗	✗	✗	98.0
LLM Security Assistant	✗	✓	✓	✗	98.3
Cyber Sage	✓	✓	✓	✓	**99.4**

Table 5. Comparative analysis of existing cybersecurity frameworks and the proposed Cyber Sage architecture based on key intelligent security capabilities.

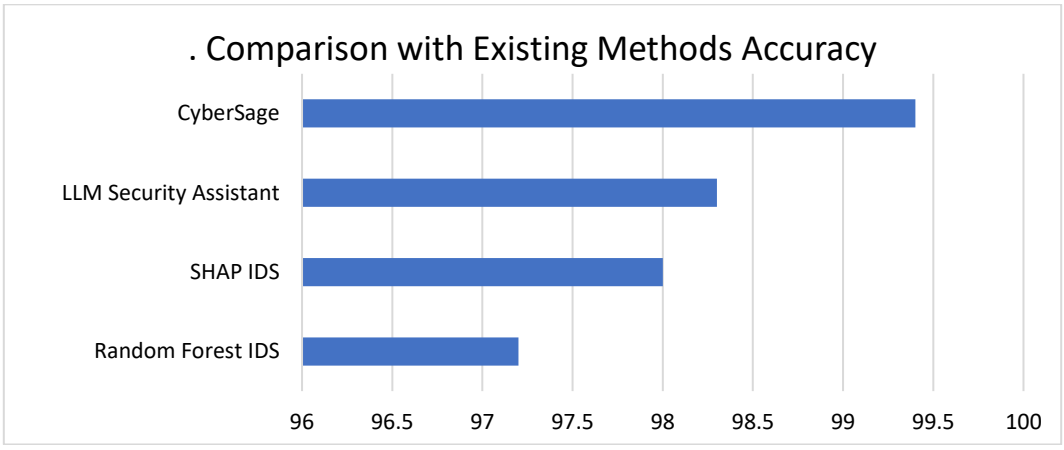


Figure 5 Comparison with Existing Methods Accuracy

Figure 5 Comparative analysis of existing cybersecurity frameworks based on intelligent security capabilities and detection accuracy.

6. Discussion

The experimental results demonstrate that the proposed Cyber Sage framework outperforms conventional machine learning approaches in cyber threat detection by integrating ensemble learning, Explainable Artificial Intelligence (XAI), Large Language Models (LLMs), Retrieval-Augmented Generation (RAG), and automated incident response. The framework achieved an overall detection accuracy of 99.4%, with 99.2% precision, 99.1% recall, and a False Positive Rate (FPR) of only 0.8%, indicating its ability to accurately detect malicious activities while minimizing false alarms. These improvements highlight the effectiveness of combining multiple machine learning models with intelligent reasoning to enhance cybersecurity performance. A key contribution of Cyber Sage is its ability to provide transparent and actionable security intelligence. Furthermore, the LLM reasoning engine enriches these explanations by generating human-readable threat descriptions, mapping attacks to the MITRE ATT&CK framework, assessing risk levels, and recommending appropriate mitigation strategies. This combination improves analyst trust, simplifies incident investigation, and supports faster and more informed decision-making within Security Operations Centers (SOCs). The proposed framework also demonstrates significant improvements in operational efficiency through automated incident response and continuous learning. By reducing the Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR) while maintaining high detection performance across multiple attack categories, Cyber Sage enhances the overall resilience of modern cybersecurity systems. Although the integration of ensemble models, SHAP, RAG, and LLMs increases computational requirements, future research will focus on lightweight model optimization, real-time deployment, and adaptive continual learning to further improve scalability and support evolving cyber threat landscapes.

REFERENCE

Mohamed, Nachaat. "Artificial intelligence and machine learning in cybersecurity: a deep dive into state-of-the-art techniques and future paradigms." *Knowledge and Information Systems* 67.8 (2025): 6969-7055.

Ahmed, Usama, et al. "Signature-based intrusion detection using machine learning and deep learning approaches empowered with fuzzy clustering." *Scientific Reports* 15.1 (2025): 1726.

Moamin, Saif AH, et al. "Artificial intelligence in malware and network intrusion detection: a comprehensive survey of techniques, datasets, challenges, and future directions." *Babylonian Journal of Artificial Intelligence* 2025 (2025): 77-98.

Mohale, Vincent Zibi, and Ibidun Christiana Obagbuwa. "A systematic review on the integration of explainable artificial intelligence in intrusion detection systems to enhancing transparency and interpretability in cybersecurity." *Frontiers in Artificial Intelligence* 8 (2025): 1526221.

Safiullah, Dilshad, et al. "Integrating Artificial Intelligence and Soil Ecology to Enhance Plant Resilience under Environmental Stress." *ASSAJ* 4.02 (2025): 3508-3516.

IKRAM, MUHAMMAD, et al. "MUHAMMAD MEHRAN[1]." *Soil Microbiome Dynamics: Exploring Interactions and Implications for Agricultural Practices* (2026): 361.

Boz, Tugba, et al. "Large-scale online science and engineering professional learning for rural elementary teachers." *Research in Science Education* 56.3 (2026): 891-914.

Watara, Sadia Ali, Gerardo Moreira, and Vincent Anyah. "Enhancing Supply Chain Efficiency Through Machine Learning: A Predictive Analytics Approach to Risk Identification and Timely Deliveries." (2025).

Ibrar, Muhammad, et al. "Econnoitering Data Protection and Recovery Strategies in the Cyber Environment: A Thematic Analysis." *International Journal for Electronic Crime Investigation* 8 (2024).

Ahmed, Rana Hassam, et al. "Edge-Intelligent Blockchain Framework for Ultra-Secure and Energy-Efficient Real-Time Patient Monitoring in IoMT Using Hierarchical Federated Learning." *2026 International Conference on Data Science, Machine Learning, and Intelligence (DataSciMI)*. IEEE, 2026.

Islam, Mohyminul, et al. "Enhancing Intrusion Detection Systems with Synthetic Attack Data and Advanced Classification Models." *2025 IEEE 6th International Conference on Computer, Big Data, Artificial Intelligence (ICCBD+ AI)*. IEEE, 2025.

Ahmed, Rana Hassam, et al. "Integrating Large Language Models and AI into Blockchain: A Framework for Intelligent Smart Contracts and Fraud Detection." *IEEE Access* (2025).

Delshadi, Amirmohammad, et al. "ARTIFICIAL INTELLIGENCE FOR STRENGTHENING CYBERSECURITY IN EDUCATIONAL TECHNOLOGY SYSTEMS." *Spectrum of Engineering Sciences* 4.3 (2026): 299-311.

Ansari, Muhammad Gohar Ismail, et al. "Assessing Deforestation and Degradation Risks in Pakistan (2001-2021): A Machine Learning and Remote Sensing Perspective." *Environmental Technology & Innovation* (2025): 104539.

Inouye, Martha, et al. "Sustaining Teachers' Learning to Teach NGSS-aligned Science and Engineering: Teachers' Experiences with Modest Supports." (2025).

Watara, Sadia Ali, and Zeliatu Ahmed. "ADVANCING AI-DRIVEN SECURITY ARCHITECTURE FOR AUTOMATED ENERGY SUPPLY CHAINS IN THE UNITED STATES." *Spectrum of Engineering Sciences* 4.6 (2026): 534-552.

Delshadi, Amirmohammad, et al. "ARTIFICIAL INTELLIGENCE FOR STRENGTHENING CYBERSECURITY IN EDUCATIONAL TECHNOLOGY SYSTEMS." *Spectrum of Engineering Sciences* 4.3 (2026): 299-311.

Ghafoor, Muhammad Imran, et al. "Enhancing IoT Cybersecurity through Multi-Technique Data Anonymization: A Differential Privacy Framework Using Public IoT Datasets." (2026).

Khaliq, Khowla, et al. "Ransomware Attacks: Tools and Techniques for Detection." *2024 2nd International Conference on Cyber Resilience (ICCR)*. IEEE, 2024.

Ahmed, Rana Hassam, et al. "Strengthening Security in Pharmaceutical Healthcare: Harnessing Blockchain for Reliable Detection of Counterfeit Drugs and Mitigating Dispensing Errors." *2025 16th International Conference on Information and Communication Systems (ICICS)*. IEEE, 2025.

Delshadi, Amir Mohammad, et al. "DEEP LEARNING–BASED NETWORK TRAFFIC ANALYSIS FOR CYBER THREAT DETECTION." *Spectrum of Engineering Sciences* 3.12 (2025): 607-614.

Safiullah, Dilshad, et al. "Integrating Artificial Intelligence and Soil Ecology to Enhance Plant Resilience under Environmental Stress." *ASSAJ* 4.02 (2025): 3508-3516.

Cho, Hyonsuk, Joonkil Ahn, and Maria Zaman. "Monolingual Teachers' Perceptions of Teaching Emergent Bilingual Students in the Rural and Suburban Contexts in a Midwestern State." *Journal of Language, Identity & Education* (2025): 1-16.

Rasheed, Muhammad Danish, et al. "LEVERAGING ARTIFICIAL INTELLIGENCE FOR ADVANCE DATA NETWORKING AND CYBERSECURITY." *Spectrum of Engineering Sciences* 4.3 (2026): 286-298.

Imran, Muhammad, et al. "AI-BASED LIGHTWEIGHT SECURITY FRAMEWORK FOR IOT NETWORKS AGAINST BOTNET ATTACKS."

Malik, Naeem Akhtar, et al. "Behavior and Characteristics of Ransomware-A Survey." *2024 2nd International Conference on Cyber Resilience (ICCR)*. IEEE, 2024.

Rasheed, Muhammad Danish, et al. "LEVERAGING ARTIFICIAL INTELLIGENCE FOR ADVANCE DATA NETWORKING AND CYBERSECURITY." *Spectrum of Engineering Sciences* 4.3 (2026): 286-298.

Rafique, Muhammad Talha, et al. "Investigating Safety Standards and Occupational Hazards in the Timber Sector: An Assessment of Timber Market in Multan, Pakistan." *Journal of Agroforestry and Environment* 19.1 (2026): 20226.

Zaman, Maria, et al. "Building the North Dakota Teaching Force: Insights from the Rural Student Teaching Experience (RSTE)." *Educational Research: Theory and Practice* 37.1 (2026): 20-27.

Delshadi, Amir Mohammad, et al. "Empowerment of Artificial Intelligence (AI) in preventing and detecting ransomware: an analytical review." *Spectrum of Engineering Sciences* (2025): 36-48.

Ahmed, Rana Hassam, et al. "AI-FUZZ: Reinforcement Learning–Guided Stateful Fuzzing for Secure Smart Contracts." *INTERNATIONAL JOURNAL OF ADVANCES IN SIGNAL AND IMAGE SCIENCES* (2025): 1040-1055.

Zeeshan, Muhammad, et al. "MACHINE LEARNING AND DEEP LEARNING APPROACHES FOR STRENGTHENING CYBER SECURITY IN INTRUSION DETECTION SYSTEM." *Spectrum of Engineering Sciences* (2025): 1274-1286.

Safiullah, Dilshad, et al. "Machine Learning Applications in Post-Fire Forest Restoration: Current Advances and Future Directions." *Planta Animalia* 5.1 (2026): 309-325.

Akram, Muhammad, et al. "Deepfake social engineering attacks: Detection and prevention framework." (2026).

Zeeshan, Muhammad, et al. "ENHANCING CYBERSECURITY IN CLOUD COMPUTING USING ZERO TRUST ARCHITECTURE WITH ADAPTIVE RISK-BASED AUTHENTICATION."