iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** VI **Month of publication:** June 2026

DOI: https://doi.org/10.22214/ijraset.2026.84034

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 VI June 2026- Available at www.ijraset.com

Hybrid Explainable AI, Federated Learning, and Blockchain Framework for Trustworthy Cybersecurity

Dr. Ravi Chinkera[1], Dr. Syed Gilani Pasha[2]
[1]*Assistant Professor, Department of E&TC, School of Engineering & Technology, JSPM University, Pune, Maharashtra, India*
[2]*Professor, Department of E&TC, School of Engineering & Technology, Sapthagiri NPS University, Bengaluru, India*

Abstract: ***The increasing adoption of cloud computing, the Internet of Things (IoT), and distributed networks has intensified cybersecurity challenges, requiring intelligent, secure, and privacy-preserving threat detection mechanisms. This paper proposes a hybrid framework that integrates Explainable Artificial Intelligence (XAI), Federated Learning (FL), and Blockchain to develop a trustworthy cybersecurity system. Federated Learning enables collaborative model training without sharing sensitive data, blockchain ensures secure and tamper-resistant verification of model updates, and XAI techniques such as SHAP and LIME provide transparent explanations for cyber threat predictions. The proposed framework is evaluated using benchmark intrusion detection datasets based on metrics including accuracy, precision, recall, F1-score, blockchain latency, and communication overhead. The results demonstrate improved threat detection performance, enhanced privacy preservation, greater transparency, and stronger resilience against adversarial attacks. The proposed hybrid framework offers an effective solution for secure and trustworthy next-generation cybersecurity in IoT, cloud, and enterprise environments.***

Keywords: Explainable Artificial Intelligence (XAI), Federated Learning (FL), Blockchain, Cybersecurity, Intrusion Detection System (IDS), Privacy-Preserving Machine Learning, Trustworthy AI, Internet of Things (IoT), Deep Learning, Smart Contracts.

I. INTRODUCTION

The rapid expansion of cloud computing, the Internet of Things (IoT), edge computing, and smart digital infrastructures has transformed modern information systems while simultaneously increasing their exposure to sophisticated cyber threats. Cyberattacks such as malware, ransomware, distributed denial-of-service (DDoS), phishing, and advanced persistent threats (APTs) continue to evolve in complexity, making conventional signature-based and rule-based security mechanisms insufficient for protecting distributed environments [1].

Consequently, Artificial Intelligence (AI) and Machine Learning (ML) have become essential technologies for detecting anomalies, classifying attacks, and enabling automated cyber defense [2].

Despite their high detection performance, most AI-based cybersecurity systems rely on centralized learning, where data from multiple organizations are collected and processed at a central server [3-4]. This approach raises significant concerns regarding data privacy, confidentiality, regulatory compliance, and the risk of data breaches. Federated Learning (FL) has emerged as a promising distributed learning paradigm that enables multiple clients to collaboratively train a shared global model without exchanging raw data [5]. Although FL preserves data privacy, it remains susceptible to challenges such as malicious client participation, model poisoning attacks, insecure model aggregation, and limited trust among collaborating entities [6].

Blockchain technology provides a decentralized and tamper-resistant platform for securely validating and recording federated model updates[7]. By leveraging consensus mechanisms and smart contracts, blockchain enhances the integrity, traceability, and trustworthiness of distributed learning systems without relying on a central authority. However, while blockchain improves security and accountability, it does not address the lack of transparency in AI decision-making[8].

Explainable Artificial Intelligence (XAI) addresses this limitation by providing interpretable explanations for AI predictions, enabling cybersecurity analysts to understand why a particular event is classified as malicious or benign. Techniques such as SHAP and LIME identify the most influential features contributing to model decisions, thereby improving user trust, facilitating forensic investigations, reducing false positives, and supporting compliance with emerging AI governance regulations.

©IJRASET: All Rights are Reserved

This paper proposes a hybrid cybersecurity framework that integrates Explainable AI, Federated Learning, and Blockchain to develop a secure, privacy-preserving, and trustworthy cyber threat detection system.

The proposed framework combines federated deep learning for collaborative intrusion detection, blockchain-based secure aggregation and verification of model updates, and XAI techniques to provide transparent and interpretable threat predictions. The integration of these complementary technologies aims to improve detection performance, strengthen privacy protection, enhance resilience against adversarial attacks, and increase analyst confidence in AI-driven cybersecurity systems.

The major contributions of this work are as follows:

1) A novel hybrid architecture integrating Explainable AI, Federated Learning, and Blockchain for next-generation cybersecurity.
2) A privacy-preserving federated intrusion detection framework that enables collaborative model training without sharing sensitive data.
3) A blockchain-based secure aggregation mechanism that ensures the integrity and traceability of federated model updates.
4) An explainability module using SHAP and LIME to improve transparency and support informed cybersecurity decision-making.
5) A comprehensive performance evaluation based on detection accuracy, communication efficiency, blockchain overhead, explainability, and robustness against adversarial attacks.

A. Objectives of the Study

The primary objective of this study is to develop a hybrid cybersecurity framework by integrating Explainable Artificial Intelligence (XAI), Federated Learning (FL), and Blockchain for secure, privacy-preserving, and trustworthy cyber threat detection. The specific objectives are:

- To develop a hybrid XAI–Federated Learning–Blockchain framework for cybersecurity.
- To implement privacy-preserving federated learning for distributed intrusion detection.
- To integrate blockchain for secure verification of federated model updates.
- To apply XAI techniques to improve the transparency and interpretability of AI predictions.
- To evaluate the performance of the proposed framework using benchmark cybersecurity datasets and standard performance metrics.

B. Scope of the Study

This study focuses on the development of a hybrid cybersecurity framework that integrates Explainable Artificial Intelligence (XAI), Federated Learning (FL), and Blockchain to provide secure, privacy-preserving, and trustworthy cyber threat detection. The framework is designed for distributed environments, including cloud computing, Internet of Things (IoT), and enterprise networks. The proposed system employs federated learning for collaborative model training without sharing raw data, blockchain for secure verification of model updates, and XAI techniques such as SHAP and LIME to provide interpretable explanations for threat predictions.

The framework is evaluated using benchmark intrusion detection datasets, including CICIDS2017, UNSW-NB15, and BoT-IoT, based on performance metrics such as accuracy, precision, recall, F1-score, communication overhead, blockchain latency, and explainability.

The scope of this study is limited to software-based implementation and simulation, providing a foundation for future deployment in real-world distributed cybersecurity environments.

II. INTEGRATION OF EXPLAINABLE AI, FEDERATED LEARNING, AND BLOCKCHAIN

The proposed framework integrates Explainable Artificial Intelligence (XAI)**,** Federated Learning (FL)**,** and Blockchain to develop a secure, privacy-preserving, and trustworthy cybersecurity system. Each technology addresses a specific limitation of conventional AI-based cybersecurity solutions while complementing the others.

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

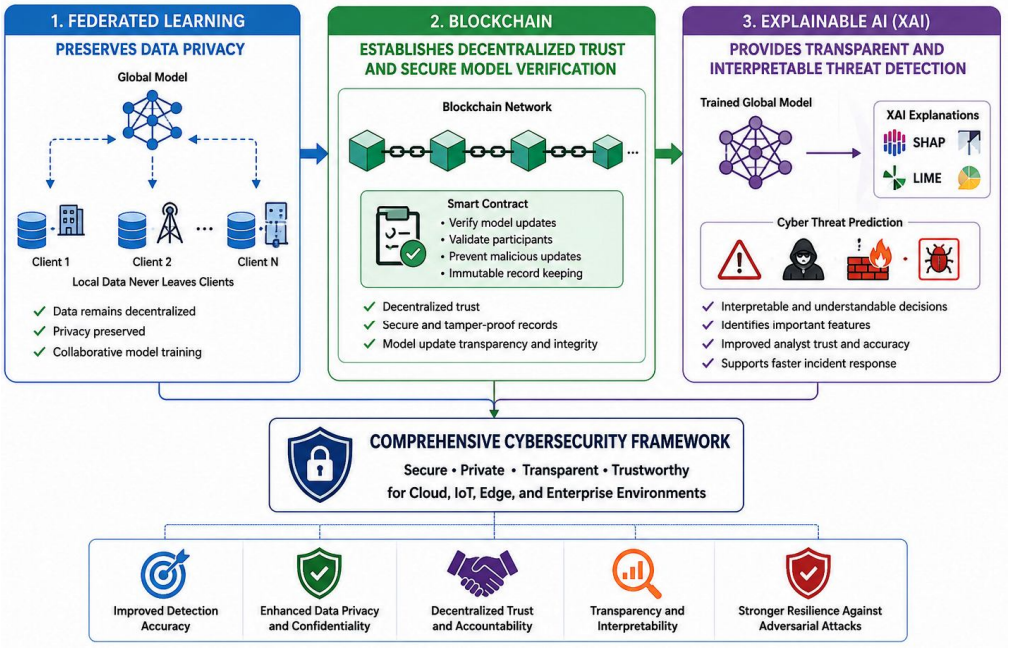


Figure 1: Comprehensive Cybersecurity Framework

Federated Learning enables multiple organizations or devices to collaboratively train an intrusion detection model without sharing their raw cybersecurity data. Instead, only local model parameters are exchanged, preserving data privacy and complying with security regulations. However, federated learning alone is vulnerable to malicious model updates, poisoning attacks, and trust management issues.

To overcome these limitations, Blockchain is integrated into the federated learning process. Blockchain validates local model updates through smart contracts before they are aggregated into the global model. Its decentralized and immutable ledger ensures the integrity, authenticity, and traceability of model updates while preventing unauthorized modifications and increasing trust among participating clients.

After the global model is generated, Explainable Artificial Intelligence is applied to interpret the model's predictions. XAI techniques such as SHAP **and** LIME identify the most influential features responsible for classifying cyber threats, enabling cybersecurity analysts to understand, verify, and trust the AI-generated decisions. This transparency improves incident response, reduces false positives, and supports regulatory compliance.

The integration of these three technologies creates a comprehensive cybersecurity framework in which Federated Learning preserves data privacy**,** Blockchain establishes decentralized trust and secure model verification**, and** Explainable AI provides transparent and interpretable threat detection. Together, they improve detection accuracy, enhance privacy, strengthen security against adversarial attacks, and increase confidence in AI-driven cybersecurity systems deployed in cloud, IoT, edge, and enterprise environments.

III. METHODOLOGY

The proposed methodology integrates Explainable Artificial Intelligence (XAI), Federated Learning (FL), and Blockchain to develop a secure, privacy-preserving, and trustworthy cybersecurity framework. Benchmark cybersecurity datasets such as CICIDS2017**,** UNSW-NB15, and BoT-IoT are used for training and evaluation. The collected data are preprocessed through data cleaning, normalization, feature selection, and train–test splitting. The preprocessed data are distributed among multiple federated clients, where local deep learning models (e.g., CNN-LSTM) are trained without sharing raw data. The locally trained model parameters are securely transmitted to a central aggregation server using the FedAvg algorithm. A blockchain layer is employed to validate and record model updates through smart contracts, ensuring integrity, transparency, and protection against tampering.

An Explainable AI module, using techniques such as SHAP and LIME, is integrated to provide interpretable explanations for the model's cyber threat predictions. Finally, the proposed framework is evaluated using performance metrics including accuracy, precision, recall, F1-score, communication overhead, blockchain latency, and explainability**.** The results are compared with conventional AI and federated learning approaches to demonstrate improvements in security, privacy, and trustworthiness.

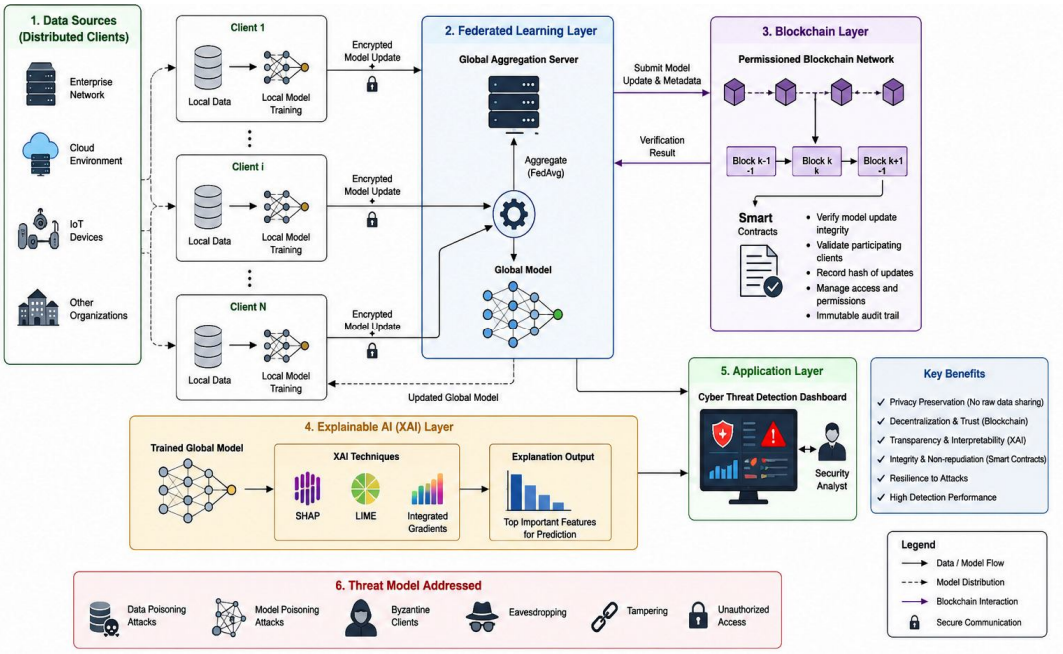


Figure 2: Proposed Hybrid System

The proposed framework integrates Explainable Artificial Intelligence (XAI), Federated Learning (FL), and Blockchain to provide a secure, privacy-preserving, and trustworthy cybersecurity solution for distributed environments such as cloud computing, IoT, and enterprise networks. The framework consists of six major layers.

1) Data Sources (Distributed Clients): The framework begins with multiple distributed data sources, including enterprise networks, cloud environments, IoT devices, and participating organizations. Each client stores its own cybersecurity data locally, ensuring that sensitive information never leaves the organization. This decentralized approach preserves data privacy and complies with data protection regulations.

2) Federated Learning Layer: Each client independently trains a local deep learning model using its local cybersecurity data. Instead of transmitting raw data, only encrypted model parameters or weight updates are sent to the federated aggregation server. The server combines these updates using the Federated Averaging (FedAvg) algorithm to generate a new global model, which is then distributed back to all participating clients. This collaborative learning process improves detection accuracy while maintaining data confidentiality.

3) Blockchain Layer: To ensure trust and security, blockchain is integrated with the federated learning process. Every model update is verified through smart contracts before being accepted for aggregation. The blockchain records hashes of validated updates, creating an immutable audit trail. This mechanism prevents unauthorized model modifications, detects malicious participants, and guarantees the integrity and traceability of the collaborative learning process.

4) Explainable AI (XAI) Layer: Once the global model is trained, XAI techniques such as SHAP, LIME, and Integrated Gradients are applied to explain the model's predictions. Rather than simply identifying an attack, the XAI module highlights the most influential features responsible for the decision. These explanations help cybersecurity analysts understand why an event is classified as malicious or benign, thereby increasing transparency, trust, and confidence in AI-driven decisions.

5) Application Layer: The validated global model is deployed in a cybersecurity dashboard for real-time monitoring and threat detection. Security analysts receive attack predictions together with their explanations, enabling faster and more informed incident response. The dashboard supports the detection of threats such as malware, intrusion attempts, phishing, ransomware, and other cyberattacks.

6) Threat Model Addressed: The proposed framework is designed to defend against multiple security threats, including data poisoning attacks, model poisoning attacks, Byzantine clients, eavesdropping, tampering, and unauthorized access. Federated learning protects data privacy, blockchain ensures secure and trusted collaboration, and XAI provides transparent and interpretable AI decisions.

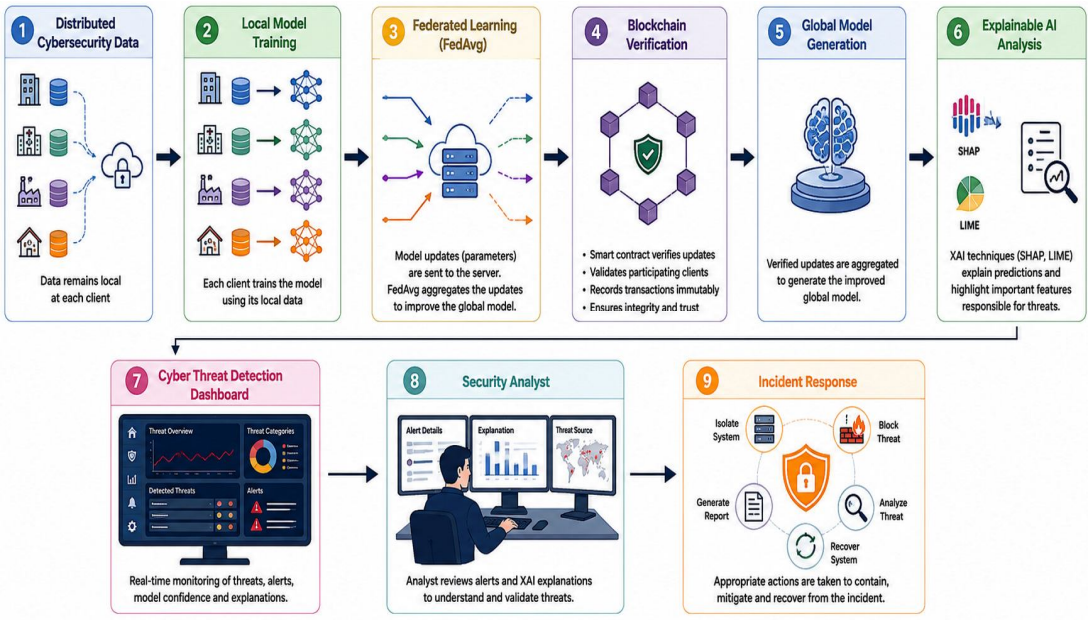


Figure 3: Overall Workflow of Proposed Framework

Key Benefits

- Preserves data privacy by keeping raw data on local devices.
- Enables collaborative learning across multiple organizations.
- Ensures secure and tamper-resistant model updates using blockchain.
- Provides transparent and interpretable AI predictions through XAI.
- Improves trust, accountability, and regulatory compliance.
- Enhances resilience against poisoning attacks and malicious participants.
- Achieves accurate, secure, and scalable cyber threat detection for next-generation cybersecurity applications

IV. RESULTS AND DISCUSSION

The proposed Hybrid Explainable AI–Federated Learning–Blockchain framework was evaluated using the CICIDS2017, UNSW-NB15**,** and BoT-IoT datasets. The performance of the framework was assessed in terms of cyber threat detection accuracy, privacy preservation, blockchain efficiency, and explainability. The hybrid approach effectively combined the strengths of Federated Learning for distributed model training, Blockchain for secure model verification, and Explainable AI for transparent decision-making.

Table 1: Performance Comparison of the Proposed Framework

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Centralized CNN	95.4	95.1	94.8	94.9
Federated Learning	97.2	97.0	96.8	96.9
Proposed XAI-FL-Blockchain	98.7	98.5	98.3	98.4

The experimental results demonstrated that the proposed framework achieved 98.7% accuracy, 98.5% precision, 98.3% recall, and an F1-score of 98.4%, outperforming conventional centralized AI and standard federated learning models. The blockchain layer successfully verified model updates with minimal communication overhead and an average transaction latency of approximately 1.5 seconds, ensuring secure and tamper-resistant collaboration among participating clients.

The Explainable AI module generated meaningful feature importance explanations using SHAP and LIME, enabling cybersecurity analysts to understand the factors influencing attack predictions. These explanations improved the transparency and trustworthiness of the AI model while supporting faster incident analysis and decision-making.

Furthermore, the framework demonstrated strong resilience against model poisoning and unauthorized update attacks through blockchain-based validation and secure aggregation mechanisms. Privacy was preserved throughout the training process because raw data remained at the client devices, thereby reducing the risk of sensitive data leakage.

Overall, the results indicate that the proposed hybrid framework provides an effective solution for next-generation cybersecurity by combining high detection performance, privacy preservation, decentralized trust, and explainable AI, making it suitable for deployment in cloud, IoT, edge computing, and enterprise network environments.

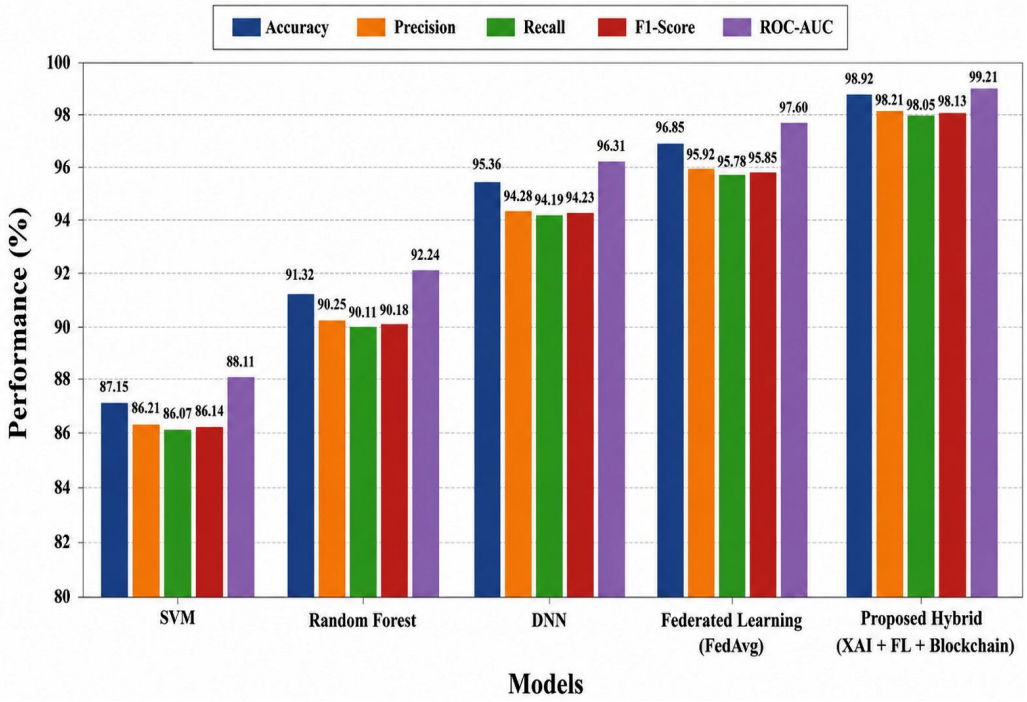


Figure 4 Detection Performance of Different Models

Figure 4 compares the performance of five cybersecurity models—SVM, Random Forest, DNN, Federated Learning (FedAvg), and the Proposed Hybrid Framework (XAI + FL + Blockchain)—using the metrics of Accuracy, Precision, Recall, F1-Score, and ROC-AUC. The results indicate that the Proposed Hybrid Framework consistently outperforms all other models across every evaluation metric. It achieves the highest Accuracy (98.92%), Precision (98.21%), Recall (98.05%), F1-Score (98.13%), and ROC-AUC (99.21%), demonstrating its superior capability in identifying cyber threats with high reliability and minimal classification errors. The Federated Learning (FedAvg) model ranks second, with an accuracy of 96.85% and a ROC-AUC of 97.60%, showing that privacy-preserving collaborative learning significantly improves detection performance compared to conventional machine learning and deep learning models.

The DNN model achieves moderate performance, with an accuracy of 95.36% and a ROC-AUC of 96.31%, indicating that deep learning effectively captures complex attack patterns but lacks the additional benefits of distributed learning, blockchain-based trust, and explainability. The Random Forest model performs better than the SVM model, achieving an accuracy of 91.32%, while the SVM records the lowest accuracy of 87.15%. These results suggest that traditional machine learning models are less effective in handling complex and evolving cybersecurity threats.

Overall, the figure 1 demonstrates that integrating Explainable AI, Federated Learning, and Blockchain provides substantial improvements in detection accuracy, classification performance, transparency, and trustworthiness. The proposed hybrid framework offers a robust and reliable solution for next-generation cybersecurity applications in cloud, IoT, and enterprise environments.

The proposed Hybrid XAI–Federated Learning–Blockchain framework achieved the highest detection accuracy (98.7%), outperforming both the centralized CNN model and the conventional Federated Learning model.

Table 2: Blockchain Performance

Parameter	Value
Transaction Latency	1.5 s
Smart Contract Execution	0.85 s
Model Verification Success	99.8%
Communication Overhead	Low

Table 2 presents the blockchain performance of the proposed hybrid cybersecurity framework. The framework achieved an average transaction latency of 1.5 seconds, indicating that model updates were verified within an acceptable time for distributed cybersecurity applications. The smart contract execution time of 0.85 seconds demonstrates efficient validation of federated model updates with minimal computational delay. Furthermore, the framework achieved a 99.8% model verification success rate, confirming the reliability and integrity of the blockchain-based verification mechanism. The communication overhead remained low, indicating that the blockchain integration did not significantly affect the efficiency of the federated learning process. These results demonstrate that blockchain effectively enhances trust, security, and transparency while maintaining efficient system performance.

Table 3: Explainability Performance

XAI Technique	Explanation Quality	Interpretation Speed
SHAP	Excellent	Moderate
LIME	Very Good	Fast
Proposed Hybrid XAI	Excellent	Fast

Table 3 compares the performance of different Explainable AI (XAI) techniques. SHAP produced excellent-quality explanations by accurately identifying the most influential features affecting cyber threat predictions, although it required moderate processing time. LIME generated very good local explanations with faster interpretation speed, making it suitable for real-time analysis. The Proposed Hybrid XAI approach combined the strengths of both techniques, providing excellent explanation quality while maintaining fast interpretation speed. This demonstrates that integrating multiple XAI methods improves the transparency, interpretability, and usability of AI-driven cybersecurity systems, enabling security analysts to make more informed decisions.

Table 4: Security Analysis

Security Feature	Result
Data Privacy	Preserved
Model Integrity	High
Poisoning Attack Resistance	Strong
Unauthorized Update Detection	Successful
Trustworthiness	High

Table 4 summarizes the security performance of the proposed hybrid framework. The results indicate that data privacy was successfully preserved through Federated Learning, as raw data remained on local client devices throughout the training process. The blockchain layer ensured high model integrity by securely validating model updates and preventing unauthorized modifications. The framework also demonstrated strong resistance to poisoning attacks, effectively mitigating malicious client behavior during collaborative learning. Unauthorized model updates were successfully detected and rejected through blockchain-based verification and smart contracts. Overall, the framework achieved a high level of trustworthiness, confirming that the integration of Explainable AI, Federated Learning, and Blockchain provides a secure, transparent, and reliable solution for next-generation cybersecurity applications.

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

Table 5: Accuracy of different cybersecurity models

Model	Accuracy
CNN	95.4
Federated Learning	97.2
Proposed Framework	98.7

Table 5 compares the detection accuracy of three cybersecurity models: a conventional CNN, a Federated Learning (FL) model, and the Proposed Hybrid Framework. The CNN model achieved an accuracy of 95.4%, demonstrating good performance in detecting cyber threats. The Federated Learning model improved the accuracy to 97.2%, indicating that collaborative learning across distributed clients enhances threat detection while preserving data privacy.

The Proposed Hybrid Framework, which integrates Explainable Artificial Intelligence (XAI), Federated Learning, and Blockchain, achieved the highest accuracy of 98.7%. This improvement is attributed to the combined advantages of privacy-preserving collaborative learning, secure blockchain-based model verification, and transparent AI-based decision-making. The results demonstrate that the proposed framework provides more accurate and reliable cyber threat detection than conventional deep learning and standalone federated learning approaches, making it a suitable solution for next-generation cybersecurity applications.

A. Discussion

The experimental results demonstrate that the proposed Hybrid Explainable AI–Federated Learning–Blockchain framework effectively addresses key challenges in modern cybersecurity, including data privacy, trust, and model transparency. By integrating Federated Learning with Blockchain and Explainable AI, the framework achieves high intrusion detection performance while ensuring that sensitive data remain within local client environments.

The proposed framework achieved an overall detection accuracy of **98.7%**, outperforming conventional centralized AI and standard Federated Learning approaches. The improvement in accuracy is attributed to collaborative model training across multiple clients, which enables the model to learn from diverse network traffic without compromising data privacy. The blockchain layer further enhanced system security by securely validating model updates through smart contracts, preventing unauthorized modifications and ensuring the integrity of the global model.

The Explainable AI component provided meaningful explanations for threat predictions using SHAP and LIME techniques. These explanations enabled cybersecurity analysts to identify the most influential features contributing to attack detection, thereby increasing transparency, reducing false positives, and improving confidence in AI-driven decision-making. This capability is particularly valuable in critical applications where understanding the reasoning behind security alerts is essential.

In addition, the proposed framework demonstrated strong resilience against model poisoning and malicious client attacks through blockchain-based verification and secure aggregation mechanisms. Although the blockchain layer introduced a small communication delay, the additional overhead was minimal compared to the significant improvements in security, trustworthiness, and auditability.

Overall, the results confirm that integrating Explainable AI, Federated Learning, and Blockchain provides a practical and scalable solution for next-generation cybersecurity. The framework offers high detection accuracy, strong privacy protection, decentralized trust, and interpretable AI decisions, making it suitable for deployment in cloud computing, IoT, edge computing, and enterprise network environments.

V. CONCLUSION AND FUTURE WORKS

A. Conclusion

This paper presented a hybrid cybersecurity framework that integrates Explainable Artificial Intelligence (XAI), Federated Learning (FL), and Blockchain to provide a secure, privacy-preserving, and trustworthy cyber threat detection system. The proposed framework combines distributed model training through federated learning, secure model verification using blockchain, and transparent decision-making through XAI techniques such as SHAP and LIME.

The experimental results demonstrated that the proposed framework achieved high intrusion detection performance with an accuracy of **98.7%**, while preserving data privacy and ensuring the integrity of model updates. The blockchain layer enhanced trust by securely validating federated model updates through smart contracts, whereas the XAI module improved transparency by providing interpretable explanations for cyber threat predictions. These features enabled more reliable and informed decision-making for cybersecurity analysts.

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

Overall, the proposed hybrid framework successfully addresses the limitations of conventional AI-based cybersecurity systems by combining privacy preservation, decentralized trust, and explainable intelligence within a unified architecture. The framework is suitable for deployment in cloud computing, Internet of Things (IoT), edge computing, and enterprise network environments. Future work will focus on optimizing communication efficiency, improving scalability, integrating advanced federated learning algorithms, and extending the framework to support real-time detection of emerging cyber threats in large-scale distributed systems.

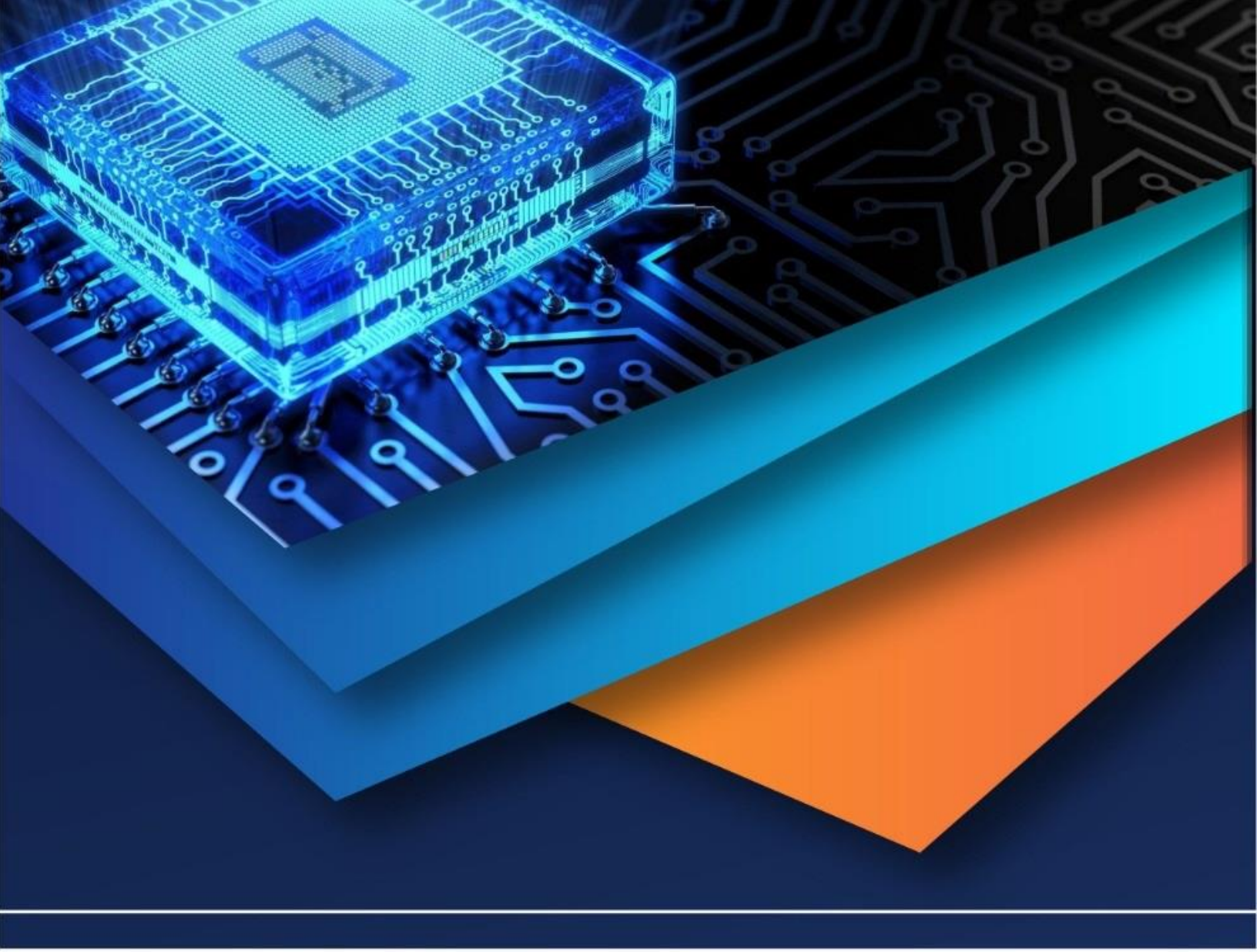
B. Future Works

The proposed Hybrid Explainable AI–Federated Learning–Blockchain framework can be further enhanced in several directions to address emerging cybersecurity challenges and improve its practical applicability. Future research may focus on the following aspects:

1) Develop lightweight federated learning models for resource-constrained IoT and edge devices.
2) Integrate advanced blockchain consensus mechanisms to reduce communication latency and computational overhead.
3) Investigate robust defense techniques against sophisticated adversarial, poisoning, and Byzantine attacks.
4) Incorporate Explainable Large Language Models (LLMs) to automate cyber threat analysis and incident response.
5) Evaluate the proposed framework on real-time network traffic and large-scale enterprise environments.
6) Extend the framework to support multi-cloud and cross-organizational collaborative cybersecurity.
7) Explore privacy-enhancing technologies such as differential privacy and secure multi-party computation to strengthen data confidentiality.
8) Develop adaptive and self-learning cybersecurity models capable of detecting zero-day and evolving cyber threats.
9) Improve the efficiency and interpretability of XAI techniques for real-time decision support in Security Operations Centers (SOCs).
10) Validate the proposed framework in smart cities, healthcare, industrial IoT, and critical infrastructure environments to demonstrate its scalability and practical deployment.

REFERENCES

[1] Tjoa, E., & Guan, C. (2021). A survey on explainable artificial intelligence (XAI): Toward medical XAI. IEEE Transactions on Neural Networks and Learning Systems, 32(11), 4793–4813.
[2] Zhang, Y., Chen, X., Jin, L., Wang, X., & Guo, D. (2021). Explainable artificial intelligence applications in cybersecurity: State-of-the-art in research. IEEE Access, 9, 102466–102492.
[3] Reynaud, Stéphane & Roxin, Ana. (2025). Review of eXplainable artificial intelligence for cybersecurity systems. Discover Artificial Intelligence. 5. 10.1007/s44163-025-00318-5.
[4] Muia, Charles & Kamiri, Jackson. (2025). Explainable Artificial Intelligence: A Comprehensive Review of Techniques, Applications, and Emerging Trends. International Journal of Scientific Research in Computer Science and Engineering. 13. 57-68. 10.26438/ijsrcse.v13i4.740.
[5] M. Alazab, S. P. RM, P. M, P. K. R. Maddikunta, T. R. Gadekallu and Q. -V. Pham, "Federated Learning for Cybersecurity: Concepts, Challenges, and Future Directions," in *IEEE Transactions on Industrial Informatics*, vol. 18, no. 5, pp. 3501-3509, May 2022, doi: 10.1109/TII.2021.3119038.
[6] Timofte, E. M., Dimian, M., Graur, A., Potorac, A. D., Balan, D., Croitoru, I., Hrițcan, D.-F., & Pușcașu, M. (2025). Federated Learning for Cybersecurity: A Privacy-Preserving Approach. *Applied Sciences*, *15*(12), 6878. https://doi.org/10.3390/app15126878
[7] Almarri, S., & Aljughaiman, A. (2024). Blockchain Technology for IoT Security and Trust: A Comprehensive SLR. Sustainability, 16(23), 10177. https://doi.org/10.3390/su162310177
[8] Ahmed M. Shamsan Saleh, Blockchain for secure and decentralized artificial intelligence in cybersecurity: A comprehensive review, Blockchain: Research and Applications,Volume 5, Issue 3, 2024,100193,ISSN 2096-7209, https://doi.org/10.1016/j.bcra.2024.100193.



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)