An Integrated Privacy Preserving Cybersecurity for Distributed IoT, Edge and Cloud Environments

Vinayak Musale[1], Basant Kumar[2]

[1] Lincoln University College, Malaysia; [2] Modern College of Business and Science, Oman

pdf.vinayak@lincoln.edu.my[1]; basant@mcbs.edu.om[2]

Abstract: The increasing convergence of Internet of Things, edge and cloud computing has transformed modern digital ecosystems but has also introduced significant cybersecurity challenges related to data privacy, trust management and regulatory compliance. Existing centralized security frameworks often rely on extensive data aggregation, creating privacy vulnerabilities and limiting their effectiveness in highly distributed environments. To address these limitations, this study presents a unified privacy preserving cybersecurity framework that integrates federated learning, differential privacy, blockchain based trust management and explainable artificial intelligence (XAI). A distributed prototype was implemented by deploying collaborative intrusion detection nodes across simulated IoT, edge and cloud infrastructures. Federated learning enables participating nodes to jointly train intrusion detection models without exposing locally generated data, while differential privacy protects model updates against potential information leakage. Blockchain technology establishes a decentralized and tamper resistant trust mechanism that strengthens auditability and collaboration among participating entities. Furthermore, explainable AI provides interpretable security insights that enables analysts to understand and validate model predictions with greater confidence. The proposed framework was evaluated using benchmark intrusion detection datasets under distributed cyberattack scenarios. Experimental findings demonstrate that the framework consistently achieves high intrusion detection performance along with preserving data privacy, maintaining trusted collaboration and improving the transparency of security decisions. These results highlight the potential of integrating decentralized learning, privacy preserving mechanisms, blockchain enabled trust and explainable intelligence to develop secure, scalable and trustworthy cybersecurity solutions for next generation distributed computing environments.

Keywords: Blockchain; Cybersecurity; Differential Privacy; Internet of Things; Threat Detection.

1. Introduction

The widespread integration of IoT, edge computing and cloud platforms has fundamentally transformed modern digital ecosystems that enables intelligent services across domains such as healthcare, industrial automation, smart cities and critical infrastructure. Despite these advancements, the growing interconnectivity of distributed devices has considerably expanded the cyberattack surface, increases the complexity of protecting sensitive data, ensures system resilience and maintain regulatory compliance. Conventional cybersecurity frameworks predominantly rely on centralized data collection and analysis, requiring large volumes of information to be transferred to a central server. Although effective in certain scenarios, these approaches often raise concerns related to data privacy, communication overhead, scalability and trust among participating entities.

Recent developments in federated learning, blockchain technology and explainable artificial intelligence have created new possibilities for designing decentralized and privacy aware cybersecurity solutions. Federated learning enables collaborative model training without exposing raw data, differential privacy minimizes the risk of information leakage during model updates, blockchain establishes a decentralized and tamper resistant trust mechanism whereas explainable AI improves the interpretability of security decisions. Motivated by these complementary capabilities, this paper proposes a unified privacy preserving cybersecurity framework which combines these technologies to strengthen collaborative threat detection across distributed IoT, edge and cloud environments. The effectiveness of the proposed framework is validated through experimental evaluation using benchmark cybersecurity datasets under representative distributed attack scenarios.

2. Related work

The growing sophistication of cyber threats has encouraged the extensive adoption of machine learning and deep learning techniques for intelligent intrusion detection and cyberattack analysis. Authors, Zhang et al. [1] proposed a CNN and LSTM based intrusion detection framework that effectively captures complex attack patterns in IoT environments where as Alazab et al. [2] demonstrated that hybrid deep learning models significantly improve the accuracy of cyberattack classification across varied network scenarios. These studies highlight the potential of data driven approaches to strengthen modern cybersecurity systems.

To overcome the privacy limitations of centralized learning, federated learning has gained considerable attention as a decentralized learning paradigm. Kairouz et al. [3] demonstrated that collaborative model training can be achieved without transferring raw data from participating devices, thereby improve privacy preservation and reduce communication risks. Nevertheless, federated learning alone does not adequately address issues related to trust establishment, data integrity and accountability among distributed participants.

Blockchain technology has been explored as a complementary solution for enhancing trust and ensuring secure collaboration in decentralized environments. Authors, Kumar and Singh [4] presented a blockchain enabled cybersecurity framework for cyber physical systems, whereas Bansal and Patel [5] introduced a blockchain based trust management model for autonomous computing environments. Although these approaches strengthen transparency and tamper resistance, they provide limited support for interpreting security decisions generated by intelligent models.

More recently, explainable artificial intelligence has emerged as an effective approach for improving the transparency and interpretability of AI driven cybersecurity systems. Wang et al. [6] emphasized the importance of explainable security analytics for building trustworthy cybersecurity solutions in Industry 5.0 environments. Despite these advances, relatively few studies have combined federated learning, differential privacy, blockchain based trust management and explainable AI within a single operational cybersecurity framework. Addressing this research gap forms the primary motivation for the framework proposed in this study.

3. System Architecture and Methodology

The proposed framework consists of five interconnected layers that collectively support secure and privacy preserving threat intelligence generation. Fig. 1 presents system architecture of the proposed privacy preserving cybersecurity framework integrating federated learning, differential privacy, blockchain-based trust management, explainable security analytics, and security operations for distributed IoT, edge and cloud environments.

3.1 Distributed Infrastructure Layer: The infrastructure layer comprises IoT devices, edge nodes, and cloud services responsible for generating and processing security-relevant data. Each participant maintains local ownership of collected information.

3.2 Federated Learning Layer: Local intrusion detection models are trained independently at participating nodes. Model parameters are periodically transmitted to a federated aggregation server where a global model is generated and redistributed.

3.3 Privacy Preservation Layer: Differential privacy mechanisms inject calibrated noise into local model updates before transmission. This process limits the possibility of reconstructing sensitive information from exchanged parameters.

3.4 Trust Management Layer: A permissioned blockchain records model updates and participant activities. Smart contracts validate transactions and maintain trust scores based on contribution quality and system behavior.

3.5 Explainable Security Analytics Layer: SHAP-based feature attribution techniques are employed to explain intrusion detection decisions. This enables analysts to understand influential features contributing to attack classifications.

3.6 Security Operations Layer: The final layer generates intrusion alerts, evaluates risk levels, and supports incident response decisions using intelligence produced by preceding layers.

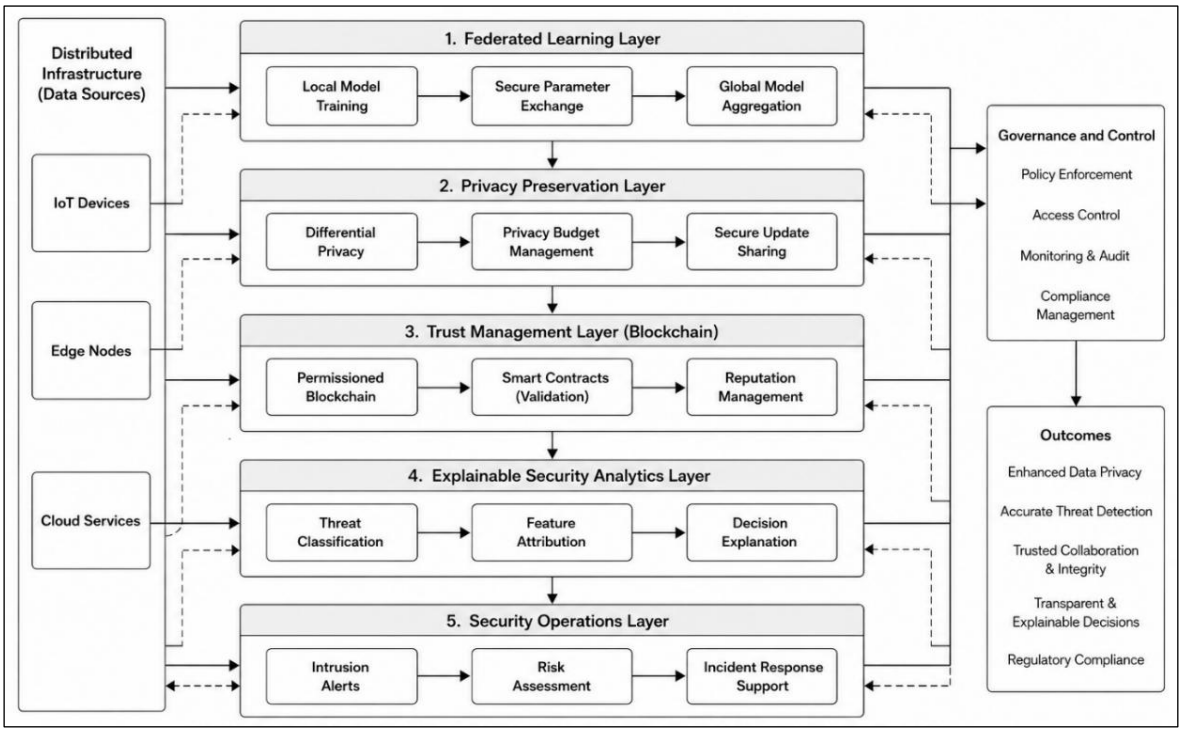

Figure 1. Architectural Design of the Privacy Preserving Threat Intelligence Framework

4. Experimental Results

4.1 Experimental Setup: A prototype implementation was developed using Python, TensorFlow Federated, Hyperledger Fabric, and SHAP. Experiments were performed on a distributed testbed. Table 1. presents experimental configuration and system parameters used for framework evaluation. The framework was evaluated using Accuracy, Precision, Recall, F1-score, Communication Overhead, and Trust Validation Rate.

Table 1. Experimental Configuration and System Parameters

Parameter	Value
IoT Nodes	50
Edge Servers	5
Cloud Server	1
Blockchain Type	Hyperledger Fabric
FL Rounds	100
Privacy Budget (ε)	1.0
Dataset	CICIDS2017

4.2 Threat Detection Performance

The federated intrusion detection model demonstrated strong classification performance across multiple attack categories. Fig. 2 presents the threat detection performance of the proposed privacy-preserving cybersecurity framework. The federated learning-based intrusion detection model achieved an accuracy of 97.8%, indicating its effectiveness in identifying malicious activities across distributed environments. The precision and recall values of 97.3% and 96.9%, respectively, demonstrate the model's ability to minimize false alarms while maintaining high detection capability.

The framework achieved an F1 score of 97.1%, demonstrating its ability to maintain a strong balance between precision and recall across a wide range of cyberattack scenarios.

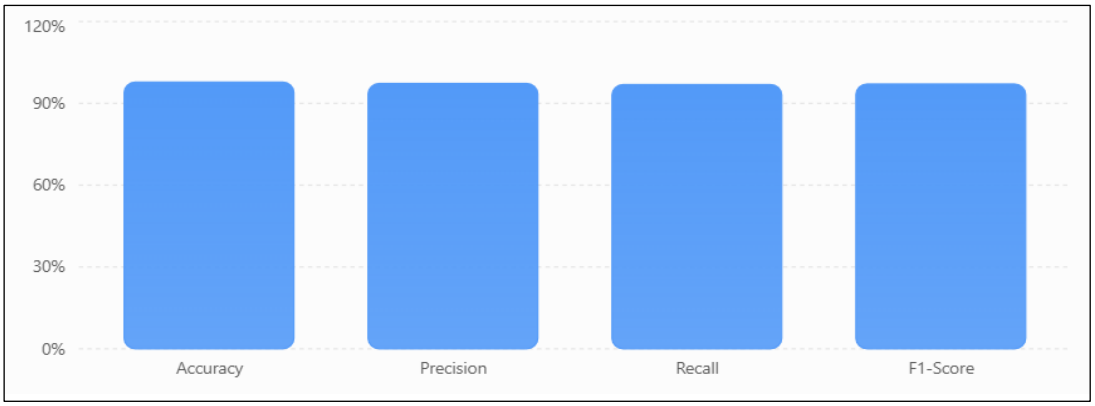

Figure 2. Threat detection performance of the proposed framework across evaluation metrics

These findings indicate that collaborative learning can deliver reliable and accurate threat detection along with preserving data privacy by eliminating the need to share sensitive raw data among participating entities.

4.3 Privacy Preservation Analysis

The incorporation of differential privacy effectively minimized the risk of information leakage while preserving a high level of intrusion detection performance. Fig. 3 shows the influence of differential privacy on the detection capability of the proposed framework. It demonstrates that privacy preservation can be achieved with only a marginal impact on overall detection effectiveness.

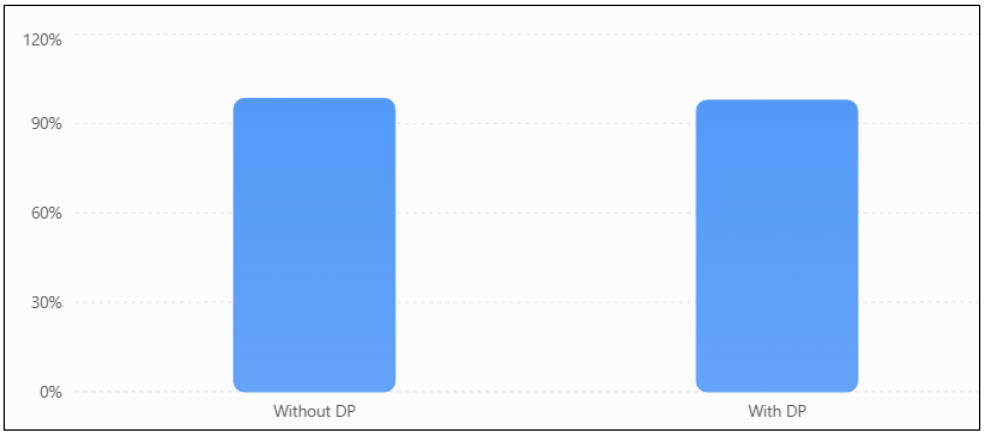

Figure 3. Effect of differential privacy on intrusion detection accuracy

The proposed model accomplished an intrusion detection with accuracy of 98.4% in the absence of privacy protection, which slightly decreased to 97.8% after the integration of differential privacy mechanisms. This reduction of 0.6% points demonstrates that stronger privacy guarantees can be incorporated without significantly compromising detection performance. The results show that the differential privacy effectively balances data confidentiality and cybersecurity effectiveness. Also this make it a practical solution for secure collaborative learning in distributed environments.

4.4 Blockchain Trust Evaluation

The blockchain layer effectively validated model updates while maintaining secure and tamper resistant audit trails throughout the collaborative learning process. Fig. 4 illustrates the performance of the blockchain based trust management layer integrated into the proposed cybersecurity framework, highlights its capability to ensure trustworthy model verification and transparent record management across distributed participants. The blockchain layer achieved a transaction success rate of 99.1%, indicating reliable processing and secure recording of security related transactions across the distributed network. In addition, a trust validation accuracy of 98.7% confirms its effectiveness in verifying participant contributions and fostering trustworthy collaboration among distributed entities.

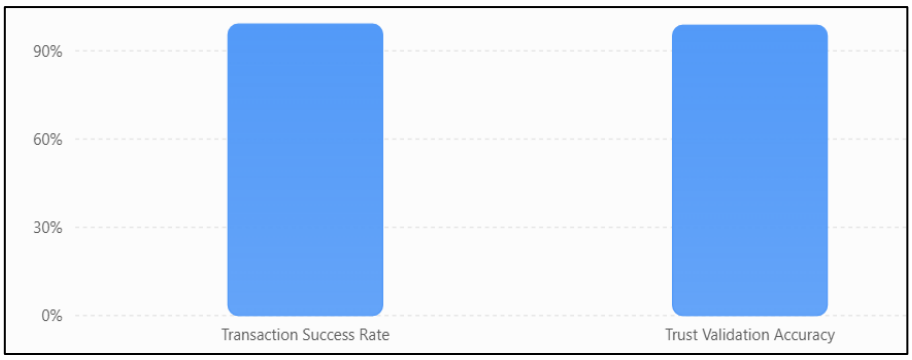

Figure 4. Blockchain Trust Validation and Transaction Success Rate Evaluation

These findings emphasize the worth of blockchain technology in preserving data integrity, strengthen accountability and enable secure information exchange across decentralized IoT, edge and cloud computing environments.

5. Conclusion and Future Scope

This paper presented the design, implementation and evaluation of a privacy preserving cybersecurity framework for distributed IoT, edge and cloud computing environments. It integrates federated learning, differential privacy, blockchain based trust management and explainable artificial intelligence to address critical challenges related to secure collaboration, data privacy, trust establishment and reliable threat detection in decentralized infrastructures.

The experimental results demonstrate the practicality and effectiveness of the proposed framework in achieving high intrusion detection performance while safeguarding data confidentiality and ensuring system integrity. The framework provides a secure and transparent approach for collaborative cybersecurity through the combination of decentralized intelligence with privacy preserving learning, blockchain enabled trust and interpretable decision making. Overall, the findings highlight the potential of the proposed architecture to strengthen cyber resilience and support trustworthy security operations across heterogeneous next generation IoT, edge and cloud ecosystems.

Future work will focus on large scale deployments, adaptive threat intelligence mechanisms and optimization of blockchain related communication overhead.

References

[1] Z. Zhang, M. Li, and A. Alazab, “An intelligent CNN–LSTM based intrusion detection framework for autonomous IoT networks,” *IEEE Internet of Things Journal*, 2022.

[2] A. Alazab, N. Islam, and R. J. Alazab, “Deep learning fusion model for IoT threat detection using CNN–GRU,” *Future Generation Computer Systems*, 2023.

[3] P. Kairouz et al., “Advances and open problems in federated learning,” *Foundations and Trends in Machine Learning*, 2021.

[4] A. Kumar and R. Singh, “Blockchain-driven AI security architecture for intelligent cyber-physical systems,” *IEEE Access*, 2024.

[5] R. Bansal and M. Patel, “Blockchain-based trust management framework for autonomous digital systems,” *Sensors*, 2023.

[6] X. Wang, H. Zhao, and K. Yu, “Hybrid privacy-preserving cybersecurity framework for Industry 5.0 systems,” *IEEE Transactions on Industrial Informatics*, 2024.

[7] T. D. Nguyen, A. Berrada, and D. S. Kim, “Differential privacy-enabled machine learning for cybersecurity applications,” *IEEE Transactions on Information Forensics and Security*, 2022.

[8] I. H. Sarker, M. A. Hossain, and S. Khatun, “Privacy-preserving healthcare IoT framework using federated learning and blockchain,” *IEEE Journal of Biomedical and Health Informatics*, 2023.

[9] M. Rahman, T. Hasan, and Y. Liu, “Reinforcement learning-based adaptive intrusion prevention in autonomous systems,” *Computers & Security*, 2023.