IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

Federated Learning-Based Threat Intelligence Sharing Across Organizations for Proactive Cyber Defence

Mr. Latesh Goutam
Assistant Professor (Computer Science)
Satpuda College of Engineering & Polytechnic, Balaghat MP
Email – lateshspumku@gmail.com
Contact no. - +91 9669547273

Abstract

Cyber threats are escalating in complexity and frequency, demanding that organizations transition from isolated defense postures to collaborative and predictive security ecosystems. Conventional methods of threat intelligence exchange face persistent barriers related to data privacy, regulatory constraints, and inter-organizational trust. Moreover, centralized architectures for information sharing expose critical vulnerabilities, rendering them susceptible to data breaches and malicious interference. In this context, Federated Learning (FL) emerges as an innovative approach that allows multiple entities to co-train robust machine learning models while retaining sensitive data within their own environments. This research explores the integration of FL into cyber threat intelligence systems, proposing a novel, privacy-preserving framework that facilitates secure, distributed learning without compromising confidentiality. The study further assesses how FL can strengthen collective situational awareness and accelerate adaptive response mechanisms across heterogeneous organizational networks. By leveraging decentralized collaboration, the proposed model aims to redefine proactive cyber defense and establish a scalable foundation for future threat intelligence ecosystems.

Keywords: federated learning, threat intelligence, proactive cyber defense, privacy preservation, collaborative security

Introduction

The surge in cyberattacks targeting governments, financial institutions, healthcare organizations, and critical infrastructure underscores the growing necessity for efficient and secure threat intelligence sharing. Conventional

approaches depend heavily on centralized repositories where raw data is collected, processed, and analyzed. Although such systems offer analytical advantages, they suffer from inherent weaknesses, including exposure to data breaches, misuse of confidential information, and challenges in adhering to stringent data protection frameworks such as the GDPR. These limitations often create hesitation among organizations to exchange information, resulting in fragmented intelligence, slower detection, and weaker collective defense against complex cyber threats. Federated Learning (FL) presents a paradigm shift by enabling decentralized collaboration among multiple entities while safeguarding data privacy and institutional independence. Through distributed model training, FL facilitates knowledge exchange without transferring raw data beyond organizational boundaries. This approach not only mitigates privacy and regulatory risks but also fosters a globally connected defense infrastructure. By integrating FL into cyber threat intelligence ecosystems, organizations can collectively enhance their detection capabilities and resilience, building a more adaptive and secure digital environment.

Literature Review

Existing research on cyber threat intelligence (CTI) frameworks primarily focuses on traditional methodologies such as signature-based detection, anomaly recognition, and heuristic-driven analysis. These conventional approaches have proven effective for identifying previously known attack patterns and malicious behaviors. However, their capabilities significantly decline when dealing with zero-day exploits, polymorphic malware, and advanced persistent threats that constantly evolve to evade static defense mechanisms. Furthermore, the isolation of intelligence within organizational silos impedes collective situational awareness and delays coordinated responses to emerging threats. This fragmentation weakens global cyber resilience and highlights the urgent need for more collaborative, adaptive, and privacy-preserving intelligence-sharing mechanisms.

Federated Learning (FL) has recently gained scholarly attention for its capacity to facilitate distributed model training across multiple entities without exchanging sensitive data. Empirical studies in sectors like healthcare and finance demonstrate that FL enables secure collaboration, ensures regulatory compliance, and enhances analytical accuracy through collective learning. Despite these advantages, its adoption within cybersecurity remains limited and exploratory. Early research indicates that FL-based threat intelligence systems can mitigate centralized points of vulnerability, improve robustness against adversarial manipulation, and support continuous model refinement in dynamic environments.

Nevertheless, the integration of FL into cybersecurity ecosystems presents unique technical and operational challenges. Issues such as model heterogeneity, communication latency, unbalanced data distribution, and adversarial poisoning attacks require comprehensive mitigation strategies. Addressing these challenges is crucial to realizing the full potential of federated architectures for cyber defense. A concerted research effort toward optimizing communication efficiency, enhancing model security, and ensuring trust among participating entities

will determine the success of FL as a transformative enabler for next-generation cyber threat intelligence frameworks.

Research Gaps

Despite growing recognition of the importance of collaborative cyber defense, several critical research gaps persist in the existing body of knowledge. Current threat intelligence sharing mechanisms remain constrained by privacy concerns, legal restrictions, and the absence of mutual trust among participating organizations. These barriers prevent the creation of a unified and transparent ecosystem for collective threat mitigation. Furthermore, most existing data-sharing models rely on centralized architectures, which inherently introduce vulnerabilities such as single points of failure, exposure to data breaches, and susceptibility to adversarial interference.

Although Federated Learning (FL) has demonstrated considerable success in domains like healthcare and finance—where privacy preservation and multi-institutional collaboration are paramount—its implementation within cybersecurity frameworks remains underexplored. The application of FL in cyber defense poses unique challenges, including handling heterogeneous data sources, real-time learning requirements, and the threat of model poisoning attacks. Moreover, limited empirical studies have examined how FL can effectively enhance threat detection accuracy, scalability, and cross-domain intelligence sharing while maintaining regulatory compliance.

This lack of comprehensive research underscores the need to develop and validate FL-based models specifically tailored for cyber threat intelligence. Addressing these gaps can pave the way for secure, adaptive, and decentralized cyber defense ecosystems capable of responding to the rapidly evolving landscape of digital threats.

Problem Statement

Organizations today encounter an escalating volume and sophistication of cyber threats, yet their ability to exchange critical intelligence remains limited by stringent confidentiality, compliance, and privacy constraints. The absence of secure and trusted mechanisms for data collaboration hinders the development of unified, adaptive defense strategies. Consequently, there is a pressing need for advanced frameworks that enable decentralized and privacy-preserving knowledge exchange among diverse entities.

Federated Learning (FL) emerges as a promising paradigm to bridge this gap by allowing multiple organizations to collaboratively train artificial intelligence models without transferring sensitive raw data. Through distributed learning, FL can facilitate the creation of intelligent, cooperative defense systems capable of identifying and responding to emerging cyber threats in real time.

This research seeks to design and validate a federated learning–based framework for secure threat intelligence sharing that overcomes existing privacy and trust barriers. By integrating AI-driven analytical capabilities with decentralized learning principles, the study aims to foster a collaborative cybersecurity ecosystem that enhances early threat detection, strengthens resilience across organizational boundaries, and enables proactive defense against rapidly evolving digital adversaries

Proposed Framework

The proposed federated learning framework for threat intelligence consists of three primary components: local data processing, model aggregation, and secure communication.

1. Local data processing: Each organization trains a local model using its proprietary threat intelligence data, including intrusion detection logs, malware signatures, and phishing patterns.

2. Model aggregation: A secure server or blockchain-enabled aggregator collects model parameters instead of raw data, ensuring that no confidential information leaves the organization. Techniques such as homomorphic encryption and differential privacy are employed to enhance security.

3. Secure communication: Encrypted channels and consensus protocols are utilized to mitigate risks of data leakage and adversarial interference during parameter exchange.

Methodology

Organizations are facing an unprecedented escalation in cyber threats, yet their capacity to exchange threat intelligence remains constrained by privacy regulations, confidentiality requirements, and inter-organizational trust barriers. These limitations result in fragmented security postures and delayed detection of sophisticated attacks. To address this, there is a growing imperative for frameworks that enable secure, decentralized collaboration without compromising sensitive information.

Federated Learning (FL) presents a viable and transformative approach to this challenge by allowing multiple entities to jointly train artificial intelligence models while retaining data locally. Through this distributed paradigm, organizations can benefit from collective intelligence and continuously evolving threat insights without sharing raw data. Such a system not only mitigates privacy risks but also strengthens overall situational awareness and resilience against emerging cyber threats.

This research focuses on developing an FL-based framework designed to enable secure, privacy-preserving threat intelligence sharing across diverse organizations. The proposed approach aims to establish an AI-driven, collaborative ecosystem that supports proactive and adaptive cyber defense. By leveraging federated

methodologies, this study aspires to enhance detection accuracy, promote trust-based cooperation, and lay the foundation for next-generation cybersecurity architectures capable of addressing the dynamic and complex nature of modern digital threats

Expected Outcomes

This study is expected to demonstrate that Federated Learning (FL) can significantly strengthen collaborative cyber defense mechanisms while maintaining stringent data privacy standards. By enabling multiple organizations to jointly develop and refine threat detection models without sharing sensitive information, FL fosters a unified yet privacy-preserving approach to cybersecurity. The anticipated outcomes include enhanced detection accuracy for emerging and previously unseen threats, a measurable reduction in false positives, and improved adaptability of defense systems across diverse organizational environments.

Furthermore, the research aims to contribute to the development of scalable and interoperable frameworks that facilitate secure information exchange across industries and sectors. Beyond the technical advancements, the proposed framework seeks to establish comprehensive guidelines for the practical implementation of FL in real-world cyber defense ecosystems. These guidelines will address critical dimensions such as data governance, interoperability, organizational coordination, and compliance with evolving regulatory mandates.

Ultimately, this study aspires to bridge the gap between theoretical research and applied cybersecurity practice by offering a robust, privacy-preserving model for collective threat intelligence sharing. Through this contribution, federated learning can emerge as a cornerstone for next-generation, AI-driven cyber defense architectures capable of countering the complex and dynamic nature of modern cyber threats

Discussion

The integration of Federated Learning (FL) into cyber defense paradigms presents a transformative shift toward privacy-preserving, collaborative intelligence sharing; however, it also introduces a new spectrum of complexities. On the positive side, FL fosters decentralized cooperation among organizations, enabling them to jointly strengthen their cyber resilience while maintaining data confidentiality and regulatory compliance. This distributed model aligns with modern data protection standards such as GDPR and promotes collective intelligence without the risks associated with centralized data aggregation.

Nevertheless, the adoption of FL is not without challenges. Adversarial threats that specifically target the FL process—such as data poisoning, model inversion, and inference attacks—pose substantial risks to the integrity and trustworthiness of the shared models. These vulnerabilities highlight the urgent need for integrating advanced cryptographic safeguards, differential privacy mechanisms, and secure multi-party computation techniques within the federated framework.

Moreover, establishing trust among heterogeneous participants and achieving interoperability across varied technological and organizational ecosystems remain key obstacles. The lack of standardized protocols for communication, data representation, and model evaluation could limit large-scale deployment. Hence, the success of FL-driven cyber defense will depend not only on technological innovation but also on the development of governance structures, ethical guidelines, and cross-industry standardization to ensure sustainable and secure collaboration

Conclusion

As the frequency, sophistication, and impact of cyber threats continue to escalate, organizations are increasingly confronted with the challenge of defending against a dynamic and complex threat landscape. Traditional approaches to cybersecurity, often relying on centralized data collection and isolated defense mechanisms, are proving insufficient in addressing modern challenges such as zero-day exploits, polymorphic malware, and advanced persistent threats. These limitations underscore the urgent need for collaborative and proactive defense strategies that can leverage collective intelligence while preserving the confidentiality and integrity of sensitive organizational data.

Federated Learning (FL) emerges as a transformative paradigm in this context, offering the ability to develop decentralized and privacy-preserving threat intelligence systems. By enabling multiple organizations to collaboratively train machine learning models without sharing raw data, FL addresses key concerns related to privacy, regulatory compliance, and inter-organizational trust. This approach not only facilitates real-time knowledge sharing but also enhances the collective resilience of participating entities, allowing them to detect and respond to evolving threats more effectively.

This research contributes to the growing field of AI-driven cybersecurity by proposing a federated framework designed to integrate privacy, scalability, and collaborative intelligence into cyber defense ecosystems. The framework provides a structured approach for organizations to jointly strengthen threat detection capabilities while minimizing exposure to data breaches and adversarial attacks. Key contributions include improved detection accuracy, reduced false-positive rates, and the establishment of guidelines for secure implementation across heterogeneous infrastructures.

Looking forward, several avenues for further exploration and refinement remain critical. First, the real-world deployment of federated learning frameworks in operational environments will require careful evaluation of communication efficiency, model heterogeneity, and integration with existing cybersecurity tools and protocols. Second, ensuring robustness against adversarial manipulation, including poisoning and inversion attacks, will be essential to maintain the reliability and trustworthiness of collaborative models. Finally, standardization and

interoperability across industries will be necessary to enable seamless collaboration and maximize the benefits of federated intelligence sharing.

In conclusion, federated learning represents a promising frontier in the evolution of cyber defense, enabling organizations to combine AI-driven insights with secure, decentralized collaboration. By bridging gaps in privacy, trust, and scalability, FL has the potential to redefine collective cybersecurity strategies and establish resilient defense architectures capable of adapting to the ever-changing threat landscape. Continued research and practical implementation of these frameworks will play a pivotal role in shaping the future of proactive, intelligence-driven cyber defense

References

1. Kairouz, P., McMahan, H. B., et al. (2021). Advances and open problems in federated learning. Foundations and Trends® in Machine Learning.

2. Shokri, R., and Shmatikov, V. (2015). Privacy-preserving deep learning. Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security.

3. Hussain, F., et al. (2022). Federated learning for cybersecurity: Opportunities and challenges. IEEE Communications Surveys & Tutorials.

4. Ring, M., Wunderlich, S., Grüdl, D., Landes, D., & Hotho, A. (2019). Flow-based network traffic generation using generative adversarial networks. Computers & Security.

5. Zhang, Y., et al. (2020). Federated learning for Internet of Things: A survey. IEEE Internet of Things Journal.