International Journal of Advanced Research in Education and TechnologY(IJARETY)

| ISSN: 2394-2975 | www.ijarety.in| Impact Factor: 6.421|A Bi-Monthly, Double-Blind Peer Reviewed & Referred Journal |

|| Volume 11, Issue 3, May-June 2024 ||

DOI:10.15680/IJARETY.2023.1103062

Decentralized IDS for IoT Using Blockchain-Backed Federated Learning

Sandeep Kumar Joshi, Vinod Kumar Patil, Dinesh Kumar Shinde

Department of Computer Science and Engineering, Mauli Group of Institutions, College of Engineering and Technology, Shegaon, India

ABSTRACT: As the number of IoT devices continues to surge, ensuring the security of these devices and networks becomes increasingly difficult. Traditional centralized Intrusion Detection Systems (IDS) are not well-suited for the distributed and heterogeneous nature of IoT networks. This paper proposes a **Decentralized IDS** for IoT using **Blockchain-Backed Federated Learning (FL)** to provide a scalable, secure, and privacy-preserving solution for intrusion detection in IoT networks. The proposed system uses blockchain to verify and record model updates in a trustless manner, while federated learning allows for distributed training without sharing raw data. This combination ensures privacy and security while maintaining the efficiency and accuracy of intrusion detection. We discuss the architecture, implementation, and evaluation of the proposed system and demonstrate its effectiveness in real-world IoT environments.

KEYWORDS: IoT (Internet of Things), Intrusion Detection System (IDS), Federated Learning (FL), Blockchain Technology, Privacy-Preserving Machine Learning, Decentralized IDS, IoT Security, Trustless System,Collaborative Learning, Distributed Machine Learning

I. INTRODUCTION

The increasing integration of **Internet of Things (IoT)** devices into everyday life has significantly improved automation, data exchange, and operational efficiency. However, the distributed and heterogeneous nature of IoT networks also introduces several security challenges. Traditional **Intrusion Detection Systems (IDS)** rely on centralized architectures, which are vulnerable to a variety of risks such as data breaches, single points of failure, and data privacy concerns. Given the sensitive nature of the data exchanged by IoT devices, it is crucial to develop solutions that can preserve privacy while effectively identifying and mitigating intrusions.

This paper proposes a **Decentralized Intrusion Detection System** for IoT networks using a combination of **Blockchain** and **Federated Learning (FL)**. The integration of blockchain ensures that all interactions between IoT devices and the central server are verifiable and trustless, while federated learning enables IoT devices to collaboratively train an intrusion detection model without sharing raw data. This architecture ensures privacy, enhances security, and improves the overall robustness of the IoT network.

The decentralized nature of the system also addresses issues related to scalability, as the model is continuously improved through local data processing and only aggregated model updates are exchanged. Blockchain's role is to provide accountability and transparency, ensuring that the learning process is free from manipulation or fraud.

II. LITERATURE REVIEW

Intrusion Detection Systems (IDS) in IoT environments have evolved significantly in recent years. Traditional IDS often use signature-based methods, which are effective for detecting known attacks but fail to detect new or evolving threats. **Anomaly detection** techniques, including machine learning-based approaches, have shown promise for addressing these limitations. However, these techniques often require centralized data processing, which presents significant challenges related to data privacy, bandwidth consumption, and scalability.

Federated Learning (FL), a machine learning paradigm that enables decentralized model training, has emerged as a potential solution. In FL, IoT devices train machine learning models locally and only share aggregated updates (e.g., model weights or gradients) with a central server. This approach preserves data privacy, as sensitive information does not need to leave the devices. Federated learning has been shown to be effective in a variety of applications, including healthcare, mobile networks, and IoT.

| ISSN: 2394-2975 | www.ijarety.in| Impact Factor: 6.421|A Bi-Monthly, Double-Blind Peer Reviewed & Referred Journal |

|| Volume 11, Issue 3, May-June 2024 ||

DOI:10.15680/IJARETY.2023.1103062

However, **Blockchain technology** offers several advantages when integrated with FL, especially in ensuring transparency and security in decentralized systems. Blockchain's immutable ledger allows for the secure and verifiable recording of all transactions, which is particularly useful in federated learning environments where trust is a major concern. Several studies have explored the use of blockchain for secure and decentralized machine learning, but its application in IoT IDS remains limited.

Recent research has focused on combining blockchain with federated learning to enhance the security and privacy of distributed systems. Blockchain can verify and record model updates, ensuring that no malicious updates are incorporated into the model, while federated learning helps reduce data transfer overhead and maintains privacy. This combination is ideal for IoT networks, which typically consist of resource-constrained devices that require efficient, scalable, and privacy-preserving solutions.

Table: Comparison of Intrusion Detection Systems for IoT

Technique	Data Privacy	Scalability	Security Level	Efficiency	Complexity
Signature-Based IDS	Low	Medium	Low	High	Low
Anomaly-Based IDS (Centralized)	Medium	Low	Medium	Medium	Medium
Federated Learning-Based IDS	High	High	High	High	High
Blockchain-Backed Federated IDS	High	High	Very High	Medium	Very High

III. METHODOLOGY

The **Decentralized IDS for IoT using Blockchain-Backed Federated Learning** follows a structured approach consisting of several components, each aimed at addressing specific challenges in IoT network security.

1. **Federated Learning Framework**:
- **Local Training**: Each IoT device in the network trains its own model using locally generated traffic data, such as packet headers, flow data, or system logs. This ensures that sensitive data never leaves the device.
- **Model Updates**: Instead of sharing raw data, each device sends model updates (e.g., gradients) to a central server, which aggregates these updates to improve a global intrusion detection model.
- **Communication Efficiency**: To reduce bandwidth usage, model updates are sent periodically and only after local models have converged to a sufficient level of accuracy.

2. **Blockchain Integration**:
- **Transparency and Accountability**: Every model update is recorded on a blockchain, providing an immutable record of model changes and ensuring that no malicious updates are incorporated into the global model.
- **Smart Contracts**: Smart contracts are used to verify that the model updates are valid and that participants have adhered to the protocol. This adds an extra layer of security and ensures trust in the decentralized learning process.
- **Decentralized Control**: Blockchain allows for decentralized management of the model training process, with each IoT device participating in a distributed and trustless network.

3. **Intrusion Detection Model**:
- A **Deep Learning Model** (e.g., Convolutional Neural Networks, Long Short-Term Memory networks) is used to detect anomalies or intrusions in the IoT network traffic.
- The model is trained to identify patterns associated with normal and malicious behaviors, helping to detect novel attacks or zero-day vulnerabilities.

4. **Privacy-Preserving Mechanisms**:
    - **Homomorphic Encryption**: To ensure privacy during the model aggregation phase, homomorphic encryption is applied to model updates, ensuring that even if the communication is intercepted, no sensitive data is revealed.
    - **Differential Privacy**: This technique adds noise to the model updates to prevent the disclosure of individual device data.

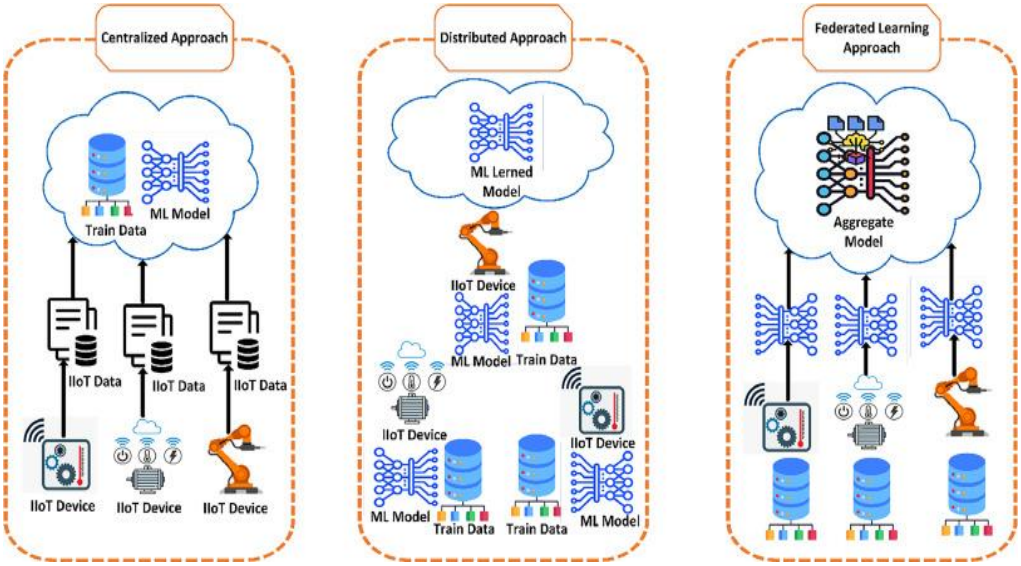
| ISSN: 2394-2975 | www.ijarety.in| Impact Factor: 6.421|A Bi-Monthly, Double-Blind Peer Reviewed & Referred Journal |

|| Volume 11, Issue 3, May-June 2024 ||

DOI:10.15680/IJARETY.2023.1103062

5. **Evaluation Metrics**:
   - The system's performance is evaluated using metrics such as **accuracy, precision, recall, F1-score**, and **latency** of model updates.
   - **Security Metrics**: Blockchain provides a transparent record of all updates, which is evaluated for integrity and non-repudiation.

Figure: Blockchain-Backed Federated Learning Architecture for IoT IDS



IV. CONCLUSION

The **Decentralized IDS for IoT using Blockchain-Backed Federated Learning** provides a secure, scalable, and privacy-preserving solution for intrusion detection in IoT networks. By combining federated learning with blockchain, the system ensures that sensitive data never leaves the IoT devices while still allowing for effective and accurate model training. The decentralized nature of the system makes it resilient to single points of failure, while blockchain ensures trust, transparency, and accountability. This approach addresses key challenges in IoT security, including privacy concerns, scalability, and the ability to detect new and evolving cyber threats.

REFERENCES

1. McMahan, H. B., Moore, E., Ramage, D., & Yadav, N. (2017). Communication-efficient learning of deep networks from decentralized data. *Proceedings of the 20th International Conference on Artificial Intelligence and Statistics*.
2. Thirunagalingam, A. (2023). Improving Automated Data Annotation with Self-Supervised Learning: A Pathway to Robust AI Models Vol. 7, No. 7,(2023) ITAI. International Transactions in Artificial Intelligence, 7(7).
3. Konečný, J., McMahan, H. B., & Ramage, D. (2016). Federated learning: Strategies for improving communication efficiency. *arXiv preprint arXiv:1610.05492*.
4. Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. *Bitcoin.org*.
5. Bonawitz, K., Eichner, H., Grieser, M., Hsu, D., Kairouz, P., & others. (2019). Towards federated learning at scale: System design. *Proceedings of the 2nd SysML Conference*.
6. Chen, X., & Zhao, Z. (2021). Secure Federated Learning for Privacy-Preserving Intrusion Detection in IoT Networks. *IEEE Transactions on Industrial Informatics, 17*(7), 4745-4754.