ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25aug074

Federated Learning Based Privacy Preservation Intrusion Detection Using Blockchain Technology

Geetanjali Rokade[1]; Ruturaj Hendre[2]; Vaishnavi Deshmukh[3]; Sejal Wavhal[4]; Deepika Ajalkar[5]

[1]Professor, Department of Cyber Security and Data Science
G H Raisoni College of Engineering and Management Pune, India
[2]Department of Cyber Security G H Raisoni College of Engineering and Management Pune, India
[3]Department of Cyber Security G H Raisoni College of Engineering and Management Pune, India
[4]Department of Cyber Security G H Raisoni College of Engineering and Management Pune, India
[5]Department of Cyber Security and Data Science
G H Raisoni College of Engineering and Management Pune, India

Publication Date: 2025/09/13

Abstract: Integration of Federated Learning (FL) with Blockchain technology to decentralized privacy-preserving, and scalable framework for strengthening cybersecurity. As cyber threats like ransomware, malware, and network intrusions grow in complexity, there is an increasing need for collaborative threat detection and mitigation. However, traditional collaborative approaches often involve sharing sensitive information across organizations, raising significant privacy concerns and regulatory challenges under frameworks like GDPR and HIPAA. FL works to solve these problems through enabling multiple entities to work together on training machine learning models without sharing their original information. Despite its advantages, FL faces challenges such as the risk of model tampering, trust deficits between participants, and dependence on a centralized server for model aggregation. To overcome these limitations the Blockchain technologies will be in used so blockchain technology provides a distributed, transparent, and non-mutable ledger that safely manages FL operations. It helps preserve the accuracy and trustworthiness of model updates via smart contracts along with consensus mechanisms, bypassing the requirement fora central aggregator. In addition, blockchain enables incentivization by introducing token-based rewards, encouraging active participation in collaborative threat detection networks. Privacy- preserving techniques to boost information security, techniques like differential privacy and homomorphic encryption are also put into practice. Such a integration of FL and blockchain is particularly impactful in securing distributed systems such as IoT devices, critical infrastructure, and enterprise networks, where privacy, trust, and scalability are crucial. This project aims to demonstrate the practical implementation of this framework, paving the way for adaptive and globally scalable cyber security systems to combat evolving threats.

Keywords: *Federated Learning, Blockchain, Cybers Security, IDS, Smart Contracts.*

How to Cite: Geetanjali Rokade; Ruturaj Hendre; Vaishnavi Deshmukh; Sejal Wavhal; Deepika Ajalkar (2025) Federated Learning Based Privacy Preservation Intrusion Detection Using Blockchain Technology. *International Journal of Innovative Science and Research Technology*, 10(8), 2954-2963.
https://doi.org/10.38124/ijisrt/25aug074

I. INTRODUCTION

As digital technologies advance, the need to protect information and privacy has reached new heights, especially in intrusion detection systems (IDS). Traditional centralized intrusion detection mechanisms face challenges such as privacy breaches, one points of Disruption, and high computational overhead. In order to resolve these concerns, this project integrates Federated Learning (FL) and Blockchain Technology to develop a privacy-preserving and decentralized intrusion detection system. Federated Learning allows multiple dis- tributed end users (edge devices) to jointly train an IDS model while maintaining the privacy of raw information, thereby protecting information confidentiality. Meanwhile, Blockchain technology enhances security by ensuring tamper-proof, im-mutable storage of model updates, preventing adversarial attacks and ensuring transparency. This project focuses on leveraging Federated Learning FL and Blockchain Technology to build a strong, privacy-focused, and secure cyber security framework. Federated Learning allows collaborative training of machine learning models across different devices or organizations while keeping raw information private. ensuring that sensitive information remains secure. However,

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25aug074

traditional FL systems face challenges such as lack of trust among participants, risks of malicious updates, and secure aggregation of model contributions. So, in this project the blockchain technology is used to address this issue as Blockchain Technology has distributed, decentralized and tamper-proof (Immutable) ledger. Blockchain records and validates model updates from participating devices, ensuring their authenticity and integrity.

II. LITERATURE SURVEY

Recent research on federated learning-based intrusion detection systems combined with blockchain technology has made significant strides in enhancing cybersecurity while preserving privacy. This survey explores how decentralized learning, secure model aggregation, and blockchain-powered threat intelligence can strengthen intrusion detection without exposing sensitive information. Studies in this field focus on various approaches, including federated learning frameworks that allow multiple devices to train models collaboratively, blockchain consensus mechanisms that ensure trust and transparency, and cryptographic techniques that safeguard information privacy. These innovations help address key challenges such as establishing trust among distributed participants, pre- venting malicious model updates, securely aggregating information contributions, and complying with privacy regulations. Additionally, researchers highlight the role of smart contracts in automating security policies and improving the reliability of IDS solutions across IoT, cloud, and enterprise environments. The methodologies used in these studies range from real- world experiments and case studies to analytical modeling, all aimed at optimizing intrusion detection accuracy and system efficiency. This growing body of research underscores the potential of federated learning and blockchain to create a more secure and resilient cybersecurity landscape. By eliminating the risks of centralized information storage while enabling real-time threat detection, these technologies deliver a flexible, transparent, along with a privacy-focused approach to modern cyber threats.

III. PROPOSED SYSTEM

This project proposes a secure and decentralized intrusion detection framework that prioritizes both privacy and transparency by integrating Federated Learning (FL) with Blockchain technology. Unlike traditional centralized approaches, the system allows several clients to enable cooperative model development using data Associated with them, without exposing it—thereby addressing key privacy concerns.

A. System Components:

➢ *User Interface (Flask GUI):*

A user-friendly web interface built with Flask allows dynamic uploading of datasets, launching of training sessions, and real-time visualization of model performance.

➢ *Federated Learning Clients:*

The system runs three independent client nodes. Each client:

- Is assigned a unique dataset.
- Handles local data preprocessing.
- Trains its own machine learning model.

➢ *Blockchain Module:*

A lightweight blockchain, custom-developed in Python, maintains hashes of each client's model updates. This ensures:

- Secure and immutable record-keeping.
- Prevention of unauthorized modifications.
- Validation of updates before aggregation.

➢ *Federated Aggregator Server:*

This central component receives verified model updates via the blockchain, performs the Federated Averaging (FedAvg) algorithm, and generates a unified global model.

➢ *Evaluation Module:*

The aggregated global model is assessed based on metrics such as accuracy and precision. Results are then displayed on the user interface for clear interpretation.

By integrating FL and blockchain, this system not only pre- serves user data confidentiality but also ensures the trust- worthiness of model updates. It is particularly well-suited for cybersecurity applications, where both data integrity and privacy are essential.

IV. METHODOLOGY

This methodology integrates the capabilities of faderated- Learning (FL) & Blockchain-Technology to design cyberse- curity framework that prioritizes both decentralization and privacy. The core concept is to enable multiple systems or users to work together in identifying cyber threats—without the need to exchange their raw data. This collaborative yet privacy-conscious approach helps keep sensitive information secure while also protecting the reliability and trustworthiness of the trained models. The following section outlines the process in detail.

A. Data Upload and Preprocessing

The workflow starts with users uploading their datasets through a web interface developed using Flask. This interface is designed to accept three separate datasets, which are then in- dividually processed and assigned to three distinct client nodes for training. Before the data is used for model development, it goes through a preprocessing stage to ensure it's clean and ready for learning.

➢ *The Preprocessing Steps Involve:*

- Cleaning: Eliminating incomplete, inconsistent, or irrelevant records from the data.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25aug074

- Normalization: Adjusting numerical values to a standardized range to support effective model training.
- Encoding: Transforming qualitative data into quantitative format using methods like One Hot Encoding.
- Feature Selection: Identifying and keeping just the important attributes to enhance model precision and reduce training complexity.

Once these steps are complete, each dataset is delivered to a specific client—Client 1, Client 2, or Client 3—where it is used for local model training, independently of the others.

B. Client-Side Training with Federated Learning

After preprocessing is complete, each client proceeds to train its own machine learning model using Federated Learn- ing. Instead of transferring raw data to a central system, each client keeps the data local and focuses on building a model based on its own dataset. Only the essential training results—such as model weights or gradients—are shared, helping to maintain data confidentiality.

- Clients can use various algorithms, like Multi-Layer Perceptrons or Convolutional Neural Networks.
- Once training is done, clients share only the model updates—not the data—ensuring privacy.
- These updates are transmitted to a central server via Blockchain for further processing.

Table 1 Literature Survey

Sr No.	Published Year [Reference]	Research Paper Name	Description
1	(2024) [1]	Federated-Learning Intrusion Detection System Based Blockchain Technology. By Ahmed Almaghthawi, Ebrahim A. A. Ghaleb , Nur Arifin Akbar.	This research introduces the development of an intrusion detection system based on blockchain and federated learning. Unlike conventional signature-based approaches, this method leverages machine learning (ML) to identify novel attack patterns. The federated learning technique maintains the privacy of sensitive information while making use of the extensive data distributed across client devices.
2	(2024) [2]	Blockchain and Federated Learning-bas- ed Intrusion Detection Approaches for Edge-enabled Industrial IoT Networks By Saqib Ali, Qianmu Li, Abdullah Yousafzai.	This paper looks at how combining federated learning and blockchain can help make Industrial IoT (IIoT) systems more secure. Since IIoT devices produce a lot of sensitive data, traditional security systems that rely on centralized machine learning aren't practical any more they 're too costly and raise privacy issues. Instead, federated learning keeps data on the devices, while still training models, and blockchain adds an extra layer of trust and security. The authors review current research, highlight what's working, suggest best practices, & point out area where more work is needed to better protect IIoT networks.
3	(2023) [3]	Enhancing Privacy-Preserving Intrusion Detection in Blockchain-Based Networks with Deep Learning. By JUNZHOU LI, QIANHUI SUN, FEIXIAN SUN.	This study focuses on solving the privacy challenges of sharing data in sensitive areas like a healthcare, where it's often hard to use machine learning because of strict data protection rule. The researchers propose a smart solution that blends federated learning, blockchain, and com- bination of Deep-Learning models (LSTM & GRU) to allow organizations to collaborate with- out exposing private data. Instead of sending raw data around, each participant trains models locally, and blockchain is used to securely share updates and reward contributors with tokens. This setup not only keeps data safe but also makes it easier for different parties to work together, achieving an impressive 99.01% accuracy in their tests.
4	(2024) [4]	BFLIDS: Blockchain-Driven Federated Learning for Intrusion Detection in IoMT Networks By Khadija Begum, Md Ariful Islam Mozumder, Moon-Il Joo.	This study introduces BFLIDS, a smart security system for medical IoT devices that protect patient data while detecting cyber threats. Rather than transmitting data to a centralized server, it uses (FL) to train models directly on devices and blockchain to securely manage updates & transactions. With advanced deep learning models and decentralized storage, BFLIDS achieved up to 98.21% accuracy, offering a reliable and privacy-friendly way to safeguard connected healthcare networks.
5	(2022) [5]	Federated Learning-Based Privacy Preservation with Blockchain Assistance in IoT 5G Heterogeneous	This Study presents a privacy-preserving framework that combines Federated Learning and Blockchain to secure information in IoT and 5G networks. The model ensures that sensitive information remains on local devices while blockchain secures communication among distributed devices. This hybrid approach enhances information

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25aug074

		Net- works. By A. Sampathkumar , Shishir K, Nebojsa Bacanin.	confidentiality, scalability, and trust in heterogeneous environments.
6	(2024) [6]	Enhancing IDS through Decentralization : A Study on Federated Learning and Blockchain Integration By Tushar Mane, Shraddha Phansalkar, Ronit Virwani	This paper introduces a smart and privacy-focused way to detect cyber threats using a mix of federated learning and blockchain. With cyberattacks getting more advanced and data privacy becoming a bigger concern, traditional security systems just aren't enough. Instead of sending private data to a centralized server, this approach lets devices train models locally & share only the updates. Blockchain ensures that all updates are secure and trustworthy. The goal is to build a system that can protect itself from threats while keeping personal data safe and private.
7	(2024) [7]	Federated-Learning Intrusion Detection System Based Blockchain Technology. By Ahmed Almaghthwi, Ebrahim A A Ghaleb.	This study presents a blockchain-powered, federated learning system for detecting cyber-attacks. Instead of relying on outdated methods that look for known attack patterns, this approach uses machine learning to identify new threats. It allows data to stay private by training the model across devices without sharing sensitive information. By combining federated learning with blockchain, the system creates a decentralized, secure way to tackle today's cyber-security challenges.
8	(2024) [8]	Survey on Federated Learning for Intrusion Detection System: Concept, Architectures, Aggregation Strategies, Challenges, and Future Directions. Bynsam Khraisat, Ammar Alazab, Sarabjot Singh.	This article looks at how Federated Learning (FL) can improve (IDS), which is crucial for, securing computer networks. Traditional IDS face issues with scalability, privacy, and heavy computational needs as network data becomes more complex. FL helps by allowing each participant to train models on their own data without sharing it keeping things private. The model updates are then sent to a central server, which combines them and shares the improved model back with everyone. The paper explores how FL can boost IDS performance, discussing its, strengths, challenges, and ways to improve privacy & security in the process.
9	(2025) [9]	Advanced artificial intelligence with fed-erated learning framework for privacy- preserving cyberthreat detection in IoT- assisted sustainable smart cities. By Mahmoud Ragab, Ehab Bahaudien Ashary, Bandar M. Alghamdi.	This study presents a new approach to Federated Learning (FL)-based AI Framework designed to, detect cyber threats in smart city IoT networks while preserving user privacy. It emphasizes the importance of decentralized model training to avoid exposing sensitive information, in sustainable urban environments. The framework combines edge intelligen with secure information aggregation and employs deep learning techniques to enhance threat detection accuracy. The study also discusses the performance benefits of FL in reducing communication overhead, and preserving energy, making it well-suited for smart city infrastructures.
10	(2024) [10]	Privacy-Preserving Federated Learning-Based Intrusion Detection Technique for Cyber-Physical Systems. By Syeda Aunanya Mahmud ,Nazmul Islam, Zahidul Islam.	This Study provides a FL strategy for IDS in Cyber Physical Systems that enhances information privacy & system security. Instead of sharing raw information, the system share only model updates, ensuring that sensitive information stays on local devices. It effectively detects cyber threats like DDoS,ransomware, and information injection attacks, while minimizing computational load and maintaining high detection accuracy.

C. Blockchain Integration for Model Trust

Blockchain is used in two crucial ways:

- *Model Authenticity: Every Update Received from a Client is Logged on a Simple Blockchain.*
- *This Log Contains:*

✓ The client's ID
✓ Timestamp of the update
✓ A cryptographic hash of the model's weights Tamper-Proof Records:

Using Blockchain ensures that these updates can't be altered or forged. This brings transparency and guarantees the authenticity of every model update.

D. Federated Model Aggregation

After collecting model updates from all clients, the

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25aug074

central server aggregates them using the Federated Averaging (Fe- dAvg) technique.

➢ *Here's how it Works:*

- It takes the average of all client-submitted weights.
- This creates a new global model that reflects the knowledge learned from all three clients.
- The unified model is then tested with a distinct testing dataset.

E. Model Evaluation and Metrics

To assess how well the global model performs, two core performance evaluation measures:

- Accuracy: The ratio of correctly predicted outcomes to the total number of predictions made.
- Precision: Precision measures how many of the predicted positive results were actually correct, which helps under- stand the quality of positive predictions.

These metrics are displayed on a results page for user review.

F. Visualizing Results

For better clarity and usability, the accuracy and precision results are presented in a visually digestible format. This helps users quickly assess how effective the global model is in detecting threats across distributed nodes.

G. Security and Privacy Features

The system is built with strong security principles in mind:

- Data Privacy: Clients never share their raw data; training stays local.
- Model Integrity: All updates are verified and stored securely via Blockchain.
- Decentralization: The system avoids a single point of failure by distributing responsibilities, enhancing trust and resilience.

V. GOALS AND OBJECTIVE

This project, "Federated Learning-Based Privacy Preservation and Intrusion Detection Using Blockchain Technology," aims to create a secure, decentralized, and privacy-focused intrusion detection system. By combining Federated Learning (FL) and Blockchain Technology, the system allows multiple entities to work together to detect cyber threats without sharing sensitive information. This ensures information confidentiality, secure model aggregation, and real-time threat intelligence sharing, all while maintaining compliance with privacy regulations like GDPR and HIPAA. The goal is to strengthen cybersecurity without compromising user privacy, making net- works more resilient and trustworthy against evolving threats. resilient and trustworthy against evolving threats.

➢ *Building a Smarter and More Private Intrusion Detection System:*

Our goal is to design a (FL) framework that enables multiple client devices to share knowledge to machine learning models while keeping original information lo- cal. This method helps protect sensitive information and maintains information privacy, still enabling a powerful, collaborative defense against cyber threats. By keeping information on local devices, we enhance threat detection while maintaining strict confidentiality, making cyber security both effective and privacy-friendly.

➢ *Using Blockchain for Secure and Trustworthy Model Updates:*

To ensure security and integrity, we integrate blockchain technology for securely logging and validating model up- dates. Blockchain's decentralized ledger guarantees that all contributions are tamper-proof and transparent, pre- venting unauthorized modifications or adversarial attacks. This approach builds trust among participants, ensuring that only genuine, high-quality updates are incorporated into the intrusion detection system.

➢ *Enhancing Security with Smart Contracts:*

To make the system more secure and efficient, we use smart contracts to automate security enforcement. These contracts automatically verify and integrate only legitimate model updates, ensuring that the system re- mains trustworthy and resistant to malicious changes. By eliminating the need for manual verification, this approach streamlines collaboration, builds trust among participants, and enhances the overall efficiency of the intrusion detection process.

➢ *Strengthening Intrusion Detection with Real-Time Threat Analysis:*

We aim to build an intelligent intrusion detection system (IDS) that can quickly identify new and evolving cyber threats across IoT, cloud, and enterprise environments. By leveraging advanced analytics, the system will detect threats in real time, enabling faster responses to security. risks before they cause harm. This proactive approach ensures stronger protection against cyberattacks, keeping networks and devices secure and resilient.

➢ *Evaluating Performance, Scalability, and Compliance:*

To ensure the system is effective in real-world scenarios, we will test and validate it using real-world information sets, measuring its accuracy, efficiency, and ability to scale across different environments. Additionally, the system will be designed to meet global information protection standards like GDPR and HIPAA, ensuring that user privacy and regulatory compliance remain a top priority.

VI. SCOPE

This research aims to build a privacy-focused and de- centralized Intrusion Detection System (IDS) by integrating Federated Learning (FL) and Blockchain Technology. The goal is to strengthen cybersecurity by enabling organizations

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25aug074

to collaborate on threat detection without compromising sensitive information. By using FL for distributed learning and blockchain for secure model updates, this system enhances threat intelligence sharing while eliminating the single points of failure that often weaken traditional IDS solutions.

- The system will feature a modular design, ensuring seamless interaction between its various components. It will include a user-friendly interface that allows individuals, researchers, and government agencies to monitor air pollution levels in real time. The development process will focus on integrating IoT-based sensors, cloud storage, and information analytics to provide meaningful insights.
- Privacy-Preserving Intrusion Detection: Enable the collaborative training of IDS models while keeping raw in- formation private. Leverage Federated Learning to ensure information remains secure and confidential throughout the process.
- Automated Security Enforcement: Use smart contracts to automatically verify and integrate only legitimate model updates. Build trust and transparency by ensuring every contribution follows strict security protocols.
- Scalability and Real-Time Threat Detection: Develop a flexible system that seamlessly adapts to IoT, cloud, and enterprise environments. Ensure fast and effective threat detection, allowing immediate response to emerging cyber risks.
- Regulatory Compliance and Incentivization: Ensure the system aligns with privacy regulations like GDPR and HIPAA, protecting sensitive information.

VII. SYSTEM ARCHITECTURE

The architecture of our Federated Learning-Based Privacy- Preserving Intrusion Detection System Using Blockchain Technology, shown in Fig. 1, is built to provide secure and decentralized threat detection. It enables real-time analysis, fosters seamless collaboration, and ensures strong information privacy, all while leveraging blockchain to maintain trust and integrity.

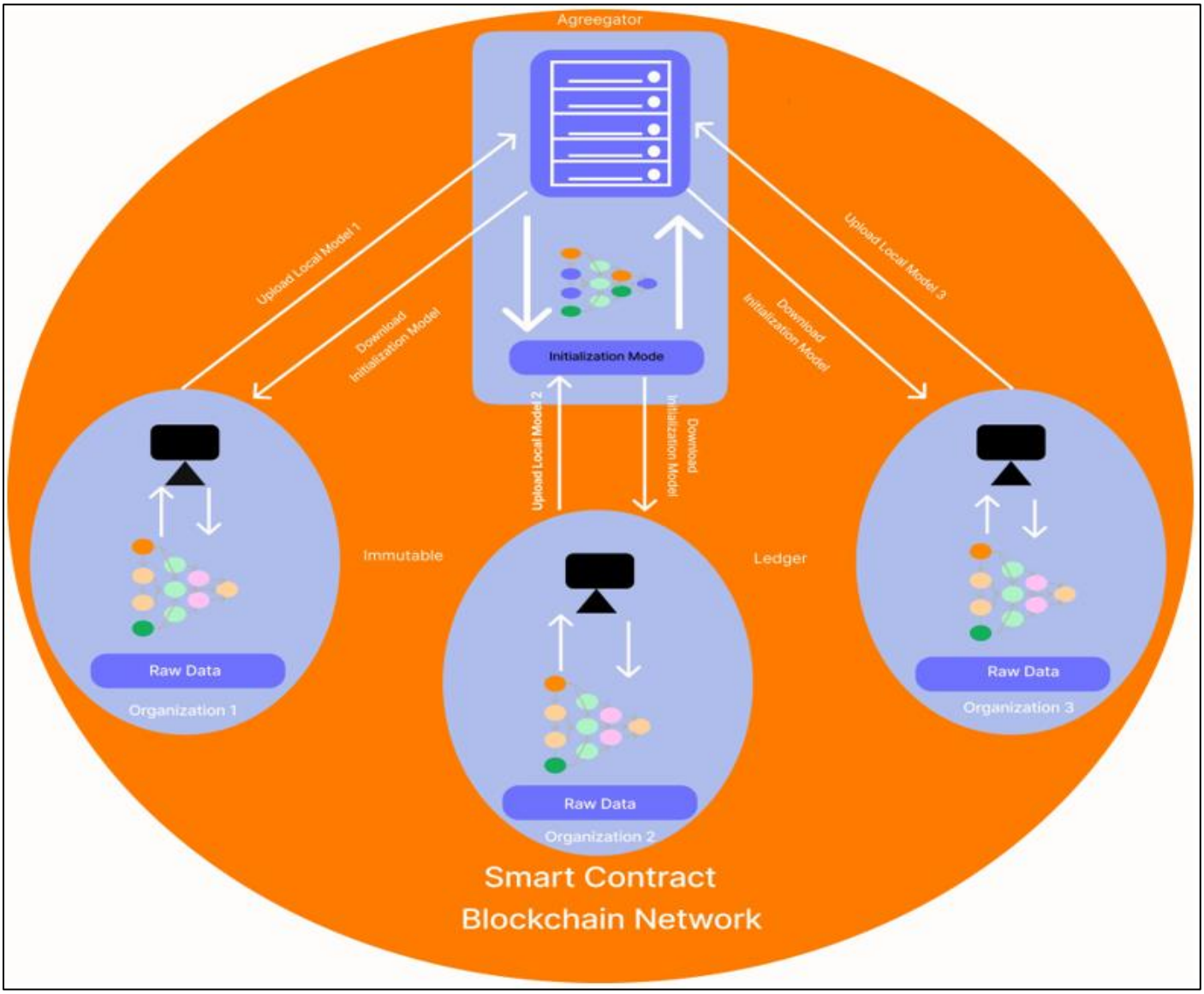

Fig 1 System Architecture

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25aug074

➢ *Client Nodes (3 Total):*

Three independent client nodes participate in the federated learning process. Each node is assigned a distinct dataset, which it uses to:

- Preprocess and prepare the data locally
- Train a local machine learning model
- Generate model updates (weights), without ever sharing raw data

➢ *Central Aggregator Server:*

The aggregator acts as the central coordination point in the federated learning setup. It receives the locally trained model weights from all client nodes.

- Validates the authenticity of updates using blockchain records.
- Applies the Federated Averaging (FedAvg) algorithm to merge the weights.
- Produces a refined global model that captures the collective intelligence of all clients.

➢ *Flask-Based Web Interface:*

A lightweight web interface built using Flask enables smooth and simple user interaction with the system. It allows users to:

- Upload datasets dynamically.
- Initiate federated training sessions.
- Monitor training status and control workflow from a centralized dashboard.

➢ *Result Dashboard:*

The system includes a built-in visualization module that offers clear and interactive feedback on the effectiveness of the global model. evaluation measures like accuracy, precision, & loss are displayed graphically, making it easier for users to evaluate model effectiveness over time.

VIII. FEATURES

The proposed system brings together Federated Learning (FL) and Blockchain Technology to build a secure, decentralized, and privacy-conscious Intrusion Detection System (IDS). This approach aims to address the limitations of centralized IDS models, especially in environments where information privacy and system trust are critical.

➢ *Information Privacy by Design*

Our system ensures that raw information never leaves the local environment. Instead, each end user trains its own model locally using federated learning. Only the model updates—not the information—are shared, which helps maintain user and organizational privacy.

➢ *Blockchain for Trust and Integrity*

To verify and record model updates securely, we use a blockchain ledger. This ensures that every contribution to the global model is tamper-proof, traceable, and added in a transparent manner—removing the need for a central authority.

➢ *Smart Contracts for Secure Collaboration*

Smart contracts are used to automate and enforce rules across the system, such as validating model contributions or controlling access. This prevents malicious participants from submitting false updates or tampering with the training process.

➢ *Scalable and Robust Architecture*

The federated approach allows the system to grow easily as more end users join. Even if some end users drop out or behave unpredictably, the system can continue functioning smoothly, making it highly reliable.

➢ *Efficient Anomaly Detection*

Each end user can detect intrusions in real-time using lightweight, locally trained models. These models are tailored to the end user's environment and are capable of identifying both known and previously unseen threats.

➢ *Secured Communication and Aggregation*

We apply secure communication techniques and, optionally, differential privacy to protect model parameters during trans- mission. Blockchain ensures that all updates are received in order and haven't been altered.

➢ *Designed for Modern Critical Systems*

This architecture is especially beneficial for sectors like smart cities, industrial IoT, and healthcare, where sharing raw information is often restricted, but collaboration is essential for strong security.

➢ *Built-in Transparency and Auditability*

Every action—whether a model update, detection event, or policy change—is recorded on the blockchain. This creates a reliable audit trail that supports incident investigation and compliance with information protection laws.

IX. RELEVANT MATHEMATICS ASSOCIATED

In this section, we break down the core mathematical concepts that make our system work effectively. By combining federated learning, intrusion detection, and blockchain technology, our approach focuses on building a secure and privacy- respecting environment. These mathematical foundations not only guide how information is processed and shared but also essential in maintaining the system's accuracy, integrity, and reliability of entire system.

A. Mathematical Models and Formulas Used

➢ *Relevant Mathematics Associated:*

This section high- lights the essential mathematical principles that underpin our system, ensuring it operates securely, efficiently, and privately in a decentralized environment.

- *Federated Averaging for Global Model Aggregation:*

Federated Learning allows each end user to train its

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25aug074

own localized model using private information. The unified model is then formed by combining these localized models through weighted averaging.

Where:

$$w_{t+1} = \sum_{i=1}^{K} \frac{n_i}{N} w_i^t \quad (1)$$

- ✓ w_i^t is localized model of end user i at time t,
- ✓ n_i is the quantity of information samples from end user i,
- ✓ $N = \sum_{i=1}^{K} n_i$ is the total count of information points,
- ✓ K is the total number participating end users.

This approach guarantees that end users information sets of greater size have a more significant effect on the global model.

- *Loss Function for Intrusion Detection:*

To classify network activity as malicious or benign, we use the Binary Cross-Entropy Loss Function:

$$L(y, \hat{y}) = -[y \log(\hat{y}) + (1 - y) \log(1 - \hat{y})] \quad (2)$$

Where:

- ✓ y represents the actual label (0 for normal, 1 for threat),
- ✓ $\hat{y}$ represents the predicted likelihood

Optimization algorithms like SGD or Adam minimize this loss during training.

- *Differential Privacy for end user Security (Optional):*

To improve information privacy, represents noise following a Gaussian distribution can be added to gradients:

$$\tilde{g} = g + N(0, \sigma^2) \quad (3)$$

Here, g is the gradient vector & $N(0, \sigma^2)$ represents represents noise following a Gaussian distribution with zero mean and variance σ^2.

- *Blockchain Hashing for Integrity:*

To guarantee tamper-proof updates, cryptographic hash functions like SHA- 256 are used:

$$H(x) = \text{SHA-256}(x) \quad (4)$$

Each model update is recorded on a blockchain block, creating a verifiable and immutable audit trail.

- *Consensus Algorithm for Model Validation:*

A Practical Byzantine Fault Tolerance (PBFT) mechanism ensures only verified model updates are added:

$$n \geq 3f + 1 \quad (5)$$

Where:

- ✓ n represents the total count of devices
- ✓ f represents maximum count of faulty or malicious devices the network can tolerate.

- *Model Evaluation Metrics:*

To assess detection performance, we use standard classification metrics:

$$\textbf{Accuracy:} \frac{TP + TN}{TP + TN + FP + FN}$$

$$\textbf{Precision:} \frac{TP}{TP + FP}$$

$$\textbf{Recall:} \frac{TP}{TP + FN}$$

$$\textbf{F1-Score:} \frac{2 \cdot \text{Precision} \cdot \text{Recall}}{\text{Precision} + \text{Recall}}$$

Here:

- ✓ TP = True Positives,
- ✓ TN = True Negatives,
- ✓ FP = False Positives,
- ✓ FN = False Negatives.

These functionality indicators help us evaluate how effectively our system identifies and blocks threats while minimizing false alarms.

X. ADVANTAGES

Our system, which brings together Federated Learning and Blockchain technology for intrusion detection and privacy protection, is designed to address modern cybersecurity challenges in a smarter, more secure, and decentralized way. Below are the key advantages that highlight the strength of this approach.

➢ *Solid Information Privacy Enforcement*

Among several most important advantages of our system is ensuring sensitive data stays within the local devices or endpoints. Rather than sending unprocessed information to a centralized server, each participant performs local model training and sends only secure, encrypted updates. This significantly reduces the risk of information exposure and aligns with the growing need to protect user privacy. This also supports organizations in meeting information protection requirements such as GDPR and HIPAA, by keeping personal or confidential information on-premise.

➢ *Decentralized and Resilient Learning Architecture*

By distributing the learning process across multiple devices or systems, Federated Learning removes the dependency on a single centralized server. This

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25aug074

decentralized structure makes the overall system more resilient against failures and cyber- attacks targeting central points. It also makes the system more scalable, allowing it to perform efficiently in large networks with many connected devices—perfect for modern environments like smart cities, IoT ecosystems, and enterprise networks.

- *Secure and Transparent Activity Logging*

Blockchain plays a key role in maintaining a secure and verifiable record of every action in the system—whether it's a model update, a decision made by the intrusion detection system, or a security alert. Since blockchain records are tamper-proof and time-stamped, they serve as a trustworthy log that can be audited at any time. This builds a layer of transparency and accountability into cybersecurity operations.

- *Real-Time Threat Adaptation*

Because the model is continuously updated with new in- sights from multiple distributed devices, the system can learn and respond to new types of cyber threats much faster than traditional centralized intrusion detection systems. This adapt- ability is critical in today's dynamic threat landscape, where attack patterns evolve rapidly.

- *Defense Against Adversarial Attacks*

Combining blockchain's cryptographic principles with Federated Learning enhances the overall robustness of the system. Consensus algorithms help validate every transaction or up- date, making it harder for attackers to inject malicious information or alter the learning process. This significantly strengthens the system's capability to identify and resist adversarial threats, information tampering, and misinformation.

- *Enhanced Transparency and user Trust*

Blockchain's inherent transparency ensures that all system activities are visible and verifiable. Every update, transaction, or decision made by the system can be traced and confirmed, which helps build trust among users, administrators, and auditors. This is especially crucial in industries like finance, healthcare, as well as defense, where industries where trust and accountability matter most.

XI. DISADVANTAGES

While our proposed system offers significant benefits by integrating Federated Learning and Blockchain offers secure and privacy-enhancing intrusion detection, but it also comes with certain challenges and limitations that must be thoughtfully addressed. These disadvantages reflect real-world implementation concerns and highlight areas for further research and optimization.

- *High Computational Overhead*

Federated learning requires each participant device to locally train machine learning models. For resource-constrained devices like IoT sensors or mobile phones, this can lead to performance bottlenecks due to limited CPU power, memory, or battery life. Additionally, the blockchain component intro- duces cryptographic operations that may further strain device capabilities.

- *Increased Communication Cost*

Since model updates are exchanged frequently between end users and the central aggregator (or smart contract-based systems), the system generates a substantial amount of communication traffic. In large-scale networks, especially with intermittent or low-bandwidth connections, this can become a significant challenge affecting performance and scalability.

- *Latency in Consensus Mechanisms*

Blockchain's consensus protocols (such as PBFT or Proof- of-Authority) ensure trust and security but often introduce latency due to the time required for validation and agreement among devices. This can delay the recording of updates or decisions, which is problematic in scenarios where real-time intrusion detection is crucial.

- *Storage Overhead on Blockchain*

Over time, the blockchain ledger can become very large, as it stores every model update, transaction, or event log. This increases the storage burden on participating devices, especially those with limited capacity. Managing blockchain size and ensuring efficient access to relevant information can become challenging as the system scales.

XII. CONCLUSION

We introduced a fresh approach in this study that brings together Federated Learning and Blockchain to create a secure, decentralized, and privacy-aware intrusion detection system. By enabling models to train directly on local devices and recording system activities on a tamper-proof blockchain, our solution tackles some of the biggest challenges in today's cybersecurity landscape especially around information privacy, trust, and scalability.

Unlike traditional systems that rely on central information collection, our framework protects sensitive information while improving transparency and resistance to attacks. Although there are still hurdles to address, such as the extra computational load and communication delays, the advantages—like real-time adaptability, legal compliance, and decentralized control—make it a strong fit for modern environments like IoT ecosystems, corporate networks, and smart cities.

Overall, this research sets the groundwork for future advancements in building intelligent, privacy-preserving cyber- security systems that can meet the demands of an increasingly connected world.

REFERENCES

[1]. Federated-Learning Intrusion Detection System Based on Blockchain Technology. (2024) Vol. 20 No. 11. By Ahmed Almaghthawi, Ebrahim A. A. Ghaleb, Nur Arifin Akbar. https://doi.org/10.3991/ijoe.v20i11.49949

[2]. Blockchain and Federated Learning-based Intrusion

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25aug074

Detection Approaches for Edge-enabled Industrial IoT Networks: a survey. (2024), Volume 152, 103320. By Saqib Ali, Qianmu Li, Abdullah Yousafzai. https://doi.org/10.1016/ j.adhoc.2023.103320

[3]. Enhancing Privacy-Preserving Intrusion Detection in Blockchain-Based Networks with Deep Learning. (2023) Volume 22, Page/Article: 31. By Junzhou Li, Qianhui Sun, Feixian Sun. https://datascience.codata. org/articles/10.5334/dsj-2023-031

[4]. BFLIDS: Blockchain-Driven Federated Learning for Intrusion Detection in IoMT Networks. Moon-Il Joo.Sensors (2024), 24(14), 4591. By Khadija Begum, Md Ariful Islam Mozumder, https://doi.org/10.3390/ s24144591

[5]. Federated Learning-Based Privacy Preservation with Blockchain Assis- tance in IoT 5G Heterogeneous Networks. (2022) Vol 21 Iss 4. By A. Sampathkumar, Shishir K, Nebojsa Bacanin. https://orcid.org/ 0000-0001-5318-5676

[6]. Enhancing IDS through Decentralization: A Study on Federated Learn- ing and Blockchain Integration. (2024) IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS) By Tushar Mane, Shraddha Phansalkar, Ronit Virwani. https:// ieeexplore.ieee.org/document/10837126

[7]. Federated-Learning Intrusion Detection System Based on Blockchain Technology. (2024) Vol. 20 No. 11. By Ahmed Almaghthawi, Ebrahim A. A. Ghaleb, Nur Arifin Akbar. https://doi.org/10.3991/ijoe.v20i11.49949

[8]. Survey on Federated Learning for Intrusion Detection System: Concept, Architectures, Aggregation Strategies, Challenges, and Future Directions. (2024) ACM Computing Surveys 57(1) By Nsam Khraisat, Ammar Alazab, Sarabjot Singh. http://dx.doi.org/10. 1145/3687124

[9]. Advanced Artificial Intelligence with Federated Learning Framework for Privacy-Preserving Cyberthreat Detection in IoT-Assisted Sustainable Smart Cities. (2025) Scientific Reports volume 15, Article number: 4470. By Mahmoud Ragab, Ehab Bahaudien Ashary, Bandar M. Alghamdi. https://www.nature.com/articles/s41598-025-88843-2

[10]. Privacy-Preserving Federated Learning-Based Intrusion Detection Tech- nique for Cyber-Physical Systems. (2024) E1: Mathematics and Com- puter Science 12(20), 3194. By Syeda Aunanya Mahmud, Nazmul Islam, Zahidul Islam. https://doi.org/10.3390/math12203194

[11]. A Novel Intrusion Detection Techniques of the Computer Networks Using Machine Learning. (2023) Vol. 11 No. 5s. By Mishra, Nilamadhab, and Sarojananda Mishra. https://www.ijisae. org/index.php/IJISAE/article/view/2772

[12]. Support vector machine used in network intrusion detection. (2018.) IOSR Journal of Engineering (IOSRJEN). By Mishra, Nilamadhab, and Sarojananda Mishra. https://www.academia.edu/128286614/ Support\Vector\Machine\Used\\\in\Network\Intrusion\ Detection