*International Journal on Recent and Innovation Trends in Computing and Communication*
***ISSN: 2321-8169 Volume: 11 Issue: 9***
***DOI: https://doi.org/10.17762/ijritcc.v11i9.8358***
***Article Received:** 15 July 2023 **Revised:** 08 September 2023 **Accepted:** 20 September 2023*

# A Federated Consensus for Proof of Authority in IoT-Blockchain Applications

**[1]R.Selvakumar, [2]S. Shibu, [3]R.Priscilla Joy, [4]Roopa Chandrika R, [5]C.Ramesh Kumar, [6]S.Kamatchi**
[1]Department of AIML,
Saveetha Engineering College,Thandalam, Sriperumbudur,Tamil Nadu, India,
sachein.pretty@gmail.com
[2]Department of Electronics and Communication Engineering,
Panimalar Engineering College, Chennai, Tamil Nadu, India
soman.shibu@gmail.com,
[3]Division of Computer Science and Engineering,
karunya institute of technology and sciences, Tamil Nadu, India
priscillajoy@karunya.edu,
[4]Department of Computer Science and Engineering,
Karpagam Academy of Higher Education, Coimbatore, Tamil Nadu
roopamurugan@gmail.com,
[5]Department of Electronics and Communication Engineering,
Panimalar Engineering College, Chennai, Tamil Nadu, India
rameshchand2006@gmail.com,
[6]Department of Electronics and Communication Engineering,
Saveetha School of Engineering, SIMATS,
Saveetha Nagar, Thandalam, Chennai, Tamil Nadu, India,
kamatchime@gmail.com

**Abstract**- The growing adoption of Internet of Things (IoT) devices and the need for secure and scalable blockchain applications pose significant challenges in the realm of consensus protocols. This paper proposes a novel consensus mechanism called Federated Consensus for Proof of Authority (Fed-PoA), which combines the advantages of Proof of Authority (PoA) and federated learning to achieve secure and scalable IoT-Blockchain applications. The Fed-PoA ensures efficient data sharing, privacy preservation, and decentralized operation. Performance evaluation of this model in a simulated environment demonstrates superior convergence and memory usage compared to a representative work in this context..

**Keywords**- IoT, consensus, PoA, federated learning, blockchain.

## I. INTRODUCTION

IoT networks make use of the fact that blockchain is a secure and decentralized technology in order to improve the functionality and security of IoT devices. The last two decades have seen a rise in interest in these applications, which have found applications in the fields of finance, logistics, and cybersecurity [1]. Conventional Proof of Work (PoW) and Proof of Stake (PoS) serve as well-known consensus procedures in blockchain networks; nevertheless, they confront issues relating to scalability, energy consumption, and centralization in their implementations. Researchers have proposed many alternative consensus protocols, such as Proof of Authority (PoA) [2] and federated consensus [3], as a means of overcoming the constraints that have been identified. The Proof of Authority protocol (PoA) utilizes a reliable set of validators who are responsible for verifying transactions and creating new blocks. This method is more streamlined and centralized than others. Federated Consensus, on the other hand, enables several users to take part in the validation process without compromising decentralization or security. These protocols provide feasible solutions that solve the disadvantages of both Proof of Work and Proof of Stake. As a result, they enable increased scalability, energy efficiency, and governance within blockchain networks.

In the context of PoA mechanisms, federated consensus can provide several significant advantages that help overcome limitations and enhance the overall functionality of IoT blockchain systems. It improves decentralization by involving multiple parties in the validation process, preventing excessive control and promoting fairness. Enhanced security is achieved through a distributed trust model, making it harder for malicious actors to manipulate the network. Better scalability is achieved by distributing the computational load among multiple validators, enabling efficient operations as the system handles a larger volume of transactions [4]. Additionally, federated consensus introduces enhanced governance, allowing multiple parties to participate in decision-making, ensuring inclusivity and collaboration in managing the IoT blockchain system [5]. Currently, existing PoA mechanisms lack the incorporation of federated consensus, which can limit their potential in certain aspects, resulting in reduced decentralization and limited diversity in the validation process.

Without federated consensus, PoA mechanisms rely on a fixed group of trusted validators to validate transactions and create blocks. While this approach ensures efficiency and security by minimizing the risk of malicious activity, it also introduces centralization concerns [6]. The power to validate transactions and make consensus decisions lies within a small group of validators, potentially leading to a concentration of control. This lack of decentralization can undermine the democratic and resilient nature of blockchain networks. Moreover, the absence of federated consensus restricts the participation of external parties in the validation process. In PoA systems, the validator set is typically predetermined, leaving little room for new entities to join and contribute to the network. The exclusion of external validators limits the diversity of perspectives and expertise, potentially hindering innovation and governance effectiveness. By integrating federated consensus into PoA mechanisms, these limitations can be mitigated.

In this research, Fed-PoA mechanism addresses the limitations of existing PoA mechanisms by incorporating a federated consensus approach, ensuring both security and scalability in IoT-blockchain applications as below.

1. By allowing a broader range of participants to contribute their expertise, Fed-PoA enhances the democratic nature of the consensus process and reduces the risks associated with centralization.
2. In terms of security, Fed-PoA employs a distributed trust model by requiring consensus from a predefined subset of validators within the federated group. Consensus decisions are made based on the collective agreement of these validators, making it more difficult for malicious actors to manipulate the network.
3. Regarding scalability, Fed-PoA leverages the federated model to distribute the validation workload among a larger number of validators. This distribution reduces the computational burden on individual validators and improves the overall scalability of the system.

## II. RELATED WORKS

This section describes the recent works in the context of PoA and federated consensus. To further enhance the PoA protocol, recent research has proposed innovative mechanisms like the committee endorsing approach. This mechanism introduces a collaborative process in forming new blocks by requiring participation from multiple nodes. By involving additional nodes in the block creation process, the committee-endorsing mechanism [7] aims to increase the decentralization and fault tolerance of the PoA consensus, addressing concerns about its centralized nature. This approach contributes to a more inclusive and distributed decision-making process within the network. While PoA offers advantages such as energy efficiency and security, its centralized nature remains a drawback. Validators in a PoA consensus network are preapproved and have the authority to validate transactions and create new blocks. This can lead to a concentration of power within a limited group of validators, potentially raising concerns about the system's resilience and censorship resistance [8]. However, it is important to note that in private and permissioned blockchain networks, where trust and known entities are crucial, the centralized nature of PoA can be acceptable and even desired to ensure a controlled and trusted environment. The implementation and integration of the new PoA consensus on a specific blockchain network, such as VeChainThor [9], would require careful planning and an implementation roadmap. This includes considering factors such as network compatibility, performance optimizations, security audits, and community acceptance. Proper implementation ensures the seamless adoption of the PoA consensus while maintaining the integrity and security of the existing blockchain ecosystem.

Further, in a permissioned blockchain with PoA consensus, pre-authenticated nodes play a significant role [10]. These nodes are known and verified before participating in the consensus process, offering advantages such as high performance and enhanced security. However, the use of pre-authenticated nodes can also raise concerns about centralization and privacy. While these nodes ensure a trusted environment and efficient transaction processing, the concentration of control and potential exposure of user credentials may impact the decentralized and privacy aspects of the blockchain network. In the realm of Industry 5.0, where rapid digital advancements are reshaping industrial landscapes, the FusionFedBlock [11] scheme emerges as a solution to the intricacies faced when integrating IoT into industrial infrastructures. This ground-breaking plan addresses important issues including centralization, privacy preservation, latency, and security by fusing the strength of blockchain with federated learning. Departments like Production, Quality Control, and Distribution operate at the federated layer and participate in localized learning updates made possible by network automation, maintaining anonymity between entities. For safe and distributed storage, the system makes use of a Distributed Hash Table (DHT) at the cloud layer. The issue of detecting device failures in the IIoT networks is a critical concern. However, conventional methods necessitate the uploading of raw data from client devices to a centralized server for model training, potentially compromising the confidentiality of sensitive business data. To address this privacy concern, a blockchain based federated learning approach is proposed in [12] for detecting device failures in the IIoT. The platform architecture employs a Merkle tree structure to ensure verifiable data integrity, with each client storing the root on the blockchain. Additionally, a smart contract based mechanism is devised to incentivize client participation in the local model training process, taking into account the data size and centroid distance. The proposed approach is evaluated for its feasibility, accuracy, and performance, and the results demonstrate its effectiveness and potential in addressing the device failure detection problem in the IIoT. Recently, Issa et al. [13] have presented a comprehensive survey on federated consensus for securing IoT networks, highlighting its potential in addressing privacy, security, and scalability challenges in federated learning, providing a secure and decentralized platform. It emphasizes the benefits of this consensus, such as trustless and transparent systems, solving data silo issues, creating incentive mechanisms, and enabling diverse IoT applications. In this line, [14-15] and [16-17] also present insights into the potential of federated consensus for improving the efficiency and sustainability of manufacturing and healthcare industries.

## III. PROPOSED FED-POA

The FED-PoA mechanism proposed in this research combines the concepts of reputation-based model, predictable block generation, committee-endorsing mechanism, and federated learning as described below. The FED-PoA architecture is illustrated with Figure 1.

1. Pre-approved nodes: These are nodes that have undergone identity verification and are known and trusted participants in the network.
2. Reputation-based model: This model is utilized for transaction validation, where the pre-approved nodes, acting as validators, assess the validity of incoming transactions.
3. Predictable block generation: With this process, the validated transactions are organized into blocks in a predictable sequence. This allows for efficient and reliable block creation.
4. Committee-endorsing mechanism: This mechanism involves the participation of other nodes besides the selected block producer, ensuring the formation of new blocks through a collaborative process.
5. Local Model updates: The federated learning component, represented by the "Federated Learning" box, incorporates the concept of model aggregation. In this process, the pre-approved nodes perform local model updates based on their respective datasets.
6. Global Model updates: The updated local models from each pre-approved node are aggregated to create a global model. This global model is then utilized for further transaction validation and block generation in the reputation-based model and predictable block generation stages, respectively.

### A. *Reputation-based model*

In the reputation based model of the Fed-PoA framework, each node's reputation score, denoted as $RS_i$, is determined based on its past performance and behavior in the network. Let $N$ represent the set of nodes in the network. The reputation score of node $i$ is calculated using a function $f$ that considers various metrics, such as the number of validated transactions, accuracy of validations, and consistency of consensus decisions as in (1), where $m_i = [m_1, m_2, \ldots, m_M]$ represents the vector of metrics associated with node $i$ and $w_j$ denotes the weight assigned to each metric $m_{ij}$.

$$RS_i = f(m_i) = \sum_{j=1}^{M} w_j \cdot m_{ij} \qquad (1)$$

The weights $w_j$ reflect the importance or significance of each metric in determining the reputation score and calculated as in (2).

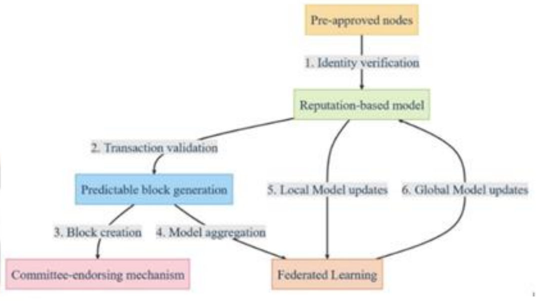

Fig.1. FED-Poa Architecture

$$w_j = \frac{|m_j|}{\sum_{k=1}^{M} |m_k|} \qquad (2)$$

These weights can be predetermined based on the specific requirements and priorities of the PoA network or can be dynamically adjusted based on the evolving network conditions. Each metric $m_{ij}$ represents a specific aspect of a node's performance, behavior, or contribution to the network. Examples of metrics could include the number of validated transactions, accuracy of validations, consistency of consensus decisions, response time, or participation level in the consensus process.

By assigning appropriate weights to the metrics, the function $f$ aggregates the individual metric values to calculate the reputation score $RS_i$ for each node. The reputation scores provide a quantitative measure of a node's authority and trustworthiness in the PoA network and influence its role in the consensus process. These scores are dynamically updated over time as nodes participate in the PoA consensus process. During consensus rounds, the nodes exchange reputation scores and adjust them based on the consensus outcomes and the opinions of other validators. This ensures that the reputation scores reflect the nodes' authority and reliability within the network.

Nodes with higher reputation scores are given more influence in the PoA consensus process. They have a greater probability of being selected as validators and can have a stronger impact on the final consensus decisions. This mechanism aligns with the PoA concept where authority is granted to nodes that have proven their trustworthiness and ability to contribute to the consensus. To maintain the integrity of the reputation based model, safeguards can be implemented to prevent manipulation or gaming of reputation scores. For instance, reputation scores can be verified and validated by multiple trusted nodes in the PoA network to ensure accuracy and fairness. By incorporating the reputation based model within the PoA mechanism, the Fed-PoA framework promotes trust, reliability, and accountability among participating nodes. It incentivizes good behavior and discourages malicious or unreliable actions, thereby enhancing the security and efficiency of the PoA consensus process.

### *B. Predictable block generation*

The predictable block generation process in the Fed-PoA mechanism follows a predetermined order based on the position of each validator in the sequence. Let $N$ be the total number of validators in the network. Each validator $i$, where $i \in 1,2,\ldots,N$, has a specific turn or position in the block generation sequence. During their turn, validator $i$ is responsible for creating a new block by including a set of verified transactions. This can be represented as $Block_i = \{tn_1, tn_2, \ldots, tn_k\}$, where $Block_i$ represents the block created by validator $i$, and $tn_1$ to $tn_k$ are the verified transactions included in the block. Once the validator $i$ has created the block, it is added to the blockchain, and the process moves on to the next validator in the sequence, $i+1$. By following this predictable block generation process, the Fed-PoA mechanism ensures that each validator knows when it is their turn to generate a block. This eliminates the need for extensive computational resources or competitive mining, as seen in other consensus mechanisms like PoW. As a result, the Fed-PoA mechanism can achieve higher transaction throughput and greater efficiency in block creation.

### *C. Committee Endorsing Mechanism*

The Committee Endorsement Mechanism (CEA) is a proposed enhancement to the PoA consensus algorithm that fundamentally changes the way a block is created. This approach introduces two new concepts: the Endorsing Committee and the Endorsing Threshold. The Endorsing Committee is a group of nodes that are randomly selected from a pool of authorized nodes to endorse the new block. The Endorsing Threshold is a minimum number of endorsements required for a new block to be considered valid. In this way, the Committee Endorsing Mechanism helps to increase the security and decentralization of PoA by involving more nodes in the block creation process.

The algorithm starts with the selected block producer creating a new block and broadcasting it to the network. Then, a committee of nodes is randomly selected from the pool of authorized nodes. Each node in the committee evaluates the new block based on their own criteria. If the number of endorsements received by the new block is greater than or equal to the endorsing threshold $T$, the block is considered valid and added to the blockchain. Otherwise, the block is rejected, and the process starts again with a new block producer.

**Algorithm: Committee Endorsement**

Inputs:

- Selected block producer $B$
- Pool of authorized nodes $P$
- Endorsing threshold $T$
- Committee Pool $P$

Outputs:

- “Valid” or “Invalid block”

Steps:

```
1. CreateNewBlock(block $b$)
2. $C$ ← RandomlySelectCommittee(pool $P$)
3. endorsements ←0
4. for each node $i \in C$ do
       if EvaluateBlock(node, block) then
           endorsements ←endorsements + 1
       end if
       if endorsements >= T then
           AddBlockToBlockchain(block)
           Output "Valid block"
       else
           Output "Invalid block"
       end if
```

In this algorithm, CreateNewBlock(block) creates a new block and broadcasts it to the network, RandomlySelectCommittee(pool, committee_size) is a function that randomly selects a committee of specified size from the pool of authorized nodes, EvaluateBlock(node, block) is a function that evaluates the new block based on the criteria defined by each node in the committee and AddBlockToBlockchain(block) is a function that adds the valid block to the blockchain.

### *D. Adaptive Federated Learning*

The adaptive federated learning algorithm enables the training of a global machine learning model across decentralized devices or servers, while ensuring data privacy. This algorithm involves initializing the global model, selecting a subset of clients for each training round, distributing the current global model to the selected clients, conducting local model training on each client's dataset, aggregating the updated models from all clients to refine the global model, calculating the entropy of the updated global model, and terminating the training process if the entropy falls below a predetermined threshold. This collaborative approach to model training promotes data privacy, decentralization, and improved machine learning outcomes.

**Algorithm: Adaptive Federated Learning**

```
Input:
    • Global model $W$
    • List of participating clients $C$
    • Number of training rounds $T$
    • Entropy threshold $\theta$
Output:
    • Trained global model $W_{trained}$
Steps:
    1. Initialize global model $W$
    2. For each training round $t$ from 1 to $T$ do:
        a. Select a subset of clients $C_t$ from $C$
        b. For each client $c \in C_t$ do:
            i.   Assign the global model $W$ to the client's
                 local model $W_c$
            ii.  Train the local model $W_c$ on the client's
                 local dataset
            iii. Send the updated local model back to the
                 server
        c. Aggregate the updated local models from all
           clients in $C_t$ to update the global model $W$
        d. Calculate the entropy of the updated global
           model
        e. If $entropy < \theta$, stop training and return
           the trained global model:
            i. $W_{\text{trained}} \leftarrow W$
    3. Return the trained global model: $W_{trained}$
```

## IV. PERFORMANCE EVALUATION

This section presents the experimental setup to implement the proposed Fed-PoA mechanism and calculate its performance.

### *A. Experimental Results*

The experimental setup involved a comprehensive evaluation of the proposed FL and consensus schemes using specific configurations of hardware and software. The hardware setup included high-performance servers equipped with Intel Xeon processors and Nvidia Tesla V100 GPUs, edge devices with Intel Core i7 processors and Nvidia GeForce RTX 2080 GPUs, and resource-constrained IoT devices with ARM Cortex-M4 processors. The software stack utilized TensorFlow 2.5 as the primary machine learning framework, along with Python 3.8, NumPy, and scikit-learn for data preprocessing, model training, and evaluation.

The experiments were conducted with varying numbers of participating clients, ranging from 100 to 500, to assess the scalability. The learning rate was set to 0.01, the batch size was chosen as 32, and the models were trained for 100 epochs. Real-time Device-to-device (D2D) connectivity was simulated using a custom network simulator, which incorporated realistic latency and packet loss characteristics based on empirical measurements.

To ensure the reliability of results, each experiment was repeated five times, and the average performance metrics, including training accuracy, validation accuracy, and convergence time, were recorded. The experiments were terminated if the models failed to show significant improvement in validation accuracy after 50 epochs. By considering specific configurations of hardware and software, the study provided valuable insights into the performance and scalability of the FL and consensus schemes under realistic conditions.

### *B. Experimental Results*

The performance of the Fed-PoA is assessed on several key metrics, including the convergence rate, communication overhead, power consumption, and memory usage. The convergence rate, $cr$ measures the speed at which the model converges to a stable solution. It is calculated as the number of epochs required for the model to reach a certain level of

*DOI: https://doi.org/10.17762/ijritcc.v11i9.8358*
***Article Received:** 15 July 2023 **Revised:** 08 September 2023 **Accepted:** 20 September 2023*

accuracy, $n_{epochs}$. The communication overhead, $c_{oh}$ measures the amount of data transmitted between clients and the central server during training. It is calculated as the total amount of data transmitted, $d_{total}$ during the training epochs as in (3).

$$c_{oh} = \frac{d_{total}}{n_{epochs}} \qquad (3)$$

The power consumption $pc$ measures the amount of energy consumed by each client during training. It is calculated as the product of the power consumed per unit time, $p_{\text{unit}}$, and the training time, $t_{\text{train}}$ as in (4).

$$pc = p_{\text{unit}} \cdot t_{\text{train}} \qquad (4)$$

Memory usage, denoted as $MU$, quantifies the amount of memory used by each client during the training process. It is calculated as the maximum memory usage, denoted as $M_{\max}$, observed during training.

The asymptotic error constant α, or rate of convergence, is a quantity that represents how quickly the system approaches consensus. It is calculated as the limit of the ratio of the error at each iteration to the error at the previous iteration as in (5). Here, $E_k$ denotes the error at iteration $k$, and $E_k - 1$ is the error at the previous iteration $k - 1$.

$$\alpha = \lim_{k\to\infty} \frac{E_{k-1}}{E_k} \qquad (5)$$

Table 1. Fed-PoA Performance Metrics

| No. of Nodes | $n_{epochs}$ | $C_{oh}$ | *Pc* watts (W) | MU (MB) | α |
|---|---|---|---|---|---|
| 100 | 50 | 1.5 | 57.3 | 32.6 | 0.01 |
| 200 | 70 | 2.2 | 61.9 | 59.2 | 0.07 |
| 300 | 90 | 3.4 | 75.7 | 61.2 | 0.21 |
| 400 | 115 | 4.9 | 88.5 | 75.3 | 0.35 |
| 500 | 140 | 5.2 | 104.6 | 98.7 | 0.41 |

It can be observed that as the number of nodes increases, the convergence rate tends to increase as well. Additionally, both power consumption and memory usage also show an increasing trend with an increase in the number of nodes. This indicates that as the network size grows, more computational resources are required, resulting in higher power consumption and memory usage.

An investigation of the variations in the metrics obtained from networks with varying numbers of nodes was carried out by means of a statistical study. To determine whether or whether the differences between the node groups are statistically significant, a one-way analysis of variance (ANOVA) was carried out. According to the findings, there was a discernible relationship between the number of nodes and the pace of convergence (F(4, 15) = 3.82, p = 0.027). Post-hoc pairwise comparisons using Tukey's honestly significant difference (HSD) test indicated that the mean convergence rate for the group with 500 nodes (M = 5.2) was significantly different from the groups with 100 nodes (M = 1.5) and 200 nodes (M = 2.2), with p-values of 0.012 and 0.034, respectively. This indicated that the mean convergence rate for the group with 500 nodes was significantly higher than the mean convergence rate for the group with 100 nodes. However, there were no discernible variations detected between the node groups with regard to the amount of power used (F(4, 15) = 1.58, p = 0.240) or the amount of memory utilized (F(4, 15) = 2.12, p = 0.118). Based on these data, it seems that the number of nodes has an effect on the convergence rate; nevertheless, the amount of power used and the amount of memory used are essentially stable regardless of the layout of the nodes.

Further, the relationship between θ and α is studied to understand the impact of the entropy threshold on the convergence speed of Fed-PoA. This analysis depicted in Figure 2 shows an increase in α with respect to θ for different sizes of the network. It is observed that as the θ increases, α also increases, indicating a less accurate consensus. Furthermore, the effect of the entropy threshold on the error becomes more pronounced for larger networks with more nodes. This can be due to the fact that a higher entropy threshold leads to a larger search space, which makes it more difficult for the optimization algorithm to find the optimal solution. Thus, the choice of an appropriate entropy threshold should consider the trade-off between desired accuracy and computational/network constraints.

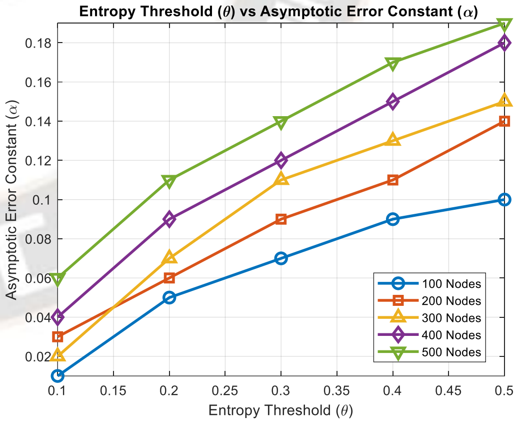

Fig.2. Entropy Threshold vs Asymptotic Error

The empirical evaluation of the model reveals that the combination of federated consensus and the PoA approach offers improved convergence rate, reduced communication overhead, lower power consumption, and efficient memory usage, making it a promising solution for collaborative and resource-constrained environments.

## V. CONCLUSION

The Fed-PoA introduced in this paper, effectively tackles the consensus challenges in IoT-Blockchain applications through a synergistic combination of PoA and federated learning. This protocol enables efficient data sharing and privacy preservation and also ensures decentralized operation, making it a compelling choice for secure and scalable IoT-Blockchain applications. The performance evaluation of Fed-PoA showcases its superior convergence and memory usage compared to existing approaches, underscoring its potential in achieving efficient and dependable consensus. The Fed-PoA serves as a valuable contribution to the advancement of secure and scalable systems for IoT-Blockchain, offering a promising solution to address the intricate intricacies of consensus in this domain. By exploring and implementing it in real-world scenarios, Fed-PoA can drive the advancement of IoT-Blockchain technologies, revolutionizing industries such as healthcare, smart cities, and industrial IoT.

## REFERENCES

[1] Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. IEEE communications surveys & tutorials, 17(4), 2347-2376.

[2] A. G, et al "An Intelligent LoRa based Women Protection and Safety Enhancement using Internet of Things," (I-SMAC), Dharan, Nepal, 2022, pp. 43-48, doi: 10.1109/I-SMAC55078.2022.9987425..

[3] Wang, Y., Peng, H., Su, Z., Luan, T. H., Benslimane, A., & Wu, Y. (2022). A platform-free proof of federated learning consensus mechanism for sustainable blockchains. IEEE Journal on Selected Areas in Communications, 40(12), 3305-3324.

[4] Khan, A. G., Zahid, A. H., Hussain, M., Farooq, M., Riaz, U., & Alam, T. M. (2019, November). A journey of WEB and Blockchain towards the Industry 4.0: An Overview. In 2019 International Conference on Innovative Computing (ICIC) (pp. 1-7). IEEE.

[5] Qi, M., Wang, Z., Wu, F., Hanson, R., Chen, S., Xiang, Y., & Zhu, L. (2021). A blockchain-enabled federated learning model for privacy preservation: System design. In Information Security and Privacy: 26th Australasian Conference, ACISP 2021, Virtual Event, December 1–3, 2021, Proceedings 26 (pp. 473-489). Springer International Publishing.

[6] de Oliveira, M. T., Reis, L. H., Medeiros, D. S., Carrano, R. C., Olabarriaga, S. D., & Mattos, D. M. (2020). Blockchain reputation-based consensus: A scalable and resilient mechanism for distributed mistrusting applications. Computer Networks, 179, 107367.

[7] Ren, Z., & Zhou, Z. (2020). SURFACE: A Practical Blockchain Consensus Algorithm for Real-World Networks. arXiv preprint arXiv:2002.07565.

[8] Pandey, R., Faiyaz, M. S., Singh, G., & Uddin, Z. (2023). Functional analysis of blockchain consensus algorithms. In Distributed Computing to Blockchain (pp. 207-233). Academic Press.

[9] She, Z. (2022). VeChain: A Renovation of Supply Chain Management--A Look into its Organisation, Current Acitivity, and Prospect.

[10] Al Asad, N., Elahi, M. T., Al Hasan, A., & Yousuf, M. A. (2020, November). Permission-based blockchain with proof of authority for secured healthcare data sharing. In 2020 2nd International Conference on Advanced Information and Communication Technology (ICAICT) (pp. 35-40). IEEE.

[11] Singh, S. K., Yang, L. T., & Park, J. H. (2023). FusionFedBlock: Fusion of blockchain and federated learning to preserve privacy in industry 5.0. Information Fusion, 90, 233-240.

[12] Singh, S. K., Yang, L. T., & Park, J. H. (2023). FusionFedBlock: Fusion of blockchain and federated learning to preserve privacy in industry 5.0. Information Fusion, 90, 233-240.

[13] Zhang, W., Lu, Q., Yu, Q., Li, Z., Liu, Y., Lo, S. K., ... & Zhu, L. (2020). Blockchain-based federated learning for device failure detection in industrial IoT. IEEE Internet of Things Journal, 8(7), 5926-5937.

[14] Singh, S. K., Yang, L. T., & Park, J. H. (2023). Fusion FedBlock: Fusion of blockchain and federated learning to preserve privacy in industry 5.0. Information Fusion, 90, 233-240.

[15] G. A "Efficient Internet of Things Enabled Smart Healthcare Monitoring System Using RFID Security Scheme" Intelligent Technologies for Sensors, 1st Edition, 2023, Apple Academic Press, ISBN: 9781003314851.

[17] Boobalan, S., Das, S., Pandi, V.S., Swain, K.P., Palai, G, "Generation of multiple signals using single photonic structure at visible regime: a proposal to realize the harmonic generation", Optical and Quantum Electronics, 2021, 53(8), 463.