Received: 20 June 2024 | Revised: 27 October 2024 | Accepted: 12 November 2024

IET Communications

DOI: 10.1049/cmu2.12870

ORIGINAL RESEARCH

Blockchain controlled trustworthy federated learning platform for smart homes

Sujit Biswas[1] | Kashif Sharif[2] | Zohaib Latif[3] | Mohammed J. F. Alenazi[4] | Ashok Kumar Pradhan[5] | Anupam Kumar Bairagi[6]

[1]Department of Computer Science, City St George's, University of London, London, UK

[2]School of Computer Science and Technology, Beijing Institute of Technology, Haidian District, Beijing, China

[3]Department of Computer Science, School of Engineering and Digital Sciences, Nazarbayev University, Astana, Kazakhstan

[4]Department of Computer Engineering, College of Computer and Information Sciences, King Saud University, Riyadh, Saudi Arabia

[5]SRM University-AP, Andhra Pradesh, India

[6]Computer Science and Engineering Discipline, Khulna University, Khulna, Bangladesh

Correspondence
Sujit Biswas, Department of Computer Science, City St George's, University of London, Northampton Square, London EC1V 0HB, UK.
Email: sujit.biswas@city.ac.uk

Funding information
Natural Science Foundation of Beijing Municipality, Grant/Award Number: IS23056; Deanship of Scientific Research, King Saud University, Grant/Award Number: RSPD2024R582

Abstract
Smart device manufacturers rely on insights from smart home (SH) data to update their devices, and similarly, service providers use it for predictive maintenance. In terms of data security and privacy, combining distributed federated learning (FL) with blockchain technology is being considered to prevent single point failure and model poising attacks. However, adding blockchain to a FL environment can worsen blockchain's scaling issues and create regular service interruptions at SH. This article presents a scalable Blockchain-based Privacy-preserving Federated Learning (BPFL) architecture for an SH ecosystem that integrates blockchain and FL. BPFL can automate SHs' services and distribute machine learning (ML) operations to update IoT manufacturer models and scale service provider services. The architecture uses a local peer as a gateway to connect SHs to the blockchain network and safeguard user data, transactions, and ML operations. Blockchain facilitates ecosystem access management and learning. The Stanford Cars and an IoT dataset have been used as test bed experiments, taking into account the nature of data (i.e. images and numeric). The experiments show that ledger optimisation can boost scalability by 40–60% in BCN by reducing transaction overhead by 60%. Simultaneously, it increases learning capacity by 10% compared to baseline FL techniques.

1 | INTRODUCTION

Smart devices, such as IoT, sensors, and control systems, equip smart homes and continuously expand their services through the development of integral technologies. Statistics show that market demand for IoT is increasing day by day; for example, the worldwide SHs are estimated to be 672.57 million, and the penetration rate will be 86.47% in 2027 [1]. As the number of houses rises, data generation increases. Figure 1 shows the connectivity of a typical SH, where the gadgets continuously produce enormous volumes of data with a variety of attributes, such as user expressions, behaviors, and contentment. Third-party service providers usually control the devices independently or collaboratively, and they use a service-specific centralised server, such as a cloud or edge server [2, 3]. Service providers, researchers use a variety of centralised technologies, including ML and statistical analysis, to study SH users' data in order to better understand customer service expectations, future market analyses, and so on. Centralised servers, which aggregate vast amounts of data and become attractive targets for cybercriminals, can enhance vulnerability scopes in an interoperable environment. It adds additional challenges when these data are used for predictive analysis using typical centralised AI approaches, as data need to be shared directly with the researchers [4].

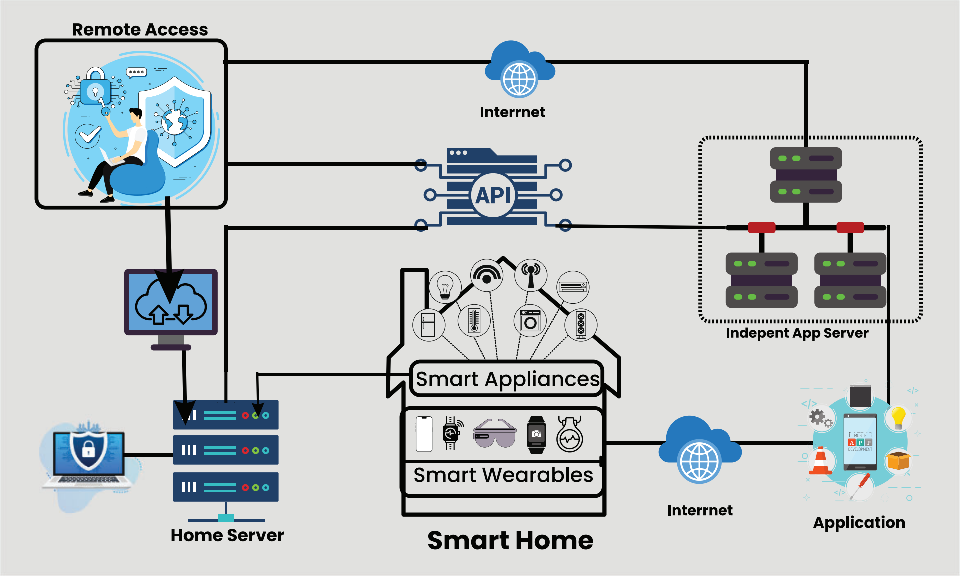


FIGURE 1 Typical smart home network.

Considering the issues, researchers recommend using privacy-preserving FL technology to integrate numerous SHs, establishing an interoperable platform to maximise data utilisation. Real-time big data can be used for intelligent analysis, service need analysis, predictive maintenance, and future forecasting by generating an updated AI model [4, 5]. Although FL allows distributed privacy-preserving ML approaches, its centralised aggregator creates another centralisation problem [6]. In light of that, researchers suggested blockchain technology to replace the centralised aggregator to ensure complete security of end-users' data, thereby surpassing the limitations of centralisation [7]. While the integration of blockchain with FL can enhance security, it may also lead to service disruptions and technical problems due to the scalability issues inherent in blockchain technology [8]. Scalability issues or transaction finalisation delays in blockchain-integrated FL smart-home ecosystems targeting run-time learning can cause three challenges: (1) transaction finalisation delays that can interrupt device-server-device smooth communication; (2) synchronisation issues that can fail block commit within consensus time; and (3) a sharp increase in blockchain ledgers that will increase memory cost.

Researchers focused on integrating FL and blockchain to address centralisation aggregation challenges [9]. Few researchers employed differential privacy-boosting security [10]. Many of them concentrated on enhancing model accuracy using various typical ML approaches in FL environments [11]. Very few studies have focused on the scalability of integrated systems. For example, in [12], the authors proposed a new consensus approach to enhance scalability, but neglected the ecosystem's uninterruptible services but AI model creation. In fact, smart home services rely on a variety of smart devices that are interdependent. Any service interruption can have the potential to disrupt regular services. For instance, if a smoke detector transmits a message to the server, a communication interruption or delayed finalisation causes the message to reach the automatic fire extinguisher later. It is critical to include run-time learning facilities alongside existing SH services that are scalable and uninterruptible. Contrary to the fact that blockchain is known to have scalability challenges, integration of FL and blockchain can result in longer transaction finalisation times and potential disruptions in SH services. Moreover, each SH transaction executed through blockchain will result in an overload of the blockchain network. Therefore, it is crucial to implement intelligent solutions that ensure the uninterrupted and prompt delivery of SH services, thereby sustaining existing services. The system will use machine learning methodologies to integrate service providers to extract insights from user data without direct access while ensuring privacy, security, and compatibility within a smart-home ecosystem.

This article proposes a blockchain-based federated learning architecture for intelligently securing access to end-user' data generated from the SH. The framework introduces a gateway peer to process insights of the data from individual SH, rather than sharing and gathering all data from various SHs under a centralised network server for ML-based analysis. As an entity of a blockchain network, the gateway peer maintains the current services of a SH and concurrently contributes to the creation of an updated model by sharing insights from local models with other SHs. Blockchain, as a component of a permissioned blockchain-controlled global learning network, provides access control and aggregator services for the overall ecosystem. The article highlights the following key contributions:

- A blockchain-controlled FL architecture that enables safe remote access to a typical SH and is useful for customer behaviour analysis of SH data. FL enables privacy preserving knowledge extraction from various SH while blockchain extends the run-time security of model aggregation.

- An ideal method for managing significant local transactions produced in a home. Introduced gateway peers handle large number local transactions itself as a result, it improves the scalability, optimised the ledger reduces the overburden in BCN.
- Presenting the technological difficulties encountered in the actual world such as quick expansion of BC ledger.
- A testbed analysis using on popular public Stanford Car datasets and IoT Dataset shows the effectiveness of the proposal.

The remaining sections of this article provide further information on the specific steps and processes involved in implementing the discussed concepts. Section 2 explicitly discusses recent contributions in the field of SH implementation terminology. The proposed architecture details are illustrated in Section 3. Section 4 provides details on the implementation settings, findings, and security analysis based on two distinct datasets, one of which is an IoT dataset. Section 5 provides the final conclusion of the whole contribution.

2 | BACKGROUND AND RELATED WORKS

This section outlines the background technologies for the proposed architecture and related works. Basically, the research offers a decentralised distributed learning network that uses Federated Learning instead of a typical machine learning network. It also includes a decentralised aggregator that gets rid of all the risks of centralisation in the ecosystem as a whole.

2.1 | Federated machine learning(FL)

FL allows several users to individually train models using their own data, without the need to share the data. Within a smart home network (SHN), either a local home server or a cloud server leads to developing a local model in FL process by effectively exploiting the vast amount of data generated by IoT. These individual models are then combined into a global model via a central aggregator. It is also known as distributed machine learning [9]. Typically, a distributed machine learning network consists of a number of nodes, each of which is capable of processing input on its own and contributing to the outcome. Multi-node machine learning (i.e. distributed ML) methods and systems are meant to increase accuracy, scale to bigger input data quantities, and improve performance, and they can be geographically dispersed. Let $P = P_1, P_2, \dots, P_n$ represent geographically distributed n participating nodes in an FL task. P_i is the controlling server of i organisation and is also responsible for securing, storing data and providing intelligent services through machine learning. Every organisation holds their own records generated by it's integral devices, such as $D_1, D_2, \dots D_n$. While P_i is going to join the FL network, a central aggregator initiates a global model (M_i^g) for P_i. Then, P_i trains the M_i^g by its data D_i which is known as a local model (M_i^l) of i. Consequently, the central aggregator collects every local model and averages them at every round of the training. Details of the local training process are shown in Section 3.3.2. A centralised aggregator arises the typical challenges of a centralised system, which is recovered by blockchain-based decentralised aggregator in this research.

2.2 | Blockchain as a decentralised aggregator

Blockchain is a cryptographically immutable, secure, distributed ledger technology (DLT) that enables secure data exchange between many parties. It enables value exchange (i.e. transactions) without the need for confidence or authority from a central institution. The transactions are recorded in a ledger that is managed by a network of interconnected computers, known as peers, rather than being held in a centralised entity such as a cloud server. The BC system does an autonomous verification (i.e. endorsement) prior to authorising the transaction, which is vital in guaranteeing security and is known as consensus [18]. Furthermore, it enables consortium's to engage in smart contract-based inter-organisational transactions, which is crucial for facilitating communication among service providers. A blockchain as a service platform has the capability to govern existing centralised servers, enabling them to transition and conform to a DLT system [19]. By replacing the centralised aggregator used in typical FL technology with a blockchain network, we can overcome the challenges that arise with a centralised system. However, the challenge is handling the continuous transactions in a BC network. In addition, typically, a block can hold a maximum of 1 MB of data, whereas in FL, each model over 200 MB has to fit into a block, which is very challenging. Therefore, we have proposed a local peer for handling the continuous transaction with a customised block structure for carrying the block with the model's replica. In this research, a cloud server generated every local model collected and created a global model in the blockchain network. The network is also responsible for access control over cloud servers.

2.3 | Related works

This section presents a detailed overview of recently suggested blockchain-based machine learning-based solutions for the best use of SH data. We have also narrowed down the related FL solutions and identified significant differences with this proposal. Till now, enormous solutions have been proposed for SH security. Indeed, most of them used traditional centralised architecture that raised single points of failure, strict security, and privacy issues [20]. Considering the limitations of centralised systems, stand-alone blockchain technology has been considered in many recent articles [21, 22] to mitigate typical SH challenges. Many of them considered data to be deemed wealth for autonomous learning and blockchain for cyber security [23, 24]. However, in typical machine learning, systems learn from users' raw data, which raises other security issues solved by

TABLE 1 Recent contributions.

Paper	Aim	Objectives	Security	Scalability	Intelligent analysis
[13]	Intrusion detection and defense mechanism	improve security	✓	X	✓
[14]	ML platform	Accuracy improvement	X	X	✓
[15]	Mutual authentication system	encryption, group signature	✓	X	✓
[16]	Smart home framework	Enhanced security	✓	X	✓
[17]	Decentralised FL system	Automation, improve security	✓	X	✓
This work	**Scalable secure analysis of data**	**Framework, privacy-preserving analysis of IoT insight**	✓	✓	✓

Google's FL technology [25]. FL allows decentralised training by data owners but shares learning outcomes with a centralised aggregator. In terms of security, this centralised aggregator is recognised as one of the downsides [26]. A blockchain-based decentralised approach to local gradient sharing is proposed as a solution in [26] where blockchain stores models.

A permissioned blockchain-supported FL platform was proposed in [27] where they suggested encryption for every local update before recording it to the BC ledger. However, federated learning and blockchain technology are considered in many application domains, such as healthcare, vehicular networks, energy sectors etc. For example, in [28], authors contributed BC-based FL that supported an adaptive framework for ensuring network trustworthiness and security. It handles individual users' trust (e.g. positive experiences, guarantees, clarity, and responsibility) to predict devices' trust values. The device failure problem in IIoT is a well-known issue that is considered in [29]. The authors proposed a blockchain-based federated learning platform that enables the verifiable integrity of client data. The proposal's significance is that it allows storing client data records periodically in tree and tree root stores on a blockchain.

The study conducted in [30] summarised the potential for data leakage from a model created by local members in a blockchain-based FL network, where they focused on inference attacks for experimental analysis. The researchers used the accidental sharing of property information to find a group of participants with a certain trait in blockchain-supported federated learning for intelligent edge computing. The authors [31] developed a blockchain-based system to incentive data owners with high-quality data in federated learning and introduced a mechanism for allocating rewards. The reputation mechanism that focuses on blockchain technology produces model aggregation of high quality in a transparent manner. Similar to other contributions, BC has a function in the calculations of rewards and credit points. Several publications have addressed the broad concerns regarding FL, including its limitations in various applications, and proposed ways to connect FL with blockchain technology. Nevertheless, the primary objective of the majority of these publications was to address the centralised aggregator concerns that emerged in the FL network by leveraging blockchain technology. Several papers proposed the use of noise in the local model as a means of augmenting security.

As depicted in Table 1, the majority of recent contributions have concentrated on matters pertaining to security and privacy. Recent contributions primarily emphasise blockchain-based decentralised solutions as a remedy for centralised aggregators. Blockchain is widely recognised as a cybersecurity tool and offers solutions to the concerns commonly discussed. Nevertheless, blockchain encounters challenges in terms of scalability, particularly when integrating an application such as SH with these services. None of them took into account the security implications and the broader SH ecosystem, including how the blockchain network will handle the significant volume of transactions created by SH devices and the constraints of using blocks to store a large model. In contrast, this article seeks to offer a reliable and advanced FL process and scalable solutions to ensure uninterrupted SH services by addressing the time-consuming finalisation of blockchain transactions. Furthermore, it guarantees access control and enhances ledger optimisation to assure the utmost technological advantages.

3 | PROPOSED ARCHITECTURE

This section presents blockchain-based privacy-preserving federated learning (BPFL), the proposed architecture of the ecosystem, which comprises a SHN and a BCN. Figure 2 shows the overall network architecture, consisting of three processing zones: the primary zone presents ubiquitous IoT-driven SHs, and the secondary zone represents gateway (GW), which controls the individual SH. Finally, the blockchain network interconnects every gateway peer (GWP) and provides access control over the whole ecosystem.

3.1 | Overview

The overall network generates a BPFL ecosystem where physical devices from SH interact with each other as well as knowledge generated from their utility data exploits the service providers to improve their services without sharing users' data directly. The ecosystem comprises a network with n number of SH (i.e. $SH_1, SH_2, SH_3, \ldots SH_n \in SHN$) that are connected with servers. The servers play a key role as a gateway to every individual SH that plays a double role, such as *controlling* the SH and *learning* different features from its local data.

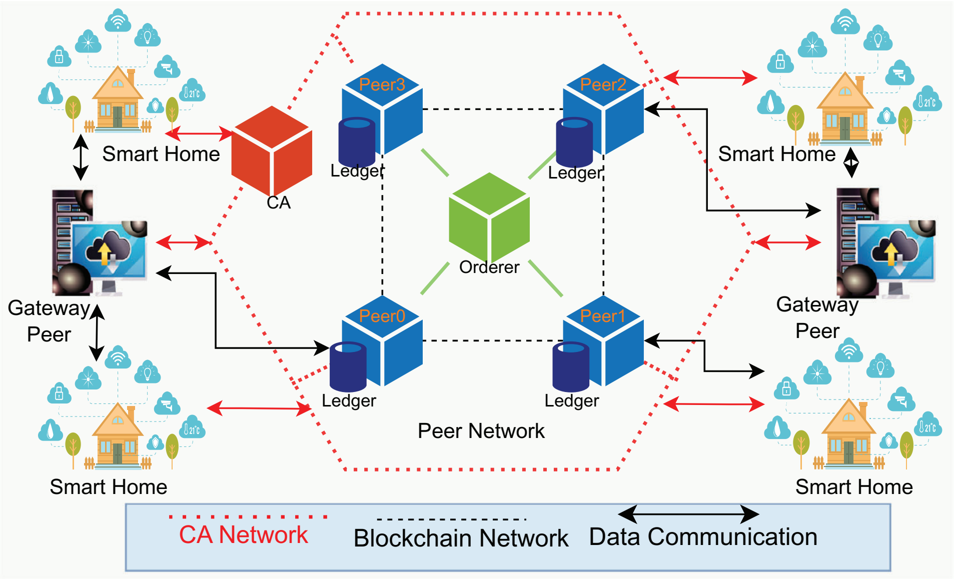


FIGURE 2 BPFL framework overview.

Interconnecting gateways with each other forms a Peer-to-Peer (P2P) network (i.e. BCN) instead of centralised processing of data. BCN access controls gateways as well as aggregates the local models with the proper consensus approval of the network members for generating global models. Every gateway continues the FL process using its local data and generates a local ML model. Consequently, BCN coordinates with gateways, collects all local models, and finally generates the global models. Then the global models are transferred to every gateway for the next iteration of learning, finally producing an optimal model. The framework has three key objectives: scalability, secure ledger optimisation, and smart prediction. Blockchain technology guarantees the protection of data and provides a safe means of accessing household appliances remotely. Secondly, ledger optimisation entails transferring the home server to a local peer by segregating transactions into local and global categories. The FL process guarantees secure and intelligent future predictions, enabling the autonomous evolution of services.

3.2 | Smart home network

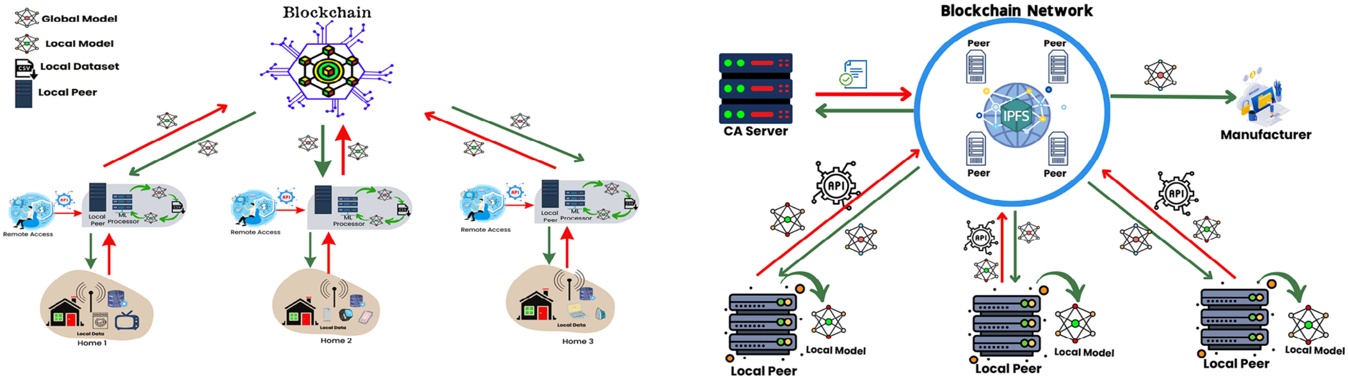
A wide range of advanced smart appliances, such as smart refrigerators, air conditioners, and smart fans, as well as wearable devices like smart watches, glasses, and shoes, are integral components of a SH which necessitate novel administration. Figure 1 illustrates a standard architecture for managing SH applications. It showcases the integration of smart devices, gateways, and back-end networking components within a SHN. Efficiently incorporating these components with the network service provider or server enables global connectivity to a SH. The gateway's physical location could be in the cloud or locally setup in the home, depending entirely on the home owner's service capacity. Within a SHN, users must utilise a home server to access and manage all devices which functions as a gateway. The gateway is accountable for ensuring the compatibility and seamless integration of domestic services. When the GW is linked to the BCN it functions as a local Peer. Access to SH devices from anywhere in the world is only authorised through BCN. Suppose, the set $\{a_1, a_2, a_3, \ldots, a_n\}$ belongs to the SH A_i, where the i^{th} SH comprises n appliances that are controlled through the gateway GW_i. An API enables the management of SHN devices for remote access. Similarly, wearable devices can be managed via a separate app server that is not affiliated with the device itself. These conventional systems all have centralised challenges, which are resolved by utilising a decentralised blockchain network.

3.3 | Blockchain network

Blockchain network consist of a combination of core peers and some local peers, where a traditional home server becomes a local peer and joins as an extended network member. A local peer uses blockchain technology and plays a solo peer role. An overview of our system architecture is shown in Figure 3. BPFL incorporates the connectivity of SHs with blockchain through local peers. It also acts as a gateway to segregate global, local, and remote transactions and ensure remote access through an API, as illustrated in Figure 3a. In a similar vein, the details of the network connectivity among the manufacturer, external parties, and the gateway are shown in Figure 3b. Every network member, including manufacturer authentication, is controlled through certificate authority (CA).

3.3.1 | Network

A device manufacturer or SH service provider who has a trusted relationship with the device manufacturer generates the BCN,



(a) Connectivity of the Ecosystem

(b) Federated Training Steps

FIGURE 3 Local peer and blockchain connectivity.

on which SH owners and other stakeholders groups can be registered. Core BCN is formed with a group of peers (more than three) interconnected to create a distributed network. Local peers interconnect with the BCN and join the consensus processes. Beyond consensus, a local peer plays a solo peer role to maintain the scalable services of SH transactions. BCN forms with Peer (P) where $P_1, P_2, P_2, \dots P_n \in BCN$.

3.3.2 | Local peer or gateway peer

Local peers exclusively cater to smart IoT devices used within SH. In the proposed framework, local peers manage specific IoT devices of a specific i SH where $D_1, D_2, D_3, \dots D_n \in P_i^l$. Similarly, $P_1^l, P_2^l, P_3^l \dots P_n^l \in BCN$. Local peers $\forall P_{i=1}^n$ function as a solo peer with a replica of the blockchain protocol, and the integrity of the gateway is maintained using CA-generated certificates, which generate and maintain the integrity of the network components. Any existing centralised server of a typical SH can play a gateway role as a solo peer. To extend the security, solo peers can be linked with multiple peers under a blockchain network for a specific SH, which means $P_1^l, P_2^l, \dots P_n^l \in SH_i$. It can eliminate the risk of a single point of failure for i SH. Local peer P_i^l handles all transactions generated from a SH. Algorithm 1 states the transaction execution approaches in detail. It has been demonstrated that P_i^l checks the origin and destination of the transaction as it is being executed. Without involving BCN, it runs locally if the transaction's source and destination are itself; otherwise, it sends it on to BCN. Initiating a smart contract, which is a programme chaincode that is preinstalled, is the first step in any locally executable transaction. The criteria and terms between two devices are reflected in the chaincode. Whenever the outcome of chaincode invocation is affirmative, the home network's local ledger is used to perform and store transactions. If the incoming transaction destination is not part of P_i^l, the BCN is prepared to execute the transaction by means of its integrated application. It can reduce transaction overloading by up to 70% [8].

ALGORITHM 1 Local peer's transaction executions.

```
Input  : $(\mathtt{sk}, \upsilon_i, Tx_i, \mathtt{pk}_{\text{sign}}^{\upsilon_i})$
Output: Success/Failure
$P^l\{Tx_i, Tx^{src}, Tx^{dst}\} \leftarrow \forall D_i^n$
if $Tx^{dst} \in P_i^l$ then
    $\overline{Tx_i} \leftarrow H(Tx_i)$ \\ Hash of Tx
    $\mathtt{B_i} \leftarrow \mathtt{append}(\overline{Tx_i}, (\mathtt{sk}, \rho_i, \delta, \mathtt{pk}_{sign}^{\upsilon_i}))$
    $L^{P_i^l} \leftarrow B_i$
    return Success Ensure Tx is recorded in DB
else
    $\mathtt{B_i} \rightarrow BCN$ \\ forwarding Tx to BCN
    $B_x \leftarrow \forall_{i=1}^n B_i$ \\ Block formation
    $L^{P_i^l} \leftarrow B_x$ \\ External Tx recorded to ledger
end
delete($P_{\text{off-chain}}$) \\ for $D_{Asst}$ only
return  Failure
```

3.3.3 | Certificate authority (CA)

CA is an integral component of the central blockchain network, which processes the issuance of credentials by each peer in the vicinity. Every local peer ensures access to authorised smart residences and their devices via in-built CA services. A distinct CA server is established utilising the Docker container framework in this experiment. Conversely, a distinct database is upheld to facilitate the generation of unique credentials for each household appliance, which are directly controlled by local peers.

3.3.4 | Distributed file storage (DFS)

To facilitate easy file sharing, global and local models are stored on the Inter Planetary File System (IPFS), which functions as a DFS. By default, it creates a distinct content ID (CID) upon uploading. A hash created by the CID and file location pointer is recorded in the blockchain. Based on epochs, ML models are serialised and saved them in HDF5 file format. IPFS services are incorporated into our blockchain peers in this study. Models are obtained from DFS using the CID during consensus. As long as the model file is hosted on at least one node, the IPFS network makes sure it is accessible.

3.4 | Distributed learning approaches

In order to address data-driven concerns, the device manufacturer has made a request to train high-quality learning models. Because doing so would violate applicable data privacy standards, manufacturers cannot gather data directly from IoT devices or utility data from these devices from SHs in order to train models. Participants, who utilise a variety of SH gadgets, are thus crowdsourced by the manufacturer to train the model using the FL framework. So, a producer can share the first model, kept in off-chain storage, with the chosen participants. To address issues with award fairness and collusion attacks, BCN employs blockchain's consensus and incentive mechanisms. As a result, more and more people are eager to participate in FL's model training tasks honestly, and no one including trusted parties can claim otherwise.

3.4.1 | Local model generation

Within our suggested architecture, Local Peer P^l assumes the dual role of overseeing machine learning operations and managing local device control. The diagram in Figure 3a illustrates the process of training models inside various network components. Let us consider that there are n instances of P^l which produce n local models M_n^l, where $m_1^l, m_2^l, \ldots m_n^l \in M_n^l$ are formed by training their respective previously generated datasets $D_1, D_2, \ldots, D_N$. A representative of the SH user i, denoted as P_i^l, decides to utilise its local dataset (D_i) and retrieve the initial global model (M_i^g) downloads from the DFS according to the hash address and CID with the approval of BCN. Upon completion of the training phase, it produces a localised model, denoted as m_i^l. Prior to transmitting to the BCN, differential privacy parameters (as described in Section 3.5) are included into a local model to provide enhanced security. Similarly, each $\forall_{i=1}^{n} GWP_i$ produces its corresponding local model $\{m_1^l, m_2^l, \ldots, m_n^l\}$, which belongs to the set $\{P_1^l, P_2^l, \ldots, P_n^l\}$. Through the utilisation of FL, users transmit their individual models to BCN in order to create a global model (M^g) for the purpose of sharing knowledge while ensuring that their sensitive data remains undisclosed. BCN commences a consensus session and appoints a leader to distribute tasks evenly. The leader constructs a worldwide model (M_i^g) using Equation (1) at the conclusion of the i^{th} training iteration.

To leverage the training process, a typical FL has been developed for a SH i which is responsible for gathering and analysing an input matrix X_i. This matrix is composed of individual input data vectors, represented as $x_{i1}, x_{i2}, \ldots x_{id_i}$. Each x_{id} represents an input vector used in the FL algorithm. Let assume that Y_{id} represents the output of X_{id}, and the output data vector for training using the FL algorithm of a local user P_i^l is denoted as $y_i = [y_{i1}, y_{i2}, \ldots y_{id_i}]$. A vector w_i determines the parameters of the local FL model (M_i^l). For instance, the expression $x_{id}^T w_i$ denotes the anticipated result in a linear regression algorithm using Equation (1), where w_i represents the weight vector. SH i attempts to minimise the training loss by finding the best possible parameters for the learning model using Equation (1).

$$M^l = \sum_{i=1}^{n} f(w_i, x_{i,d}, y_{i,d}), \tag{1}$$

where $f(w_i, x_{i,d}, y_{i,d})$ is the loss function.

ALGORITHM 2 Model aggregation

```
Input: $B_i(M_i^l, \delta), T_i^{acc}$
Output: (Block ($B_x$), $M_i^g$)
BCN Peers verify Credentials of $B_i$ generator;
Leader Selected based on the best $T^{acc}$ for an epoch session;
Leader executes:
    $M_i^g = \frac{1}{D} \sum_{i=1}^{n} M_i^l$;
if the validators signs >> 2/3 and agree on $block_r$: then
    $B_x \leftarrow \mathrm{H}(M_i^g)$;
    $M_i^g \rightarrow$ IPFS (offchain);
else
    $B_x$ is rejected and session canceled;
end if
```

3.4.2 | Global model generation

The peers confirm the credentials and make sure the models came from a reliable source when they get the model upload transactions from each participant. The consensus leader then downloads each encrypted local model and applies algorithm 2 and Equation (2) to compute the model aggregate. The Algorand consensus algorithm, in which the leader logs the aggregate result into a transaction, is what we employed for this experiment [32]. Upon receiving the new block, every peer broadcasts their vote and confirms that the aggregation results in this new block are accurate. The new block is approved if the majority of validators (i.e. more than two-thirds) agree with the leader's block. If not, the following priority worker will take the lead and repeat the voting, aggregation, and fresh block generation. Algorand thus ensures the accuracy and integrity of the aggregate by guaranteeing that any malicious aggregation result can be rejected. The global model is updated with the aggregated version, which is stored in the blockchain as a hash of the model's parameters. The leader then disperses the updated version to all local peers in preparation for the upcoming training cycle. Their neighbouring peer in the blockchain network will lead the subsequent round of global model generation based on who is best accurate in the last-generated global model. Overall processes maintain the following steps:

- **Step 1**: Peers validate the reliability of transactions (i.e. local model blocks). Upon submission of the transaction Tx_i, r to the blockchain by a participant P_i^l, the peer verifies the digital signature of the uploaded transaction to ascertain that it originates from a legitimate participant. Subsequently, the peer forwards the verified transactions to the blockchain's leaders for consensus.
- **Step 2**: The elected leader generates a new block and executes the aggregation operation. The Algorand consensus algorithm selects a leader who, once all participants have uploaded their locally trained models, computes the aggregation value using model parameters obtained from DFS.
- **Step 3**: Lastly, a consensus mechanism is used to validate the aggregated model, which then generates a version of the global model. So, for the following round, it moves on to the local peers.

$$M_i^G = \frac{1}{D} \sum_{i=1}^{n} M_i^l. \tag{2}$$

3.5 | Differential privacy (DP)

Incorporating DP parameter into a local model is intended to reduce the accuracy and diversity of models by introducing stochastic variations. Although the installation of DP does modify the model, its impact on the pattern is anticipated to be negligible. Maintaining the secrecy of the underlying model is advantageous, as recent research has shown the possibility of retrieving original data from the ML model [10]. DP allows technology businesses to collect and distribute aggregated data about user activities while also protecting the privacy of individual users. This research employs DP to ensure the confidentiality of data while engaging numerous stakeholders in collaborative learning. We integrate a FL system with DP capabilities to safeguard data from both external and internal sources, such as analysts, during the training process. Its robust security features make it highly recommended in both academia and industry. As an illustration, RaPPOR employed DP in the Google Chrome browser [33] with a reduced privacy parameter. A randomised algorithm f provides (ϵ, δ) differential privacy if their neighbouring datasets D and $\acute{D}$ and f confirm that

$$Pr[f(D) \in Y] \leq e^{\epsilon} Pr[f(\acute{D}) \in Y] + \delta.$$

Here, δ is included to accommodate the likelihood (Pr) of violating plain ϵ-DP [34]. The variable Y traverses all subsets of the output range of mechanism f. When the value of δ is equal to zero, the mechanism f achieves ϵ–differential privacy. Let's say a SH wants to publish the average uses of electricity units to researchers in a privacy-preserving manner. So, they employ a deferentially private randomised algorithm that adds noise to the exact average.

The actual dataset D includes a one-month record and $\acute{D}$ is a neighboring dataset where $\acute{D}$ is only one day data difference. The value of $f(D) = 5$ and $f(\acute{D}) = 5.1$ before adding noise. After adding Laplace noise $b = 1/\epsilon$ where $\epsilon = 0.5$ and $\delta = 0$ based on equation the value $f(D) = 4.7$ or close to 5 and $f(\acute{D}) = 5.4$ or close to 5.1. Hence the equation,

$$Pr[f(D) = 5.2] \leq e^{\epsilon} Pr[f(\acute{D} = 5.2]$$

will be as below while $\epsilon = 0.5$ and

$$0.3 \leq 0.4616.$$

Hence, if we fix $\delta = 0.01$, it will create vary less impact on model parameters but will ensure privacy by changing real-value.

4 | EVALUATIONS AND ANALYSIS

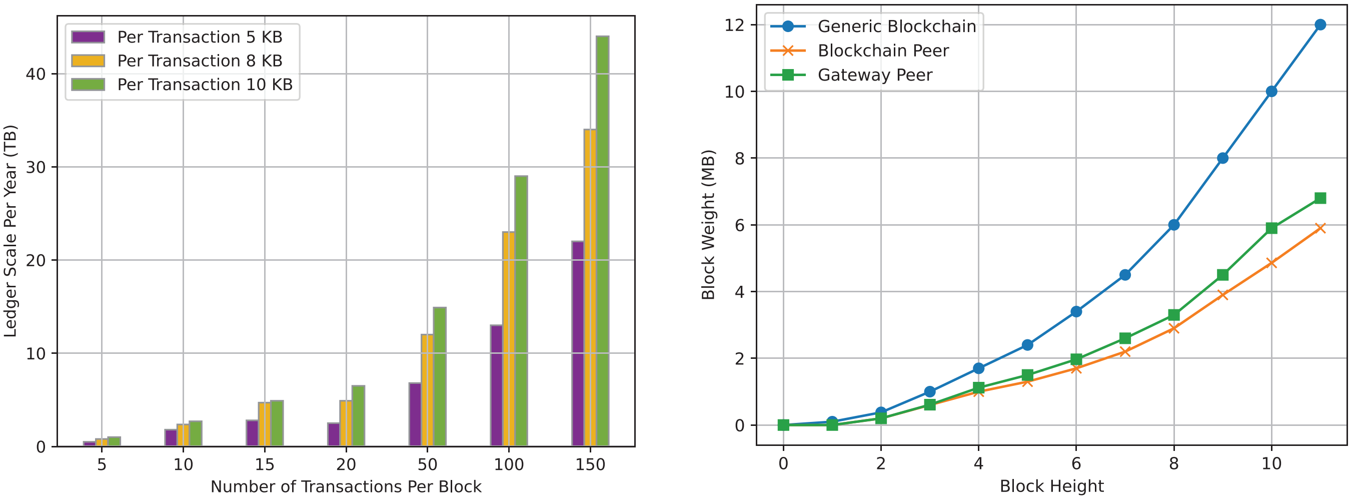
We evaluated the performance of the proposed BPFL framework on two experimental platforms. Initially, we tested the identification of ledger optimisation issues in BCN without the use of machine learning. This typical BCN-related experiment is evaluated on the Hyperledger Fabric (v2.0) platform, utilising a Docker container platform. It helps to predict a real-life application's software-based implementation. As machine learning application implementation in Hyperledger Fabric is a complicated task, we simulated it in a Python environment again to evaluate the whole ecosystem performance (details in Section 4.3).

4.1 | Stand-alone blockchain applications

Every individual peer carries out the ML execution procedures using the NVIDIA GeForce RTX 2080 GPU. At first, various local training settings utilised private servers equipped with four GPUs. Each GPU operates as a separate learning node for experimental purposes. Concurrently, the central processing unit (CPU) of a private server functions as a participant in the blockchain network. The blockchain network comprises six peers operating on the Docker container platform and implemented on an Intel Xeon E7 v3/CoreTM i7-5960X CPU running at a frequency of 3.00 GHz, 8 cores, and 125 GB of RAM. The blockchain network and consensus procedure are emulated using Python 3.8.

4.2 | Scalability evaluation

The summary of ledger growth and ledger scalability is shown in Figure 4. It assesses the effects on BC Ledger's ledger expansion as well as the execution of continuous transactions in the BC network. Figure 4a shows a typical blockchain experimental



(a) Memory Optimisation Effect

(b) Leger Scalability in Proposed Framework

FIGURE 4 Scalability impact on local peer implementation.

evaluation. We observed that each transaction frequently consumes up to 10 KB, that blocks generate 500 transactions per second on average, and that the size of block headers is 4.5 KB. We estimate the growth at a rate of approximately 50–100 KB/s, which translates to 4–8 GB/day or 1.5–3 TB/year. This becomes unworkable in a 10,000-house network with 20 gadgets per home, even though it doesn't appear to be a huge amount for a single node. Figure 4a shows a summary of the ledger growth for 1000 SHs on a blockchain network, with approximately fifteen devices per home. It demonstrates three possible outcomes that highlight how transaction weight could differ among sources based on format. For this test, we thought of three distinct sizes: 5–7 KB, 8–9 KB, and 10–12 KB. The size of a transaction and its amount determine the size of the ledger.

A simulated application based on node-red distributes transactions from 1000 SHs to gateway peers at random. The gateway peers categorise the transactions based on their intended destinations. Which means if a device D_i from $\mathrm{SH_i}$ sends a transaction to another device of $\mathrm{SH_i}$ $\mathrm{GW_i}$ processed itself otherwise forward to BCN. Figure 4b shows how transactions are transferred and the ledger growth in a generic blockchain where the gateway is not present. It also shows ledger growth in comparison to the proposed framework, specifically in the gateway peer for local transactions and the BCN ledger. Here gateway peers store multiledgers. As shown in Figure 4b, the presence of a gateway peer reduces burden almost 60% in comparison to generic blockchain from 4th block to subsequent blocks. Hence, it reduces the transaction execution cycle with the same percentages that scales the ecosystem execution performance by 60%. The system evaluates the next 10 blocks in both the gateway peer and blockchain networks. In the absence of a gateway peer, generic BCN must handle every local transaction generated from $\mathrm{SH_i}$ which creates overburden on BCN.

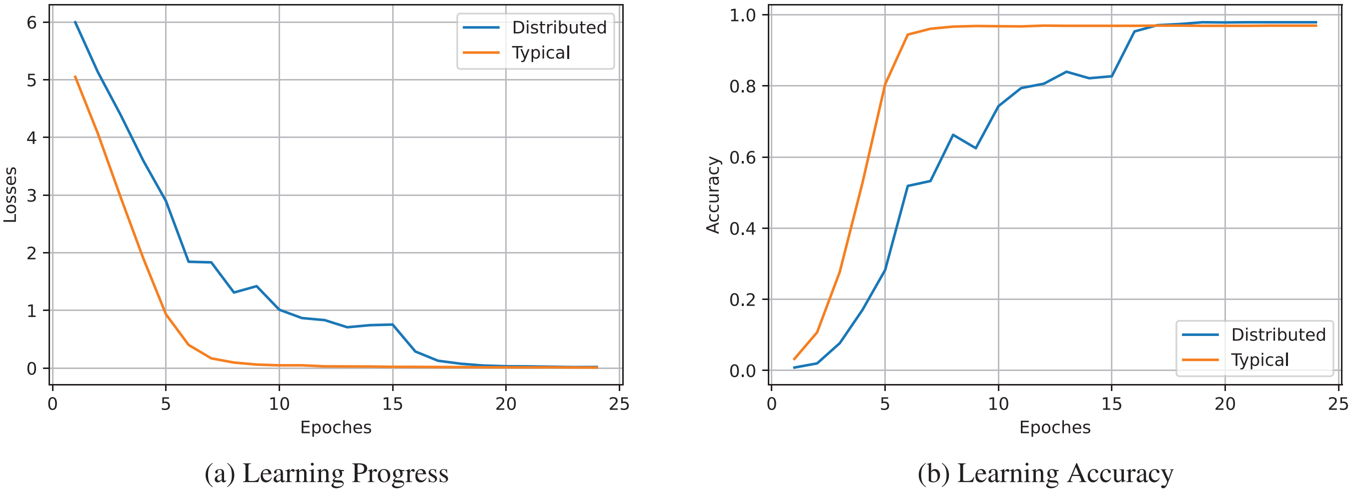
4.3 | Prediction analysis

4.3.1 | Using image dataset

The overall performance of the ecosystem is evaluated using a popular public Stanford Cars Dataset [35] that contains 16,185 images, including 8,144 training and 8,041 test images for 196 classes of cars. To prepare a balanced dataset for every user, we split the overall training and test sets equally based on their classes. The same customised dataset is used in typical FL without blockchain for baseline understanding. Furthermore, to fix the baseline, we extend the same experimental setup with a stand-alone approach using typical ML where parameters are used in the FL-integrated BPFL system.

We used the SGD optimiser and a 0.01 learning rate to train the model on a ResNet50 model that had already been trained to do classic image classification. The local training process was finished in the gateway peer of each SH. Each local learning node uses GPU services for local training independently. Simultaneously, the CPU of a private server acts as a gateway peer to evaluate the blockchain execution process. The blockchain network consists of ten peers running in a Docker container environment. A well-designed CNN network contains hidden layers for feature extraction and fully connected layers for classification [36]. The network employs two hidden layers with 30 and 80 channels, respectively. The dimension is lowered for output by utilising the Max-pooling layer. Max-pooling layers enhance the rate of learning in the neural network. Normalisation is applied to each CNN layer, facilitating the calculation of sensitivity to identify the appropriate level of noise to introduce. This process also enhances the learning rate and regularises gradients, minimising the impact of distractions and outliers.

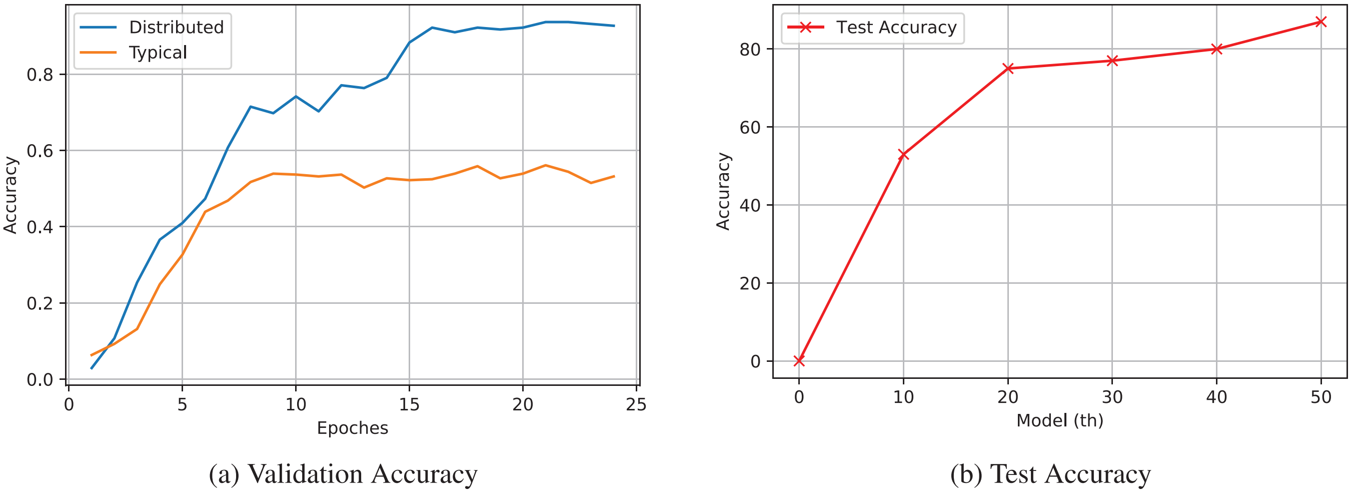
The suggested BPFL framework's overall learning outcomes are shown in Figure 6. It demonstrates the efficacy of federated



(a) Learning Progress

(b) Learning Accuracy

FIGURE 5 Training outcomes.



(a) Validation Accuracy

(b) Test Accuracy

FIGURE 6 Validation and test evaluations.

learning-based distributed machine learning within the BPFL framework as ‘Distributed’, in contrast to conventional machine learning as ‘Typical’. As shown in Figure 5, the accuracy and training progress where six federated local learning nodes perform the experiment 100 rounds. Each local peer executes a split dataset, while the FL network creates the global model by averaging the insights generated by various local nodes. As shown in Figure 5a the loss rapidly decreases, which illustrates training success. Compared to our suggested approach, loss drops fast in the baseline (i.e. standard ML). But nearly at the conclusion of the same cycle (i.e. the 18th epoch), they arrive at a convergence point. Figure 5b presents the training accuracy, comparing the object detection model’s learning accuracy to baseline and common approaches. The outcome of the simulation indicates that the suggested framework converges with conventional methods nearly simultaneously.

Figure 6 also presents how the proposed system can classify the images compared to standard ML approaches. The proposed method is evaluated based on a validation dataset and testset. Figure 6a illustrates the validation accuracy based on the validation dataset. It shows that the proposed scheme can recognise the images 88% cases, which is approx. 30% better than standard ML. As distributed ML merging all local models which performing on full dataset while standard ML performing based on splitted dataset. Moreover, the ultimate goal of this experiment is to improve FL in terms of users’ data security and privacy. Some test images have been tested on the proposed framework-generated models, which have been illustrated in Figure 6b. We have used different global models generated by averaging the FL models to verify their accuracy in real-life scenarios. The figure shows 10th global model can classify almost 56% of images, and the last model (50th) can classify 86% of test images successfully. Therefore, the overall performance accuracy of the proposed distributed system is relatively better than traditional ML approaches. Moreover, BPFL enhances the scalable services in SH network.

4.4 | Smart home dataset

For evaluating the impact of the proposed architecture on IoT devices used in SH, we have developed an experimental platform for a SH network using the Node-Red application, which contains ten SH applications that forward data from an existing dataset by choosing randomly to the local peer. Local peer is developed on the Docker container platform. Other core blockchain peers were also developed on the Docker container platform. We have used ten blockchain peers for maximum participation in consensus mode. The dataset used from a public source (e.g. Kaggle) contains 503K and 31 features that contain various home appliances used for energy data. We split the full dataset equally for every SH, as our ultimate goal is to justify the effectiveness of the framework. The suggested architecture's accuracy in model testing, network performance metrics, and local peer setup are all confirmed by the simulation platform.

An input layer, an output layer, and eight hidden layers make up the Deep Neural Network (DNN) model that serves as the training model for the BPFL and baseline techniques. We set the batch size to 64 and the learning rate of the model to 0.01. The model tunes the local training epochs to 10, while setting the FL and suggested training epochs to 15. Furthermore, the training epochs are immediately set to 150 by the local training. This experiment investigates three scenarios within the BPFL framework: standard ML with a split dataset, typical FL without the full function of the Gateway peer in the BPFL framework, and FL with the full function of Gateway peers. Typical FL's training accuracy is lower because it doesn't incorporate all local transactions from Gateway peers, which ultimately control the transaction flow. Similarly, typical machine learning (ML) exhibits lower accuracy due to its performance on split datasets. The purpose of this control is to enhance the performance of blockchain scalability, which most consortiums undertake. The distributed line illustrates the full performance features of the BPFL framework, which includes a complete dataset before segregating transactions at the gateway peer. Here, the gateway peer performs its regular function by extracting insights from transactions to create a local model, which in turn creates the global model.

The training accuracy shows that the convergence of BPFL is fairly steady, as shown in Figure 7. Moreover, it has shown a notable increase in model accuracy, outperforming the other two baseline methods by over 5%.

Tables 2 and 3 illustrates the amount of time taken to compute SH data in the BPFL system. We systematically increased the quantity of local peers in tandem with the fixed blockchain network peers. As a consensus team is formed with local peers and blockchain peers, consensus participants are also raised. For example, while the local peer is 7, the consensus participant is 17. The average execution time for local model building per epoch is almost consistent, regardless of the similar nature of local peers, as it averages the computation time. In contrast, the process of generating a global model for the same round takes slightly longer, as it is dependent on the number of consensuses. This process typically takes around 10 seconds for the network with 10 local and 10 BC peers, which is considered reasonable.

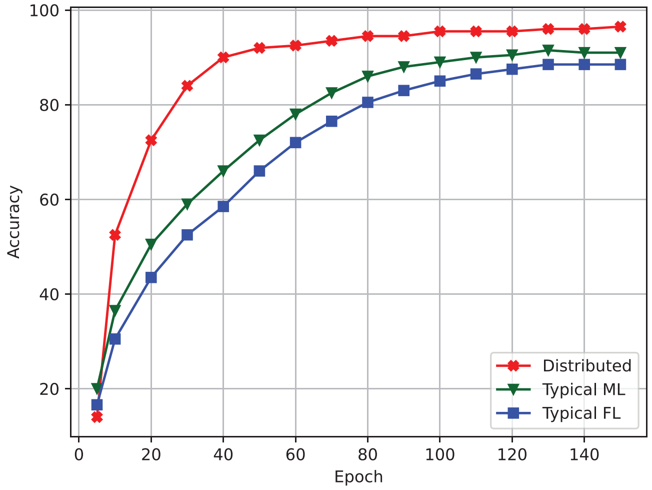


FIGURE 7 Training accuracy benchmarking.

TABLE 2 Symbols with labels.

Symbol	Meaning
Tx	Transaction from local peer.
B_i	Block generated at i^{th} local Peer P^l
L^{P^l}	BC ledger at local Peer
Tx^{dst}	Destination address of Tx
T^{src}	Source address of Tx
L^{Tx}	Consensus leader at BCN
D_i^n	n number of devices in i SH
$\mathtt{pk}_{\text{sign}}^{\rho_i}$	Public key with signature of users
υ	User
$\mathtt{sk}$	Secret key of υ of SH
M^l	Local model
M^g	Global model

TABLE 3 Computation time.

Local peers	BC peers	Time for local model (MS)	Time for global model (s)
3	10	786	3.2
5	10	795	6.36
7	10	865	7.65
10	10	846	9.78

The overall execution time of the global model encompasses the time required for model aggregation and consensus.

5 | CONCLUSION

SH users aim to enjoy the advantages of automation while maintaining their personal data safety and secrecy. In order to ensure the safety of the entire ecosystem, it is imperative to own the most up-to-date system. Furthermore, it is imperative to have stringent regulations in place for standard external services. The proposed framework includes safety protocols for automated forecasting and updated maintenance. Blockchain technology is being employed to address issues related to secure automation, and gateway peer serves to mitigate certain existing scalability challenges in blockchain. FL enhances security measures by preventing data exchange for machine learning purposes. The testbed results indicate that the contribution offers solutions to substantial issues that may arise from the integration of SH with blockchain and an intelligent automation system. The proposed BPFL significantly enhances scalability. It reduces ledger overhead by over 60% compared to traditional procedures that ultimately enhance the scalability of the ecosystem. It formulates a practical and secure approach for managing the ongoing data generated by SH. Moreover, the outcome shows the computation time is also reasonable, which is within 10 seconds for a 20-peer network. Overall, BPFL opens up a new path, leveraging distributed learning approaches and generating new advanced models with the latest data for manufacturers without compromising end-user security. This research will be applied to predictive maintenance by ensuring higher accuracy and runtime network service monitoring based on end users' feedback ratings.

AUTHOR CONTRIBUTIONS

Sujit Biswas: Writing—original draft; writing—review and editing. **Kashif Sharif**: Conceptualization; supervision; writing—review and editing. **Zohaib Latif**: Validation. **Mohammed J. F. Alenazi**: Writing—review and editing. **Ashok Kumar Pradhan**: Formal analysis. **Anupam Kumar Bairagi**: Writing—review and editing.

CONFLICT OF INTEREST STATEMENT

The authors declare no conflicts of interest.

DATA AVAILABILITY STATEMENT

Data openly available in a public repository (Available at https://github.com/nguyentruonglau/stanford-cars and DOI: https://doi.org/10.1109/CVPR.2015.7299023).

ORCID

Sujit Biswas https://orcid.org/0000-0002-6770-9845

REFERENCES

1. Revenue of the smart home industry worldwide 2019-2028 (2023). https://www.statista.com/forecasts/887554/revenue-in-the-smart-home-market-in-the-world
2. Lee, Y.T., Hsiao, W.H., Huang, C.M., Chou, S.C.T.: An integrated cloud-based smart home management system with community hierarchy. IEEE Trans. Cons. Electron. 62(1), 1–9 (2016)
3. Lakhan, A., Sodhro, A.H., Majumdar, A., Khuwuthyakorn, P., Thinnukool, O.: A lightweight secure adaptive approach for internet-of-medical-things healthcare applications in edge-cloud-based networks. Sensors 22(6), 2379 (2022). https://www.mdpi.com/1424-8220/22/6/2379
4. Yang, J., Zou, H., Jiang, H., Xie, L.: Device-free occupant activity sensing using wifi-enabled iot devices for smart homes. IEEE Intern. Things J. 5(5), 3991–4002 (2018)
5. Dawadi, P.N., Cook, D.J., Schmitter Edgecombe, M.: Automated cognitive health assessment from smart home-based behavior data. IEEE J. Biomed. Health Inf. 20(4), 1188–1194 (2016)
6. Mukherjee, A., Balachandra, M., Pujari, C., Tiwari, S., Nayar, A., Payyavula, S.R.: Unified smart home resource access along with authentication using blockchain technology. Glob. Trans. Proc. 2(1), 29–34 (2021)
7. Wu, Q., Chen, X., Zhou, Z., Zhang, J.: Fedhome: Cloud-edge based personalized federated learning for in-home health monitoring. IEEE Trans. Mob. Comput. 21(8), 2818–2832 (2022)
8. Biswas, S., Sharif, K., Li, F., Nour, B., Wang, Y.: A scalable blockchain framework for secure transactions in iot. IEEE Intern. Things J. 6(3), 4650–4659 (2019)
9. Dinh, C.T., Tran, N.H., Nguyen, T.D., Bao, W., Balef, A.R., Zhou, B.B., et al.: Done: Distributed approximate newton-type method for federated edge learning. IEEE Trans. Parallel Distr. Syst. 33(11), 2648–2660 (2022)
10. Zhu, T., Ye, D., Wang, W., Zhou, W., Yu, P.S.: More than privacy: Applying differential privacy in key areas of artificial intelligence. IEEE Trans. Knowl. Data Eng. 34(6), 2824–2843 (2022)
11. Zhao, Y., Zhao, J., Jiang, L., Tan, R., Niyato, D., Li, Z., et al.: Privacy-preserving blockchain-based federated learning for iot devices. IEEE Intern. Things J. 8(3), 1817–1829 (2021)
12. Ferenczi, A., Bădică, C.: Fully decentralized privacy-enabled federated learning system based on byzantine-resilient consensus protocol. Simul. Model. Pract. Theor. 136, 102987 (2024). https://www.sciencedirect.com/science/article/pii/S1569190X24001011
13. Hei, X., Yin, X., Wang, Y., Ren, J., Zhu, L.: A trusted feature aggregator federated learning for distributed malicious attack detection. Comput. Secur. 99, 102033 (2020)
14. Zhu, B., Lu, K., Tao, T.: A blockchain-based federated learning for smart homes. In: 2023 4th International Conference on Information Science, Parallel and Distributed Systems, ISPDS 2023. IEEE, Piscataway (2023)
15. Lin, C., He, D., Kumar, N., Huang, X., Vijayakumar, P., Choo, K.K.R.: Homechain: A blockchain-based secure mutual authentication system for smart homes. IEEE Intern. Things J. 7(2), 818–829 (2019)
16. Khan, M.A., Abbas, S., Rehman, A., Saeed, Y., Zeb, A., Uddin, M.I., et al.: A machine learning approach for blockchain-based smart home networks security. IEEE Netw. 35(3), 223–229 (2021)
17. Zhao, Y., Zhao, J., Jiang, L., Tan, R., Niyato, D., Li, Z., et al.: Privacy-preserving blockchain-based federated learning for iot devices. IEEE Intern. Things J. 8, 1817–1829 (2021)
18. Jung, S.S., Lee, S.J., Euom, I.C.: Delegation-based personal data processing request notarization framework for gdpr based on private blockchain. Appl. Sci. 11(22), 10574 (2021)
19. Biswas, S., Sharif, K., Li, F., Latif, Z., Kanhere, S.S., Mohanty, S.P.: Interoperability and synchronization management of blockchain-based decentralized e-health systems. IEEE Trans. Eng. Manage. 67(4), 1363–1376 (2020)
20. Arif, S., Khan, M.A., Rehman, S.U., Kabir, M.A., Imran, M.: Investigating smart home security: Is blockchain the answer? IEEE Access 8, 117802–117816 (2020)
21. Dorri, A., Kanhere, S.S., Jurdak, R., Gauravaram, P.: Blockchain for iot security and privacy: The case study of a smart home. In: 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), pp. 618–623. IEEE, Piscataway (2017)
22. Lin, C., He, D., Kumar, N., Huang, X., Vijayakumar, P., Choo, K.K.R.: Homechain: A blockchain-based secure mutual authentication system for smart homes. IEEE Intern. Things J. 7(2), 818–829 (2020)
23. Khan, M.A., Abbas, S., Rehman, A., Saeed, Y., Zeb, A., Uddin, M.I., et al.: A machine learning approach for blockchain-based smart home networks security. IEEE Netw. 35(3), 223–229 (2021)
24. Kim, D.: A reverse sequence hash chain-based access control for a smart home system. In: 2020 IEEE International Conference on Consumer Electronics (ICCE), pp. 1–4. IEEE, Piscataway (2020)
25. McMahan, B., Moore, E., Ramage, D., Hampson, S., Arcas, B.A.Y.: Communication-Efficient Learning of Deep Networks from Decentralized Data. In: Singh, A., Zhu, J. (eds.) Proceedings of the 20th International Conference on Artificial Intelligence and Statistics, vol. 54, pp. 1273–1282. PMLR, New York (2017)

26. Ramanan, P., Nakayama, K.: Baffle: Blockchain based aggregator free federated learning. In: 2020 IEEE International Conference on Blockchain (Blockchain), pp. 72–81. IEEE, Piscataway (2020)
27. Sun, J., Wu, Y., Wang, S., Fu, Y., Chang, X.: Permissioned blockchain frame for secure federated learning. IEEE Commun. Lett. 26(1), 13–17 (2022)
28. Otoum, S., Ridhawi, I.A., Mouftah, H.: Securing critical iot infrastructures with blockchain-supported federated learning. IEEE Intern. Things J. 9(4), 2592–2601 (2022)
29. Zhang, W., Lu, Q., Yu, Q., Li, Z., Liu, Y., Lo, S.K., et al.: Blockchain-based federated learning for device failure detection in industrial iot. IEEE Intern. Things J. 8(7), 5926–5937 (2021)
30. Shen, M., Wang, H., Zhang, B., Zhu, L., Xu, K., Li, Q., et al.: Exploiting unintended property leakage in blockchain-assisted federated learning for intelligent edge computing. IEEE Intern. Things J. 8(4), 2265–2275 (2021)
31. Qi, J., Lin, F., Chen, Z., Tang, C., Jia, R., Li, M.: High-quality model aggregation for blockchain-based federated learning via reputation-motivated task participation. IEEE Intern. Things J. 9(19), 18378–18391 (2022)
32. Gouget, A., Patarin, J., Toulemonde, A.: Unpredictability properties in algorand consensus protocol. In: 2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), pp. 1–3. IEEE, Piscataway (2021)
33. Erlingsson, U., Pihur, V., Korolova, A.: Rappor Randomized aggregatable privacy-preserving ordinal response. In: CCS '14: Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, pp. 1054–1067. Association for Computing Machinery, New York (2014).
34. Dwork, C., McSherry, F., Nissim, K., Smith, A.: Calibrating noise to sensitivity in private data analysis. In: Halevi, S., Rabin, T. (eds.) Theory of Cryptography, pp. 265–284. Springer, Berlin Heidelberg (2006)
35. Yang, L., Luo, P., Loy, C.C., Tang, X.: A large-scale car dataset for fine-grained categorization and verification. 2015 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), pp. 3973–3981 (2015)
36. Islam, M.M., Islam, M.Z., Asraf, A., Al Rakhami, M.S., Ding, W., Sodhro, A.H.: Diagnosis of covid-19 from x-rays using combined cnn-rnn architecture with transfer learning. BenchCouncil Trans. Benchmarks Standards Eval. 2(4), 100088 (2022). https://www.sciencedirect.com/science/article/pii/S2772485923000054

How to cite this article: Biswas, S., Sharif, K., Latif, Z., Alenazi, M.J.F., Pradhan, A.K., Bairagi, A.K.: Blockchain controlled trustworthy federated learning platform for smart homes. IET Commun. 1–13 (2024). https://doi.org/10.1049/cmu2.12870