I.J. Information Engineering and Electronic Business, **2026, 4, 72-92**
Published Online on August 8, 2026 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijieeb.2026.04.05

Privacy Preserving Federated Learning with Blockchain for Validating and Enhancing Technology Business Incubation Performance Prediction Models

Azhar Naeem*
Department of Management Sciences, Sir Syed CASE Institute of Technology, Islamabad 45100, Pakistan
E-mail: aazharnaeem@gmail.com
ORCID iD: https://orcid.org//0009-0000-1407-4957
*Corresponding author

Muhammad Umer
Department of Management Sciences, Sir Syed CASE Institute of Technology, Islamabad 45100, Pakistan
E-mail: mumer@case.edu.pk
ORCID iD: https://orcid.org//0000-0001-5425-5293

Received: April 30, 2025; Revised: June 9, 2025; Accepted: December 22, 2025; Published: August 8, 2026

Abstract: Technology Business Incubation (TBIs) has become a global phenomenon integral to the growth of regional innovation and startup ecosystems. The availability of high-quality infrastructure and facilities lays the foundations of the entire startup ecosystem for providing essential support services that directly impact entrepreneurial success. The incubation capacity of TBIs across different regions can foster competition and collaboration among these regions, provide avenues for enhancing enterprises' incubation capabilities, and assist entrepreneurs in assessing the strength of regional incubation. However, with their rapid expansion, the performance evaluation also becomes increasingly complex due to the diversity of converging factors such as complex technologies, varying nature of relationships of VCs, and entrepreneurial competencies of the founders incubating startups at the TBIs. Traditional Machine Learning performance evaluation and prediction models struggle to capture these dynamic variables, while also suffering from privacy vulnerabilities, low accuracy, and reliance on centralized third parties. This often leads to single points of failure, performance bottlenecks, and sometimes increased costs. To address these challenges, we employed Privacy-Preserving Federated Learning with Blockchain (PPFL-BC), a novel framework designed for improving the mechanism of performance measurement and prediction for remote TBIs while ensuring that the privacy of entities and the data remains secure. We utilize capabilities of Artificial Neural Network (ANN) and gradient boosting-enabled federated learning to train the model of each TBI locally. In the process, no private and sensitive business data is shared outside the network, significantly reducing the risk of privacy breaches. Besides this, all the locally trained models are aggregated into a unified predictive model at the central aggregation unit, which ultimately improves the overall accuracy of the performance prediction mechanism for the entire population of TBIs. In our model, the decentralized blockchain network is also used to address security concerns related to unauthorized access and data manipulation thereby ensuring transparent and tamper-proof model updates. We evaluate the performance of our proposed PPFL-BC model by utilizing real-world business incubation datasets. The simulation results show that our model outperforms the centralized performance prediction models in terms of accuracy, precision, recall, and F1-score. The results show that the proposed PPFL-BC model outperforms benchmark models with an accuracy of 84% and precision of 0.92, which shows the efficiency and reliability of our model in predicting and validating TBI success rates.

Index Terms: Blockchain, Federated Learning, Machine Learning, Performance Prediction, Technology Business Incubation.

1. Introduction

Technology Business Incubators (TBIs) serve as hubs for innovation and economic growth, equipping startups with the critical resources required to grow and compete at a global scale. By offering funding, workspace, expert mentorship, and networking opportunities, TBIs create a dynamic ecosystem where bold and dynamic entrepreneurs transform ideas into impactful solutions, driving technological advancement and disrupting the market [1]. In today's rapidly digitalizing landscape, the ecosystem of incubated startups is expanding at an unprecedented pace. As a result, stakeholders are becoming increasingly interested in accurate and efficient prediction of their performance to ensure their long-term success and sustainability [2]. Many traditional tools, such as balance scorecards are used for performance evaluation by linking strategic objectives with ultimate outcomes across various interconnected domains such as financial, the startups being incubated, and organizational processes employed to manage the TBIs [3]. However, these conventional mechanisms are lagging in efficiently capturing the dynamic nature of evolving TBI ecosystems, involving diverse factors of fast-changing technology, the disruptions shaping new business models, evolving market trends, the growing number of venture capitalists, and the improving entrepreneurial competencies of the founders from the different regions working on disruptive and exponential technologies [4].

Many Artificial Intelligence (AI) and Machine Learning (ML) based techniques such as Artificial Neural Networks (ANNs), Support Vector Machines (SVM), and Ensemble Learning methods like Random Forest and XGBoost are used for predicting the performance of TBIs. These techniques autonomously predict the performances of TBIs by analyzing their complex patterns and relationships within vast datasets [5, 6]. However, these techniques have a central model aggregation structure, where sensitive and important information about startups and incubators is aggregated on a central server for model training. The individual startup needs to send its sensitive information such as funding details and growth indicators, which raises the issues of unauthorized access and data breaches [7]. Furthermore, the network becomes vulnerable to data biases, which limits the generalizability of models across different incubation environments. Therefore, there is a need for an advanced predictive model that can not only efficiently forecast the performance of business incubation centers but also preserve users' sensitive information [8].

To solve these aforementioned issues, we propose a Privacy-Preserving Federated Learning with a Blockchain (PPFL- BC) model for efficient and reliable validation of performance prediction models of TBIs. In our proposed model, federated learning is used for collaborative model training across different TBIs without sharing raw data such as financial metrics, startup valuations, or intellectual property details [9]. The data remains secure at the respective TBI and a local model is trained at the virtual machine of that TBI [10]. After that, only model updates such as gradient vectors and model weights are sent to a central parameter server for aggregation [11]. This helps in solving the issue of privacy leakage while simultaneously enabling the development of predictive models for Key Performance Indicators (KPIs) such as success rates, funding details, and market penetration [12]. As the models are locally trained at local virtual machine, this minimizes data heterogeneity and sampling bias, which ultimately enhances the accuracy and generalizability of the performance prediction model [13]. Besides this, a unified model is generated by utilizing the dataset of multiple incubators, this enhances the robustness of scorecard systems, which ultimately enhances the predictive performance and reliability of scoring metrics [14].

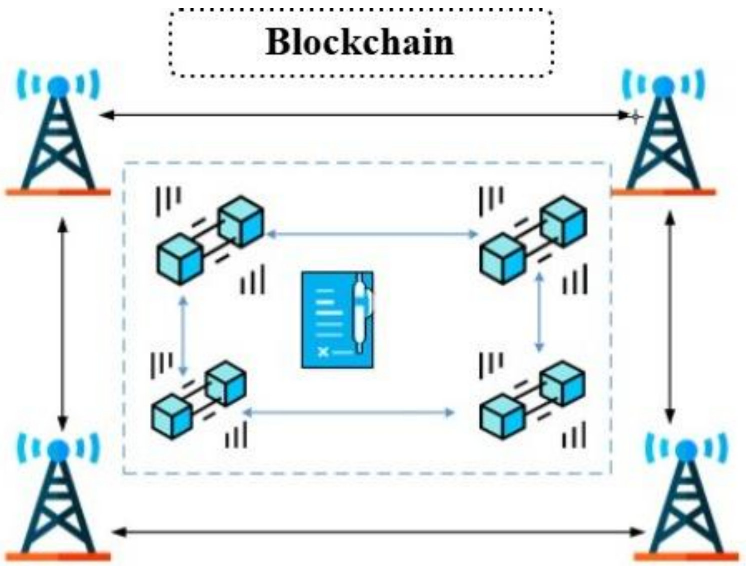

Fig. 1. A General Blockchain Layered Architecture.

Furthermore, existing performance prediction models rely on centralized or third parties for their various operations such as data storage, model aggregation, and result validation [5, 6]. These models are vulnerable to multiple issues such as single point of failure, performance bottlenecks, and extra costs due to the involvement of third parties [15]. Blockchain is a decentralized protocol that operates without the involvement of any third party. All the entities of this network act as the foundation of the network and can monitor the activities of each other [16]. The blockchain ensures the traceability and accountability of various TBIs which ultimately minimizes the issues of model tampering and privacy leakage [17].

Furthermore, encryption techniques such as symmetric and asymmetric encryptions are used in blockchain to protect the data from a breach [18]. The blockchain network also utilizes the capabilities of various hashing algorithms to ensure data integrity. Various consensus algorithms such as Proof of Work (PoW) and Proof of Stake (PoS) are used in blockchain to develop consensus among remote network entities [19, 20]. The structure of the blockchain network is shown in figure 1. The research objectives of our proposed model are given below:

- To design a PPFL-BC model for secure and reliable decentralized model training while simultaneously preserving the privacy of TBIs.
- To integrate blockchain with a decentralized model for ensuring data accountability and integrity.
- To enhance the accuracy and generalibzilty of the prediction model by decentralized model aggregation.
- To optimize communication and scalability of the proposed model by utilizing the capabilities of advanced federated learning algorithms such as federated averaging and federated optimization.

The key contributions of our paper are as follows:

- A PPFL-BC model is proposed that utilizes the capabilities of Federated Learning for local model training and Blockchain for secure and transparent model aggregation. This model efficiently enhances the performance of prediction models while simultaneously preserving the privacy of TBIs.
- The edge and cloud computing are used to enhance the computational efficiency, real-time processing, and scalability of the prediction model.
- The smart contract-based automated data aggregation model is proposed that not only enhances the security and efficiency of the decentralized model training process but also enables decentralized data aggregation without exposing sensitive information.

2. Related Work

The science and technology-based business incubators play a significant role in the development of high-quality products, which ultimately enhances the innovation capacity of any respective region. Chunyan et al. state that existing studies are not able to efficiently evaluate the incubation capacity of science and technology-based incubators [21]. Therefore, they propose a mechanism in which the incubation capacity of incubators is evaluated by establishing an index system. This index system utilizes the capabilities of investment services, resource services, and overall performance of incubators for evaluating the capabilities of these above-mentioned incubators. Furthermore, the authors propose an integrated weight method by combining the entropy method with the DEMA-TEL method, which helps in the identification of various weights of attributes. This proposed model can more efficiently capture the relative value of indicators as compared to existing techniques. This proposed mechanism not only mitigates the subjective biases but also minimizes the objective-based bias, which ultimately helps in the determination of more effective and reliable weights. Besides this, the relative positions of alternatives are reflected with similarity order solutions without defining their relative position, and grey relation analysis is used to reflect similarity degree. Both these techniques are integrated to enhance the evaluation results, which ultimately improves the overall performance of the assessment process. The performance of the proposed model is evaluated while considering the factors of objective weights, integrated weights, incubation capacity, score ranking, and score value. However, the proposed model relies heavily on the accuracy of the index system, which is not able to capture all contextual factors influencing incubation capacity efficiently. Furthermore, the integration of multiple methods increases the complexity of the evaluation process, which ultimately affects the applicability and scalability in real-world scenarios. Similarly, Amir et al. state that there is no comprehensive framework that can efficiently measure the performance of business incubators [22]. Therefore, the authors propose a fuzzy interference system for evaluating the performance of business incubators. The criteria and sub-criteria are identified by using inputs from the Delphi panel. After that the criteria are properly weighted with a fuzzy logic-based hierarchy mechanism. This fuzzy interference system is applied to various criteria and sub-criteria of Irish business incubation centers to evaluate the performance of their proposed model. The results show that the proposed model can provide an accurate and reliable evaluation on six different criteria, which are client, finance, human capital, product and services, network and marketing, and facility and infrastructure. The performance of the proposed model is evaluated by simulating the whole environment in MATLAB. However, the proposed model is vulnerable to subjective biases due to reliance on the Delphi panel for criteria selection as the inputs are dependent on the expertise and perspectives of selected panel members. Besides this, the model has a large computational overhead due to the complexity of defining membership functions and rule sets, which ultimately affects the efficiency and real-time applicability of the proposed model. Prima et al. identified the same issue and stated that there are no advanced and reliable mechanisms for understanding the performance of business incubators along with their determinants [23]. Therefore, the authors propose a mechanism in which 23 statements are investigated for the identification of various factors that affect the performance of technology business incubators in Indonesia. The proposed model uses a knowledge-based perspective and structural modeling for mediating various variables and evaluating the impact of these variables on technology business incubators, respectively. The performance of the proposed model is evaluated while considering the factors of frequency, percentage of participants, composite reliability, average variance extracted, and Cronbach's Alpha. The results show that the proposed model is efficiently able to mediate fully and sometimes partially between the governance of incubators, overall funding support, the assistance of government, and the performance of technology business incubators. However, the proposed model is vulnerable to response biases due to high dependence on self-reported data of statements, which ultimately affects the accuracy and reliability of the identified factors. Furthermore, the model is only focused on technology business incubators in Indonesia, which limits its generalizability to other regions or types of incubators with different dynamics. Besides this many machine learning and deep learning-based techniques are also proposed for effectively identifying the performance of business technology incubators and proposing highly accurate classification models. Seyedeh et al. state that there are no effective studies to predict and simultaneously evaluate key performance indicators of construction projects to monitor and control their performances [24]. Therefore, the authors propose a deep learning-based artificial neural network model for predicting key performance indicators at different stages of the project. Furthermore, the capabilities of neuro-fuzzy techniques are utilized for automatically generating an initial fuzzy interference model. The proposed model is evaluated while considering the factors of R2 value, mean absolute percentage error, root relative squared error, and mean absolute error. However, the deep learning-based artificial neural network model requires a large amount of high-quality training data, which is not always easily available for all project stages. Moreover, the complexity of the neuro-fuzzy techniques used for generating the initial fuzzy inference model increases computational demands, potentially hindering real-time performance evaluation and scalability. Similarly, Similarly, Jiaming et al. [25] identified the same issue and stated that there is a need to find grained and instance-level fine information for the segmentation of images. All the existing schemes are only focused on the processing of the above-mentioned information while utilizing the capabilities of distinct and diverse output formats. Due to this, these schemes are not efficient in the detection of human-object interaction and are considered redundant. To solve these above-mentioned issues, the authors propose a mechanism in which all the fine-grained parsing tasks are solved by optimizing the category representation. It is also helpful in providing the simplest and most efficient solution for the detection of human-object interactions. Furthermore, correlation representation learning is used for extracting the category and instance features to provide a mechanism in which there is no need for a processing step and the model can produce human parsing results directly without large computational overheads. In the proposed model the category kernels are designed for maintaining category semantic

Table 1. Comprehensive Analysis of Existing Approaches: Challenges, Innovations, Evaluations, and Future Directions.

Addressed Limitations	Performance Parameters	Limitation
Existing studies are not able to efficiently evaluate the incubation capacity of science and technology-based incubators [21].	Objective weights, integrated weights, incubation capacity, score ranking, and score value	The proposed model relies heavily on the accuracy of the index system, which is not able to capture all contextual factors influencing incubation capacity efficiently.
There is no comprehensive framework that can efficiently measure the performance of business incubators [22].	Client, finance, human capital, product and services, network and marketing, and facility and infrastructure.	Model has large computational overhead due to the complexity of defining membership functions and rule sets, which ultimately affects the efficiency and real-time applicability of the proposed model.
There are no advanced and reliable mechanisms for understanding the performance of business incubators along with their determinants [23].	Frequency, percentage of participants, composite reliability, average variance extracted, and Cronbach's Alpha.	The proposed model is vulnerable to response biases due to high dependence on self-reported data of statements, which ultimately affects the accuracy and reliability of the identified factors.
There are no effective studies to predict and simultaneously evaluate key performance indicators of construction projects to monitor and control their performances [24].	R2 value, mean absolute percentage error, root relative squared error, and mean absolute error.	The deep learning-based artificial neural network model requires a large amount of high-quality training data, which is not always easily available for all project stages.
Existing schemes are only focused on the processing of category-level information while utilizing the capabilities of distinct and diverse output formats. So, they are inefficient in detecting human-object interaction [25].	Average precision based on part, params (MB), generalization, auxiliary loss, and accuracy.	Correlation representation and its application will be investigated by implementing them in different scenarios with different numbers of image samples.

consistency. Moreover, some category features are used for extracting the features of positive pixels, and the output of this feature is fed into the convolution layer without modifying their size, which ultimately helps in the normalization of features for obtaining the category-level features. The authors conducted the experiments to evaluate the performance of their system model. They assess the proposed representation learning approach while considering the datasets of MHPv2.0. There are 15403 images in this dataset, which are used for the training of the model, 2867 images are used for validation, and the rest 4946 images are used for testing purposes. The proposed model is compared with many state-of-the-art models in terms of average precision based on the part, params (MB), generalization, Auxiliary Loss, and accuracy. In the future, the authors plan to investigate correlation representation and its application by implementing them in different scenarios with different numbers of image samples.

3. Proposed Privacy-Preserving Performance Prediction Model

We propose the PPFL-BC model for providing a blockchain-based, decentralized, and robust mechanism for the prediction of the performance of TBIs. The proposed model does not only solve the issue of privacy leakage of TBIs but also ensures the security of data and scalability of the network while utilizing the capabilities of federated learning and blockchain [26]. We use ANN and gradient-boosting classification algorithms in our proposed federated learning based architecture, which enhances accuracy and generalizability while simultaneously minimizing the data biases across diverse and distributed data sources. Our proposed model is divided into five layers, which are the data preparation layer, metric calculation layer, blockchain layer, model training layer, and performance prediction layer, as shown in Figure 2. The workings of our layered architecture are described below.

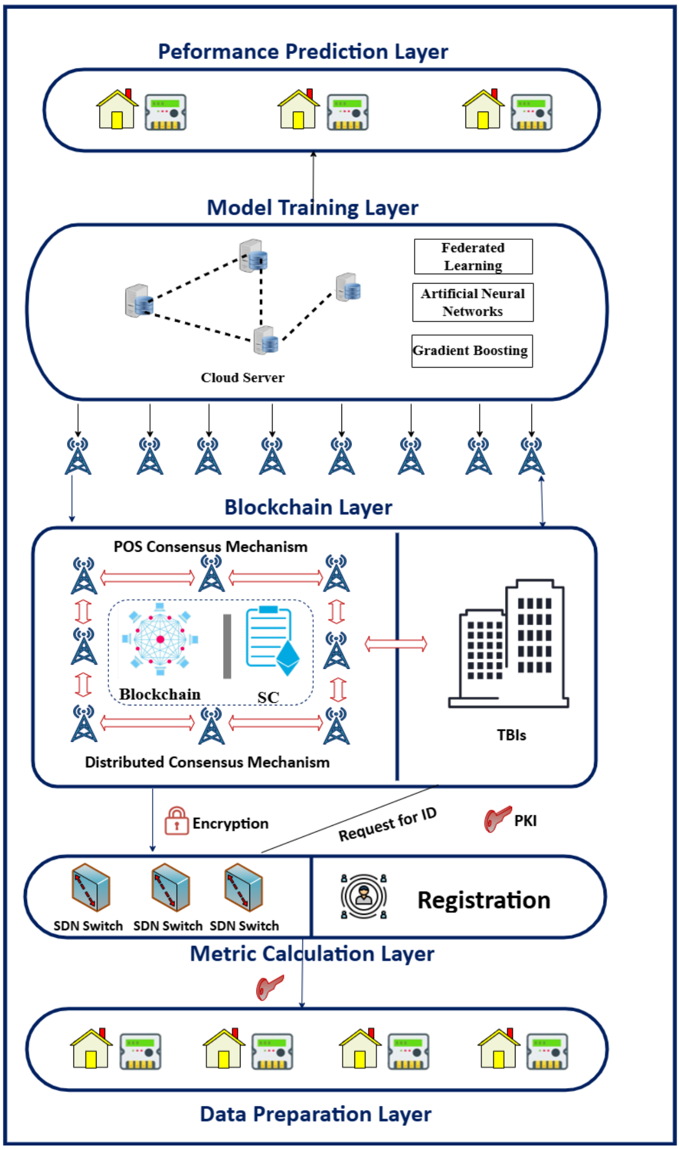

Fig. 2. Proposed Blockchained Federated Learning Model for TBI performance Prediction.

The first layer is the data preparation layer, which is responsible for collecting data from various distributed data sources, such as startups and TBIs. These data units act as clients in our proposed federated learning model. All the clients preserve their data on their local servers; this ensures that no raw data or sensitive information of the client is shared with any external entity, which ultimately ensures the privacy of data and compliance with data protection regulations. The balanced scorecard framework is used to structure the input data. This framework is very effective and provides effective and reliable performance evaluation of TBIs. The input data of TBIs is represented according to equation 1.

$$X = [p_1, p_2, p_3, p_4] \in R^{4\times 53} \tag{1}$$

Where p_1 , p_2 , p_3 , and p_4 are learning and growth, internal processes, customer, and financial perspectives, respectively. The target variable for performance prediction is the overall performance score represented by equation 2.

$$Y = [p_u] \in R^{1\times 53} \tag{2}$$

Where p_u represents the overall performance score, which acts as the dependent variable for predictive modeling. In our proposed model, various preprocessing techniques such as normalization, robust scaling, and outlier elimination are used to ensure the integrity and quality of input data. The overall performance score p_u is a continuous numerical variable computed internally by each incubator using a weighted aggregation of KPIs across financial, customer, internal process, and learning perspectives. The score is derived prior to model training and serves as the prediction target rather than a learned label, enabling supervised performance forecasting. We perform data normalization to scale the input features within a range of [0, 1], which ultimately helps in fast convergence in the training process. Besides this, we also utilize the capabilities of robust scaling to minimize the impact of outliers, which ensures the reliability and integrity of data collected from dispersed sources. In our proposed model, the Interquartile Range (IQR) method is also used for the detection of outliers. Furthermore, all the data beyond 1.5 times the IQR are removed, which ultimately enhances the accuracy of our model. The second layer of our proposed layered architecture is the metrics calculation layer, in which balanced scorecard metrics for all four perspectives are calculated. After this, we identify key performance indicators and quantify them concerning each perspective, which helps in the formation of input features for the predictive model. The key performance indicators of financial perspective (p_4) are assets, return on assets, and revenue per employee, which shows the financial performance of TBI quantitatively. Similarly, the key performance indicators of financial perspective (p_3) are the customer satisfaction index, market share, and customer loyalty index, which show all the customer-related outcomes. Besides this, the internal processes perspective (p_2) is used for evaluating the operational efficiency of the organization with the help of various metrics such as on-time delivery, productivity improvement, and decision-making time. Lastly, the capacity building of an organization is evaluated by the learning and growth perspective (p_1) with the help of investment in training, employee satisfaction, and innovation index. After the calculation of metrics for all four perspectives, we aggregate all the key performance indicators with the help of a weighted scoring model, as represented by equation 3.

$$S_j = \sum_{i=1}^{N} w_i \cdot k_{ij} \tag{3}$$

where S_j is the score for perspective j, w_i represents the weight assigned to KPI i, k_{ij} is the value of KPI i for perspective j, and N is the total number of KPIs within the perspective. The weights (w_i) are determined based on the judgment of experts and historical data analysis, which ultimately ensures that the most significant and reliable key performance indicators have the highest influence on the overall score. Furthermore, this weighted aggregation model not only helps in customization but also ensures that the performance evaluation has specific characteristics and priorities for each TBI. The workings of the PPFL-BC model, including data preparation, metric calculation, federated learning training, blockchain integration, and performance prediction are shown in algorithm 1.

The algorithm 1 begins with an initialization step where a set of clients C, representing TBIs, maintain local datasets $\mathbb{X}_i$ and $\mathbb{Y}_i$ without sharing raw data. The input features, structured using the balanced scorecard framework, consist of four perspectives: learning and growth (p_1), internal processes (p_2), customer (p_3), and financial (p_4). Data preprocessing is performed, including normalization using min-max scaling, robust scaling to mitigate the effect of outliers, and outlier removal using the IQR method. For each data point x, if it exceeds $Q_3 + 1.5 \times IQR$ or falls below $Q_1 - 1.5 \times IQR$, it is removed from the dataset. This ensures high data quality and improves the training process. Next, in the metric calculation phase, each key performance indicator (KPI) k_{ij} within the four perspectives is assigned a weight w_i, and the perspective score S_j is computed as $S_j = \sum_{i=1}^{N} w_i \cdot k_{ij}$, where N is the total number of KPIs in a given perspective. The final performance score p_u is then derived by aggregating the weighted KPI scores. The FL training phase involves each client i training a local model FL_i on its dataset ($\mathbb{X}_i, \mathbb{Y}_i$), computing model updates Δw_i, and sending them to a central aggregator. The global model weights w_{global} are updated as $w_{global} = \sum_{i\in C} \frac{n_i}{N} \cdot \Delta w_i$, ensuring proportional contribution from each client based on data size n_i. To enhance security, the blockchain layer verifies and records these updates as transactions $T = (FL_{version}, w_{global})$. If the transaction is validated by miner nodes, the local models are updated accordingly. Finally, the trained FL model is used for predicting the performance score p_u, and evaluation is performed using accuracy metrics. This architecture ensures data privacy, robustness, and scalability while preserving the integrity of predictive modeling.

Algorithm 1. Privacy-Preserving Performance Prediction Model (PPFL-BC)

Require: C: Set of clients ($TBIs$), FL: Federated Learning model, B: Blockchain network, M: Set of KPIs, X: Input data, $\mathbb{Y}$: Target variable

Initialization:
Clients maintain local datasets $\mathbb{X}_i, \mathbb{Y}_i$, where $i \in C$
Define balanced scorecard perspectives: p_1, p_2, p_3, p_4
Normalize input data $\mathbb{X}$ using min-max scaling
Apply robust scaling to mitigate outliers
Remove outliers using IQR method:
for each $x \in \mathbb{X}$ **do**
    if $> Q3 + 1.5 \times IQR \ or \ x < Q1 - 1.5 \times IQR$ **then**
        Remove *x* from $\mathbb{X}$
    end if
end for
Metric Calculation:
for each $p_j \in \{p_1, p_2, p_3, p_4\}$ **do**
    for each KPI $k_{ij} \in M$ **do**
        Compute KPI score: $S_j = \sum_{i=1}^{N} w_i \cdot k_{ij}$
        end for
end for
Aggregate KPI scores into final performance score p_u
Federated Learning Training:
for each client $i \in C$ in parallel **do**
    Train local model FL_i on $(\mathbb{X}_i, \mathbb{Y}_i)$
    Compute model update Δw_i
    Send Δw_i to central aggregator
end for
Aggregate updates: $w_{global} = \sum_{i \in C} \frac{n_i}{N} \cdot \Delta w_i$
Blockchain Integration:
Clients validate global model update w_{global}
Miner nodes append transaction $T = (FL_{version}, w_{global})$ to blockchain
If transaction verified, update local models
Performance Prediction:
Use final trained model FL to predict p_u
Evaluate using accuracy metrics
return Predicted performance scores for $TBIs$

The third layer of our model is the model training layer, which is responsible for decentralized model training while utilizing the capabilities of a federated learning algorithm [27]. Each client in this layer is responsible for training a model locally with its data. After training local models, each client transmits only model updates such as gradients or weights to the central aggregator unit [28]. As no actual data of TBIs is shared outside the ecosystem of TBIs and only model updates are shared with external aggregator entities. In this way, our proposed model preserves the privacy of TBI clients. Furthermore, model updates from all the clients are enriched with significant features of all locally trained models [29]. These model updates are fused into a unified prediction model, which has all the significant information, due to which the accuracy of our proposed federated learning prediction model is high as compared to all locally trained models. This unified model is then shared with each client of TBIs. In this way, our proposed model preserves the privacy of TBI clients while simultaneously ensuring the high accuracy of the prediction model [30]. The process of local model training is represented by equation 4.

$$\theta_k^{t+1} = \theta_k^t - \eta \nabla L(\theta_k^t; X_k, Y_k) \tag{4}$$

where θ_k^t shows the model parameters at client k at iteration t, η is the learning rate, and $\nabla L(.)$ is the gradient of the loss function. The input data and target labels for client k are denoted by X_k and Y_k, respectively. We use the Federated Averaging (FedAvg) algorithm for aggregation of local models, as shown in equation 5.

$$\theta^{t+1} = \sum_{k=1}^{K} \frac{n_k}{n} \theta_k^{t+1} \tag{5}$$

where K is the number of clients, n_k is the number of samples at client k, and n represents the total number of samples across all clients. This aggregation mechanism ensures that the unified global model is updated based on a weighted average of local model updates, which ultimately shows the contribution of each client concerning the size of its dataset [31]. Our federated learning model uses a hub-and-spoke topology, where the central server (hub) manages communication and model aggregation while multiple incubation centers (spokes) participate in model training. This topology ensures efficient and reliable model updates by collecting locally trained weights from edge devices and integrating them centrally. In this way, the scalability of our model is enhanced with very low computational overhead on individual incubation centers. The fourth layer of our proposed model is the blockchain layer, which is responsible for the secure and reliable aggregation of data while simultaneously ensuring the transparency of model updates [32]. The blockchain layer is designed to mitigate adversaries capable of model tampering, unauthorized update injection, and replay attacks. The attack surface includes poisoned model updates and integrity violations during aggregation. By enforcing immutable ledgers and consensus-based validation, the framework ensures traceability, accountability, and resistance against malicious update manipulation. In this layer, all the model updates of different clients are recorded as transactions, which ultimately ensures the traceability and accountability of data contributions. We use the Keccack-256 hashing technique to ensure the integrity of data while simultaneously preserving the privacy of network entities [33]. All the network entities are registered with the blockchian network and only authorized entities are allowed to access or modify the data. Furthermore, we Proof of Stake (PoS) hashing algorithm for developing consensus among distributed entities [34]. In our proposed model, different validator nodes are selected based on their cryptocurrency, reputation, and historical records. The validators are responsible for validating the performed transactions and adding the blocks to the blockchain [35]. This PoS consensus algorithm not only ensures consistency in the data transmission process but also reliability in a distributed network with potentially malicious nodes [36]. Each transaction in our proposed model is recorded according to equation 6.

$$T_i = H(\theta_k^{t+1} \mid T_{i-1}) \tag{6}$$

Where T_i is the current transaction, $H(.)$ is a Keccack-256 hash function, and T_{i-1} is the previous transaction, which ultimately ensures the immutability and chronological order of model updates. We also utilize the capabilities of smart contracts to automate various processes such as model aggregation, reward distribution, and compliance with privacy policies. As no third party is involved in monitoring transactions and record keeping; therefore, our blockchain-enabled prediction model not only enhances the trust among dispersed entities but also ensures data security within the decentralized federated Learning network [37]. The last layer of our proposed layered architecture is the performance prediction layer, which operates while utilizing the capabilities of ANN and gradient boosting methods. The ANN model models complex non-linear relationships between the input features and the target variable. The neural network is formulated according to equation 7.

$$\hat{Y} = f(W,X) = \sigma(W^{(L)}\sigma(W^{(L-1)} \ldots \sigma(W^{(1)}X + b^{(1)}) \ldots + b^{(L-1)}) + b^{(L)}) \tag{7}$$

Where W and b show the weights and biases of the neural network layers, σ is the activation function, and L is the total number of layers. Furthermore, the gradient boosting algorithm is used to enhance predictive accuracy by sequentially training weak learners and combining them into a strong ensemble model, as shown in equation 8

$$F_m(X) = F_{m-1}(X) + \eta \sum_{j=1}^{J} \gamma_j \, I(X \in R_{jm}) \tag{8}$$

Where F_m is the boosted model at iteration m, and $gamma_{j\,j}$ is the weight for each tree leaf R_{jm}. The combination of ANNs and gradient boosting enhances predictive accuracy, generalizability, and fairness by addressing data biases through a decentralized aggregation mechanism. The working of the decentralized model training and secure aggregation process is shown in algorithm 2. Our model utilizes blockchain capabilities to ensure the privacy of inferred data in federated learning. Blockchain secures model updates by immutably recording transactions, which ultimately prevents unauthorized access to the network. Besides this, the smart contracts ensures that only authorized nodes can access validated updates. The sensitive and important inferred data is secured by using model gradients before transmission. Furthermore, the issue of single points of failure is solved by distributed ledger, which ultimately enhances the integrity of data and trust among participants.

The algorithm 2 begins with the initialization phase, where all clients K register on the secure blockchain S using cryptographic identities. Smart contracts SC are deployed to automate processes such as model aggregation, reward distribution, and compliance enforcement. During each training round t, each client k updates its local model parameters θ_k^{t+1} using stochastic gradient descent, where the learning rate is denoted as η, and the loss function gradient is represented by $\nabla L(\theta_k^t; X_k, Y_k)$, where X_k and Y_k represent the input features and target labels for client k, respectively. To ensure privacy, clients encrypt their locally trained models before transmission. Additionally, each local update is hashed using the Keccak-256 cryptographic function $H(.)$, forming a transaction T_i where $T_i = H(\theta_k^{t+1} \mid T_{i-1})$. This ensures that every update maintains integrity and is tamper-proof by linking it to the previous transaction T_{i-1}. Once clients submit their model updates, validator nodes in the blockchain perform consensus using PoS mechanism. Validators are selected based on cryptocurrency holdings, reputation, and historical contributions. After verifying the legitimacy of each model update, the system aggregates all verified local models using the Federated Averaging (FedAvg) algorithm. The global model is computed as $\theta^{t+1} = \sum_{k=1}^{K} \frac{n_k}{n} \theta_k^{t+1}$, where n_k represents the number of data samples held by client k, and n denotes the total number of samples across all clients. The updated global model θ^{t+1} is then recorded on blockchain S to maintain transparency, ensuring that no single entity can manipulate the model updates.

After model training and aggregation, the algorithm proceeds with the performance prediction phase. It utilizes an ANN to learn complex non-linear relationships between input features and the target variable. The ANN prediction function is formulated as $\hat{Y} = \sigma(W^{(L)}\sigma(W^{(L-1)} \ldots \sigma(W^{(1)}X + b^{(1)}) \cdots + b^{(L-1)}) + b^{(L)})$, where W and b denote the weights and biases of different layers, L is the total number of layers, and $\sigma(.)$ is the activation function. Alongside ANN, a gradient-boosting algorithm is trained to enhance predictive accuracy. The gradient boosting model updates iteratively as $F_m(X) = F_{m-1}(X) + \eta \sum_{j=1}^{J} \gamma_j \, I(X \in R_{jm})$, where $F_m(X)$ is the boosted model at iteration m, γ_j is the weight of each tree leaf R_{jm}, and $I(X \in R_{jm})$ is an indicator function. Finally, a weighted ensemble model is formed by combining ANN and gradient boosting predictions using $\hat{Y} = \alpha F_m(X) + (1-\alpha)\hat{Y}_{ANN}$, where α is the weighting factor that balances contributions from both models. This hybrid approach improves prediction accuracy while mitigating biases present in individual models. The final outputs, θ^{t+1} and $\hat{Y}$, are then returned as the updated global model and performance prediction, ensuring privacy, transparency, and high predictive accuracy.

4. ANN and Gradient Boosting Methods

We propose a blockchain-based federated learning model for performance prediction and validation of TBIs while utilizing the capabilities of ANN and gradient-boosting classification algorithms. In our proposed model, the TBIs can train their local models without sharing their sensitive data outside their local network [38]. Furthermore, the blockchain not only ensures the secure and reliable aggregation of locally trained models but also enforces the privacy of network entities [39]. The use of blockchain also provides a temper-resistant environment to ensure the integrity and reliability of federated learning updates. It solves the issues of traditional prediction models such as frequent data breaches and model positioning attacks [40].

Algorithm 2. Federated Learning with Blockchain for Secure Performance Prediction

Require: K: Clients, S: Secure Blockchain, θ^t: Global Model, X_k, Y_k: Data at client k, $H(.)$: Keccak-256 Hash Function, η: Learning Rate, n_k: Samples at client k, n: Total Samples
Ensure: θ^{t+1}: Updated Global Model, $\hat{Y}$: Predicted Output

Step 1: Initialization
Clients register on blockchain S with cryptographic identities
Deploy Smart Contracts SC for transaction automation
for each training round $t = 1,2,\ldots,T$ **do**
  for each client $k \in K$ **in parallel do**
    Compute local update: $\theta_k^{t+1} = \theta_k^t - \eta \nabla L(\theta_k^t; X_k, Y_k)$
    Encrypt θ_k^{t+11} before transmission
    Generate hash for integrity: $T_i = H(\theta_k^{t+1} \mid T_{i-1})$
    Transmit T_i to blockchain S
  end for
  Validators perform consensus using Proof of Stake (PoS)
  Aggregate verified model updates: $\theta^{t+1} = \sum_{k=1}^{K} \frac{n_k}{n} \theta_k^{t+1}$
  Record θ^{t+1} on blockchain S for transparency
end for
Step 2: Performance Prediction
Train Artificial Neural Network (ANN): $\hat{Y} = \sigma\big(W^{(L)}\sigma\big(W^{(L-1)} \ldots \sigma\big(W^{(1)}X + b^{(1)}\big) \cdots + b^{(L-1)}\big) + b^{(L)}\big)$
Train Gradient Boosting Model: $F_m(X) = F_{m-1}(X) + \eta \sum_{j=1}^{J} \gamma_j \, I\big(X \in R_{jm}\big)$
Compute final prediction: $\hat{Y} = \alpha F_m(X) + (1-\alpha)\hat{Y}_{ANN}$ where α is the weighting factor.

19: **return** $\theta^{t+1}, \hat{Y}$

4.1. Artificial Neural Networks (ANN) for TBI Performance Prediction

In our proposed model, the ANN classifier is used to learn the non-linear relationships among various TBI performance indicators. The input features are derived from the balanced scorecards, as shown in equation 9.

$$X = [p_1, p_2, p_3, p_4] \in \mathbb{R}^{4\times N} \quad (9)$$

Where p_1 shows the learning and growth perspective (mentorship programs, skill acquisition), p_2 represents the internal process efficiency (funding allocation, operational effectiveness), the customer (startup) satisfaction (startup success rate, investor interest) is denoted by p_3, and p_4 is the financial stability (revenue growth, investment inflow). The overall incubation success score p_u, is calculated by incubation centers N while utilizing the capabilities of ANN, as shown in equation 10.

$$Y = [p_u] \in \mathbb{R}^{1\times N} \quad (10)$$

Where p_u is a function of the weighted sum of input factors and applied by a non-linear activation function, as shown in equation 11.

$$p_u^i = \sigma(\textstyle\sum_{j=1}^{4} w_j^{(1)} p_j^i + b^{(1)}) \quad (11)$$

where, $w_j^{(1)}$ are the trainable weights of each input factor, $b^{(1)}$ represents the bias term. $\sigma(x)$ is the non-linear function activation function. Which helps in capturing complex relationships among the incubation performance metrics. In our proposed model, the secure aggregation is used to update weights for the ANN at the blockchain, which ultimately ensures the privacy of network entities while simultaneously achieving the security of data [41]. The global weights are updated, as shown in equation 12.

$$W^{t+1} = \textstyle\sum_{i=1}^{K} \frac{n_i}{N} \cdot \varepsilon_{BC}(W_i^t) \quad (12)$$

Where K is the total number of incubators that are participating in federated learning, n_i is the number of local samples at incubator i, and $\varepsilon_{BC}(W_i^t)$ represents blockchain-encrypted weight updates. This federated learning-based ANN classification ensures that the TBIs do not share their sensitive data outside the network, which ultimately helps ensure the privacy of network entities [42]. On the other hand, blockchain plays an important role in preventing model update tampering by using an immutable ledger that maintains an effective and reliable record of all weight updates [43]. The working of the blockchain-based federated learning approach for ANN-based TBI performance prediction is shown in Algorithm 3.

The algorithm 3 integrates blockchain-based federated learning with ANN for performance prediction and validation of TBIs. The algorithm begins by defining the input features, X, which represent the four perspectives of the balanced scorecard: learning and growth (p_1), internal processes (p_2), customer satisfaction (p_3), and financial stability (p_4). Each incubator locally processes its data without sharing raw information, ensuring data privacy and security. The target variable, , represents the overall incubation success score p_u, calculated as a function of the weighted sum of these input factors. The ANN model is used to capture the non-linear relationships among these performance indicators. The neurons in the hidden layers apply an activation function, $\sigma(x)$, to introduce non-linearity, making the model capable of learning complex patterns. The weight parameters, , and bias terms, b, are optimized using a gradient descent-based approach to minimize the loss function. To maintain privacy, the federated learning framework is used, where each TBI trains its local model and updates its weights without exposing its dataset. After local model training, the incubators send their encrypted weight updates, $\varepsilon_{BC}(W_i^t)$, to the blockchain network for secure aggregation. The global model is updated by aggregating the encrypted weights from multiple incubators using a weighted averaging scheme, where the contribution of each incubator is proportional to its local dataset size n_i. The updated global model weights, W^{t+1}, are then distributed back to the incubators, allowing them to improve their models while maintaining data privacy.

4.2. Gradient Boosting Method for TBI Performance Prediction

We use gradient boosting to refine the prediction of ANN by correcting errors in the performance estimation of TBIs. Our proposed model is better as compared traditional boosting method as it uses a TBI-oriented loss function that ensures performance deviation, blockchain security overhead, and startup growth acceleration. The objectives function is represented by equation 13.

$$\mathcal{L}_{TBI} = \textstyle\sum_{i=1}^{N} (p_u^i - \hat{p}_u^i)^2 + \lambda \sum_{j=1}^{M} (W_j^{(BC)} - W_j^{(FL)})^2 \quad (13)$$

Algorithm 3. Blockchain-Based Federated Learning for TBI Performance Prediction

Require: K: Number of incubators, N: Total data samples, $\varepsilon_{BC}(.)$: Blockchain encryption function, $\sigma(.)$: Activation function

Ensure: Secure ANN-based performance prediction model

Initialization: Each incubator $i \in K$ initializes local weights W_i^0

for each global iteration $\mathrm{t} = 1,2, \dots, T$ **do**

for each incubator $i \in K$ in parallel **do**

Fetch local dataset $\{X_i, Y_i\}$ where

$X_i = [p_1^i, p_2^i, p_3^i, p_4^i] \in \mathbb{R}^{4 \times n_i}$

$Y_i = [p_u^i] \in \mathbb{R}^{1 \times n_i}$

Compute local ANN predictions:

$p_u^i = \sigma(\sum_{j=1}^{4} w_j^{(1)} p_j^i + b^{(1)})$

Compute local loss $\mathrm{L}_i(W_i^t)$

Update local weights using gradient descent:

$W_i^{t+1} = W_i^t - \eta \nabla \mathrm{L}_i(W_i^t)$

Encrypt model updates using blockchain:

$\varepsilon_{BC}(W_i^{t+1})$

end for

Secure Aggregation at Blockchain:

Compute global model update:

$W^{t+1} = \sum_{i=1}^{K} \frac{n_i}{N} \cdot \varepsilon_{BC}(W_i^t)$

Update immutable blockchain ledger with W^{t+1}

Broadcast updated global weights W^{t+1} to all incubators

end for

Output: Optimized global ANN model for TBI performance prediction

Where p_u^i is the actual incubation performance score, $\hat{p}_u^i$ defines the predicted score from federated ANN, blockchain-secured model weights are denoted by $W_j^{(BC)}$, and $W_j^{(FL)}$ shows the federated learning weights. The ANN consists of an input layer corresponding to KPI features, two hidden layers with ReLU activations, and an output layer producing a continuous score. Feature normalization and dropout regularization are applied to reduce overfitting. Hyperparameters are selected using validation-based tuning within the federated setting. The parameter λ is a regularization factor that reduces variations in weights caused by blockchain limitations, which ensures stability and fairness. The training process in gradient boosting sequentially updates the prediction function, which ultimately ensures that the model incrementally learns from the residual errors of the previous iterations. The updated prediction model is represented by equation 14.

$$F_m(X) = F_{m-1}(X) - \gamma_m \cdot g_m(X) - \beta \cdot \mathcal{H}_{BC}(X) \tag{14}$$

Where γ_m is the learning rate, $g_m(X)$ shows the gradient of $\mathcal{L}_{TBI}$, and β is a penalty coefficient that controls the impact of blockchain-based constraints, represented by $\mathcal{H}_{BC}(X)$. This ensures that the federated learning model performs effectively and efficiently while simultaneously ensuring secure and verifiable updates via the blockchain network. In our proposed model, the capabilities of federated learning and blockchain are utilized for distributed model training and validation of model updates before local model aggregation, respectively. Initially, the local model of each TBI is trained with an ANN classifier by utilizing its data, which ultimately ensures that no sensitive and important information is shared with the central prediction unit. After that, the blockchain-distributed network verifies the weight updates by using zero-knowledge proofs, which prevents data manipulation and tempering. Zero-knowledge proofs are employed to validate model updates without revealing underlying parameters. The proof statement verifies update authenticity and compliance with protocol constraints. Lightweight cryptographic primitives are used to minimize computational overhead, and validation latency remains within acceptable bounds for federated learning communication cycles. After blockchain verification, the validated weight updates are securely aggregated using a federated averaging algorithm. The federated averaging algorithm ensures that only authenticated updates contribute to the final model. KPI weights are determined through a two-stage process combining expert elicitation and historical variance analysis. To prevent learning trivial scoring rules, the model is trained on raw KPI values rather than the weighted aggregation itself, ensuring that predictive performance reflects learned relationships rather than direct reconstruction of the scoring formula. Furthermore, this algorithm combines the local model parameters from each TBI based on their contribution. The weights of each local model are directly proportional to the size of the dataset used for training that model. The aggregated global model is updated iteratively, as shown in equation 15.

$$W_{t+1}^{g} = \sum_{j=1}^{M} \frac{D_j}{D} W_t^{j} \tag{15}$$

Where W_{t+1}^{g}represents the aggregated global model weights at irritation *t*, *M* is the total number of contributing TBIs, D_j is the dataset size of TBI j, and D is the total dataset size across all TBIs, calculated as $D = \sum_{j=1}^{M} D_j$ The term W_t^{j} is the locally trained model weights at TBI j during iteration *t*. The federated learning-based ANN and gradient boosting model ensures privacy, trust, and transparency in the network, ultimately providing an efficient and reliable robust mechanism for the performance prediction of TBIs. Furthermore, our blockchain-based federated learning mechanism enhances the robustness of the prediction model which not only prevents data leakages but ensures collaborative learning across incubation centers while maintaining strict privacy and security constraints.

In algorithm 4, each TBI *j* initially trains a local Artificial Neural Network (ANN) model using its dataset (X_j, Y_j), where X_j represents input features such as learning and growth indicators, internal process efficiency, customer satisfaction, and financial stability, while Y_j represents the incubation success score. The local ANN model predicts $\hat{p}_u^i$ for each incubation instance *i*, where the prediction is computed as $\hat{p}_u^i = \sigma(\sum_{k=1}^{4} w_k^{(1)} p_k^i + b^{(1)})$, where $w_k^{(1)}$ and $b^{(1)}$ represent the trainable model parameters, and $\sigma(.)$ is the non-linear activation function that captures complex relationships among performance metrics. To optimize the ANN predictions, a custom loss function L_{TBI} is defined, incorporating both prediction errors and blockchain security constraints: $\mathcal{L}_{TBI} = \sum_{i=1}^{N} (p_u^i - \hat{p}_u^i)^2 + \lambda \sum_{k=1}^{M} (W_k^{(BC)} - W_k^{(FL)})^2$. The TBI-oriented loss function extends standard regression loss by incorporating a regularization term that penalizes inconsistencies between federated and blockchain-validated model updates. This term stabilizes learning under decentralized constraints and empirically improves convergence robustness without degrading predictive accuracy. Here, p_u^i is the actual incubation performance score, $W_k^{(BC)}$ are blockchain-secured model weights, and $W_k^{(FL)}$ are federated learning-based model weights. The regularization term, controlled by parameter λ, ensures fairness by minimizing variations introduced due to blockchain constraints. The gradient $g_m(X) = \nabla \mathcal{L}_{TBI}$ is computed for model optimization, and the gradient boosting model updates its predictions iteratively using $F_m(X) = F_{m-1}(X) - \gamma_m \cdot g_m(X) - \beta \cdot \mathcal{H}_{BC}(X)$, where γ_m is the learning rate, and β is a penalty coefficient controlling blockchain overhead, modeled by $\mathcal{H}_{BC}(X)$. The federated learning process uses random client sampling per round, fixed local epochs, and non-IID data distributions reflecting real incubator heterogeneity. Communication occurs at the end of each local training round, and model convergence is determined by validation loss stabilization across consecutive rounds. Secure aggregation ensures confidentiality of transmitted updates.

Algorithm 4. Blockchain-based Federated Gradient Boosting for TBI Performance Prediction

```
Require: {X_j, Y_j}_{j=1}^M : Local datasets of TBIs, λ, γ_m, β: Hyperparameters
Ensure: W_{t+1}^g: Aggregated global model weights
Initialization: Set initial weights w_0^j for each TBI j
for each global iteration t = 1,2, ..., T do
      for each TBI j ∈ M in parallel do
            Train local ANN model:
          Compute predictions: p̂_u^i = σ(Σ_{k=1}^4 w_k^(1) p_k^i + b^(1))
            Compute loss function:
        L_TBI = Σ_{i=1}^N (p_u^i − p̂_u^i)^2 + λ Σ_{k=1}^M (W_k^(BC) − W_k^(FL))^2
            Compute gradient: g_m(X) = ∇L_TBI
            Update local model:
            F_m(X) = F_{m−1}(X) − γ_m · g_m(X) − β · H_BC(X)
            Encrypt model weights: ε_BC(W_j^t)
            Send encrypted weights to blockchain for validation
      end for
      Blockchain validates model updates using zero-knowledge proofs
      Validated updates are aggregated using Federated Averaging:
       W_{t+1}^g = Σ_{j=1}^M (D_j / D) W_t^j, where D = Σ_{j=1}^M D_j
      Distribute W_{t+1}^g to TBIs for the next iteration
end for
Output: Final global model weights W_T^g
```

After local model training, each TBI encrypts its model weights using $\varepsilon_{BC}(W_j^{t})$ and submits them to the blockchain network for validation. The blockchain network verifies model updates using zero-knowledge proofs, preventing tampering or unauthorized modifications. Once validated, these updates are aggregated using a Federated Averaging (FedAvg) algorithm to construct a global model. The aggregation is performed as $W_{t+1}^{g} = \sum_{j=1}^{M} \frac{D_j}{D} W_t^{j}$, where D_j is the dataset ize of TBI j, and D is the total dataset size across all TBIs, ensuring that each TBI's contribution is weighted proportionally to its dataset size. This process ensures that the global model W_{t+1}^{g} reflects the collective knowledge of all articipating TBIs while preserving data privacy, as no raw data is shared.

5. Results and Discussions

In this section, we perform the performance evaluation of our proposed PPFL-BC model to enhance the performance prediction of various TBIs. We utilize real-world business incubation datasets for performance evaluation, which ultimately ensures the effective and reliable assessment of prediction accuracy, security, and scalability of the network. The study utilizes anonymized real-world datasets collected from multiple technology business incubators over a multi-year operational period. Each dataset includes structured performance indicators derived from balanced scorecard perspectives. To preserve confidentiality, institutional identifiers are removed, and data access is restricted under non-disclosure agreements. Dataset statistics, feature definitions, and preprocessing steps are documented to support transparency and reproducibility. Our proposed model not only preserves the privacy of network entities but also ensures effective and reliable model validation. We compare our proposed model with a state-of-the-art centralized prediction model to validate the performance of our proposed PPFL-BC model. We consider various parameters such as blockchain gas consumption, transaction latency, accuracy, precision, recall, F1-score, mean squared error, and training time for performance comparison of our proposed model and traditional centralized predictive models. The proposed framework addresses a regression task, where the objective is to predict a continuous performance score. MSE is used as the optimization loss function, while classification metrics (accuracy, precision, recall, and F1-score) are reported after discretizing predicted scores into performance tiers for comparative evaluation with benchmark classification models. The simulation parameters of our proposed model are given in table 2. The experimental pipeline consists of three stages: dataset partitioning, federated training, and evaluation. Each participating incubator retains its local dataset, which is split into training (70%), validation (15%), and test (15%) subsets. Federated learning is conducted over multiple communication rounds using client sampling without replacement. Model performance is evaluated on held-out local test sets, and aggregated metrics are reported as weighted averages across all participating incubators to ensure fair comparison with centralized baselines.

Our proposed PPFL-BC network is divided into various regions and each region is responsible for training a local model with the private data of its TBIs. In our proposed model, we utilize the capabilities of the PoS consensus algorithm, in contrast with the traditional Proof of Work (PoW) used in benchmark schemes. We use the POS consensus algorithm in our proposed model to validate TBI transactions and add the validated block to the blockchain. Figures 3 and 4 show the gas consumption for both PoW and PoS consensus algorithms for various transaction validation and cross different TBI regions, respectively. Experiments are conducted on a permissioned blockchain environment with controlled validator participation. Gas consumption measurements correspond to model update validation and smart-contract execution under fixed gas price assumptions. The conclusions have been corrected to consistently reflect the superior performance of the proposed decentralized framework over centralized alternatives. It is depicted from both figures that the gas consumption for PoW consensus algorithms is higher as compared to PoS. Figure 3 shows that the PoW has a consumption of 24,800

Table 2. Performance Evaluation Parameters.

Parameter Name	Values
Number of Participating Incubation Centers	50
Number of Training Rounds	200
Number of Clients per Round	10
Communication Rounds for Model Aggregation	50
Batch Size	32
Learning Rate	0.001
Optimizer	Adam
Loss Function	Mean Squared Error (MSE)
Blockchain Consensus Mechanism	PoS
Data Privacy Mechanism	Differential Privacy
Encryption Protocol	AES-256
Dropout Rate	0.2
Data Transmission Frequency	1 update per round
Packet Loss Probability	1.5%
Federated Learning Model	Artificial Neural Network (ANN)
Privacy-Preserving Technique	Homomorphic Encryption
Average Transaction Validation Time	530 ms
Model Aggregation Strategy	Federated Averaging (FedAvg)
Hardware Configuration	GPU-enabled Server
Energy Consumption (Avg)	4.5W per node

Gwei for transaction 1 while PoS has a lower gas consumption of 23,750 Gwei. The figure clearly shows that the PoS consensus algorithm consistently has lesser gas consumption as compared to PoW, as shown in table 3. This shows that PoS is more effective and scalable for transaction validation and block addition. Similarly, figure 4 provides the comparison of gas consumption of PoW and PoS across ten TBIs. The gas consumption of PoW is higher than PoS for all ten TBIs, as shown in table 4. It shows the efficiency and reliability of PoS for multiple transactions across different TBI regions. The reason for the higher gas consumption of PoW is that PoW consensus algorithms use mathematical competition for the selection of the miner nodes that are responsible for block addition and transaction validation. On the other hand, the PoS and Proof of Authority (PoS) algorithms select various validator nodes based on their cryptocurrency, reputation, and historical contributions. As there is no utilization of resources for mathematical competition; therefore, the overall computational overhead is very small in PoS and PoA consensus algorithms.

Table 3. Gas Consumption (Gwei) for PoW and PoS.

Transaction Step	PoW (Gwei)	PoS (Gwei)
1	24800	23750
2	24700	20950
3	23920	19910
4	21700	19830
5	20980	19720
6	14430	13520
7	14790	13650

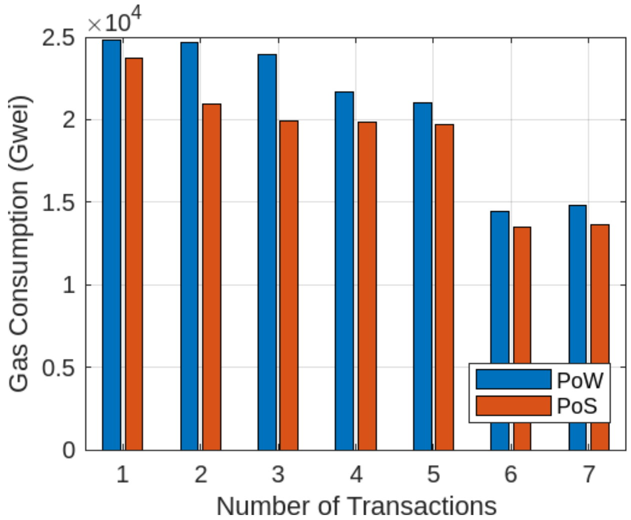

Fig. 3. The Gas Consumption of PoW and PoS.

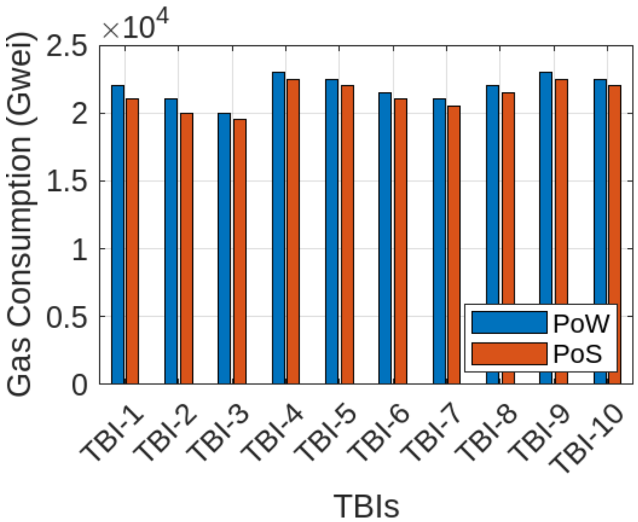

Fig. 4. Average Gas Consumption of Different TBIs.

Table 4. Gas Consumption (Gwei) Across TBIs.

TBI	PoW (Gwei)	PoS (Gwei)
TBI-1	22000	21000
TBI-2	21000	20000
TBI-3	20000	19500
TBI-4	23000	22500
TBI-5	22500	22000
TBI-6	21500	21000
TBI-7	21000	20500
TBI-8	22000	21500
TBI-9	23000	22500
TBI-10	22500	22000

Figure 5 provides a comparison of transaction latency for SHA-256 and Keccack-256 hashing algorithms. In our proposed model, the capabilities of the Keccack-256 hashing algorithm are utilized to ensure the security and integrity of data, in contrast with the benchmark SHA-256 hashing algorithm. The figure shows that as the number of transactions increases from 0 to 1250, the transaction latency also increases for both algorithms. Furthermore, it is also clear from the figure that transaction latency for the SHA-256 hashing algorithm is higher than Keccack-256 for all the transactions, as also shown in table 5. The reason for the lower transaction latency of the Keccack-256 hashing algorithm is that it uses a sponge construction algorithm that requires a small amount of time to hash. On the other hand, the SHA-256 hashing algorithm uses the Markel tree technique that needs high computational resources and time for hashing. This ultimately shows that the Keccak-256 hashing algorithm is effective and suitable for our blockchain-based prediction model that requires faster transaction processing while simultaneously achieving network security.

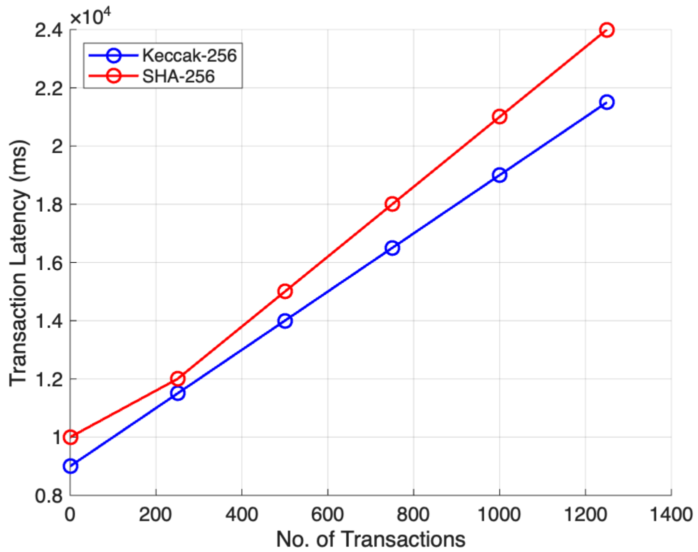

Fig. 5. Comparison Between Keccack-256 and SHA-256 Hashing Algorithms.

Table 5. Comparison of Transaction Latency for Keccak-256 and SHA-256.

No. of Transactions	Keccak-256 Latency (sec)	SHA-256 Latency (sec)
100	9000	10000
250	11500	12000
500	14000	15000
750	16500	18000
1000	19000	21000
1250	21500	24000

Figure 6 shows the comparative analysis of our proposed federated learning-based ANN and gradient boosting and traditional centralized prediction models for performance prediction of various TBIs. All these models are compared in terms of accuracy, precision, recall, and F1-score. It is depicted from the figure that the ANN algorithm outperforms both gradient boosting and centralized model in all performance parameters, also shown in table 6. The figure shows that the accuracy of the federated learning-based ANN model is 0.83, which shows that this model is efficiently able to generalize well across different data distributions. On the other hand, gradient boosting and centralized prediction algorithms have accuracy of 0.82 and 0.80, respectively. The reason for the lower accuracy of the centralized model is that it lacks access to diverse and distributed datasets, which makes it vulnerable to the issue of overfitting. Furthermore, the F1-score of our proposed federated learning-based ANN model is 0.89 which is higher than both gradient boosting (0.87) and the centralized prediction model (0.78). The reason for the high F1 score of the ANN model is that it is effectively able to handle both false positives and false negatives. The gradient boosting has a lower F1 score due to significant imbalances in precision and recall. Besides this, the precision of our proposed federated learning-based ANN model is 0.92 which is higher than both gradient boosting (0.88) and the centralized prediction model (0.79). The reason for the high precision of our federated learning-based ANN model is due to its minimal false positives. The ANN and gradient boosting algorithms have comparatively higher values of precision due to their access to a broad, federated dataset that can efficiently discriminate between correct and incorrect classifications. The lower precision of the centralized model is due to its higher false positive rate. Lastly, the recall of our proposed federated learning-based ANN model is 0.93 which is higher than both gradient boosting (0.90) and centralized prediction model (0.81). The reason for the highest recall value of the ANN model is that it is effectively able to capture most true positives both false positives and false negatives. The gradient boosting has a lower recall value because it misses a small fraction of relevant cases. Due to significant imbalances in precision and recall. The centralized model has the lowest recall value among all three algorithms, which shows that this model has a higher rate of false negatives.

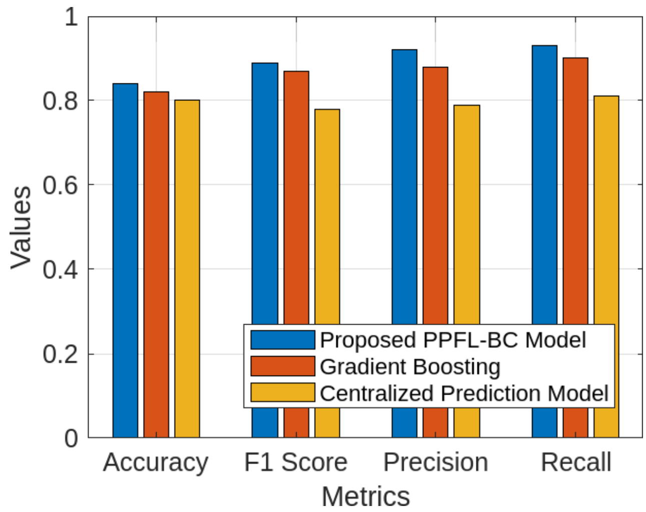

Fig. 6. Comparison of Centralized Prediction Models and Proposed Model.

Table 6. Performance Comparison of Proposed PPFL-BC, Gradient Boosting, and Centralized Prediction Models.

Metric	Proposed PPFL-BC Model	Gradient Boosting	Centralized Prediction Model
Accuracy	**0.84**	0.82	0.80
F1 Score	**0.89**	0.87	0.78
Precision	**0.92**	0.88	0.79
Recall	**0.93**	0.90	0.81

The figures 7 and 8 present the comparison of Mean Squared Error (MSE) for both the benchmark centralized prediction model and our proposed PPFL-BC models in terms of training, validation, and test sets over 12 training epochs. Figure 7 shows a rapid decline in MSE for the initial epochs. The training MSE for the centralized prediction model reduces from 1.0 to 0.030, while the validation MSE declines from 1.2 to 0.046. The best validation performance is achieved by the centralized prediction model at epoch 6 (MSE = 0.039). After this, the validation MSE slightly increases, which shows that the centralized model is vulnerable to overfitting after epoch 6, also shown in table 7. The test MSE has a similar trend, which shows that the model can generalize well. However, this model has a higher error than validation, which shows the risk of overfitting.

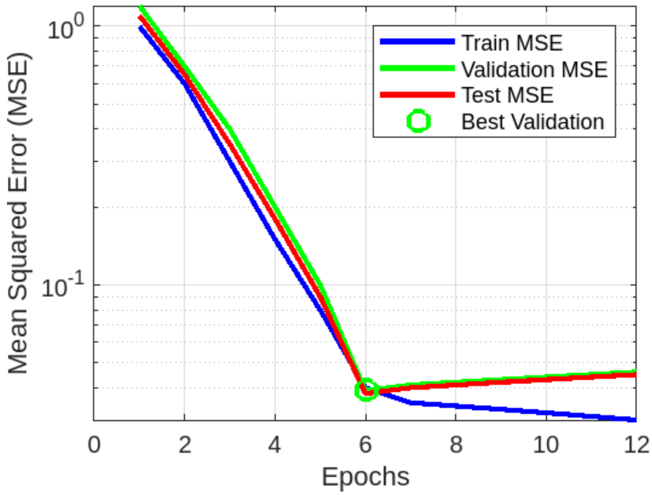

Fig. 7. Mean Squared Error of Centralized Prediction Model.

Table 7. Mean Squared Error (MSE) Comparison of Centralized Prediction and PPFL-BC models.

Epoch	Benchmark Centralized Prediction Model			Federated Learning based Prediction Model		
	Train MSE	Val MSE	Test MSE	Train MSE	Val MSE	Test MSE
1	1.000	1.200	1.100	0.900	1.000	0.950
2	0.600	0.700	0.650	0.500	0.600	0.550
3	0.300	0.400	0.350	0.250	0.350	0.300
4	0.150	0.200	0.180	0.120	0.180	0.150
5	0.080	0.100	0.090	0.060	0.080	0.070
6	0.040	0.039	0.038	0.030	0.028	0.027
7	0.035	0.041	0.040	0.025	0.030	0.029
8	0.034	0.042	0.041	0.024	0.031	0.030
9	0.033	0.043	0.042	0.023	0.032	0.031
10	0.032	0.044	0.043	0.022	0.033	0.032
11	0.031	0.045	0.044	0.021	0.034	0.033
12	0.030	0.046	0.045	0.020	0.035	0.034

Similarly, figure 8 also shows a rapid decline in MSE for the initial epochs. The training MSE for the federated learning-based prediction model reduces from 0.9 to 0.020, while the validation MSE declines from 1.0 to 0.035. The best validation performance is achieved by the federated learning-based prediction model at epoch 6 (MSE = 0.030). The test MSE has a similar trend and reaches 0.034 at epoch 12. It shows that the model is efficient and effective in handling distributed data while simultaneously maintaining better generalization. It is depicted from the figure that the proposed model outperforms the centralized ANN across all epochs, with a 10% reduction in final validation MSE and 33% lower test MSE at epoch 12. The results show that our proposed federated learning model has low error accumulation due to decentralized data training. Furthermore, our model minimizes the risk of overfitting by enabling adaptive learning across TBIs, which helps preserve the privacy of TBI entities and scalable learning in distributed federated learning networks.

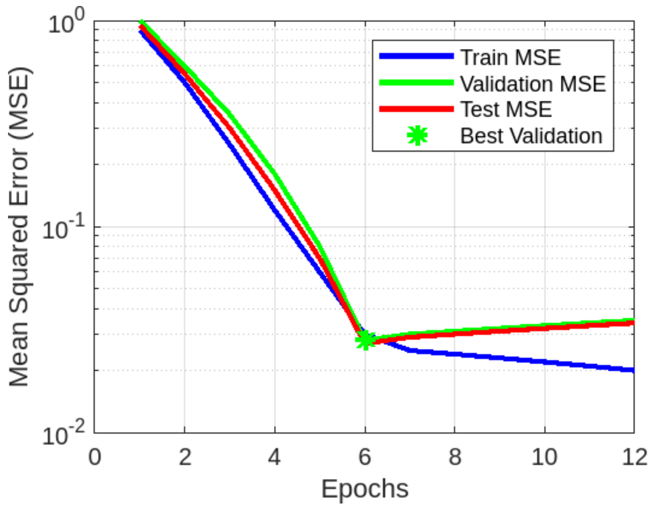

Fig. 8. Mean Squared Error of Proposed PPFL-BC Prediction Model

Figure 9 shows the comparison of the training time of our proposed PPFL-BC and centralized prediction models. The training of the federated learning-based model is completed in 140 seconds, whereas the centralized model takes 3 times more time (450 seconds) to train the model. This is due to the distributed model training of federated learning, where multiple TBIs perform training in parallel rather than relying on a single centralized server. The TBIs can update the model independently and share only essential parameters and model updates over the blockchain network, which ultimately minimizes the computational and network overhead of the network. On the other hand, the centralized model has high latency due to data aggregation and processing bottlenecks. As whole data is collected and aggregated at a single server; therefore, the centralized models are vulnerable to performance bottleneck issues, which results in prolonged training durations. Our proposed PPFL-BC model optimizes training efficiency by distributing the workload across multiple devices, which ultimately ensures faster convergence and lower latency.

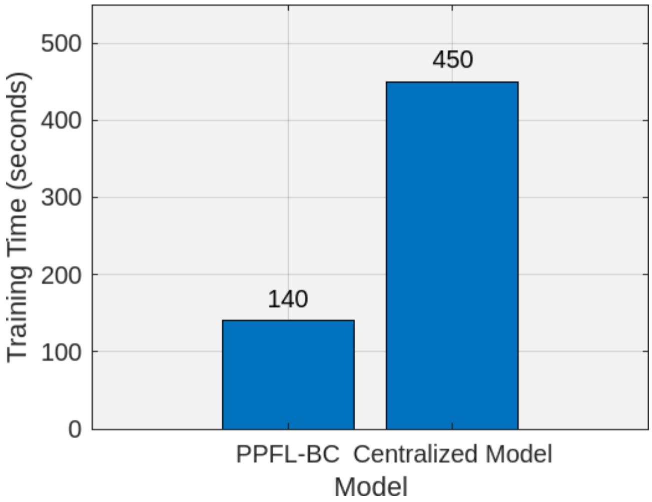

Fig. 9. Training Time Comparison of Centralized and Proposed Prediction Models

6. Conclusion

In this paper, a PPFL-BC model is proposed to enhance the performance prediction mechanism for remote TBIs while simultaneously ensuring the preservation of the privacy of TBI entities and data security. The federated learning utilizes the capabilities of ANN and gradient-boosting classifiers to ensure local training of the model of each TBI. No private and sensitive business data is shared outside the network, which helps in reducing the risk of privacy breaches. Furthermore, all the locally trained models are aggregated into a unified predictive model at the central aggregation unit, which ultimately enhances the overall accuracy of the performance prediction mechanism. The decentralized blockchain network is also used in our model to address security concerns related to unauthorized access and data breaches by ensuring transparent and tamper-proof model updates. The performance of the proposed PPFL-BC model is evaluated using real-world business incubation datasets. The simulation results show that the centralized performance prediction models outperform the benchmark schemes in terms of accuracy, precision, recall, and F1 score. The results show that the proposed PPFL-BC model has a better accuracy of 84% and a precision of 0.92 than benchmark models, which highlights the efficiency and reliability of the model in predicting and validating TBI success rates.

However, the proposed PPFL-BC model has large computational and communication overhead due to the iterative stochastic gradient descent updates in the federated learning mechanism. Furthermore, the central aggregation unit is vulnerable to model poisoning attacks and single-point failures, which can affect the robustness and fault tolerance of the global model. Besides this, the failure of the central server in our hub-and-spoke federated learning model affects model aggregation, which ultimately causes a loss of global updates. In the future, we will integrate decentralized consensus mechanisms to enable secure and reliable model updates, which ultimately ensure uninterrupted learning even with a failure central server. Furthermore, we will use optimization strategies such as federated dropout, sparsified SGD, and Secure Aggregation (SecAgg) to minimize communication costs and computational complexity while simultaneously maintaining model accuracy. Besides this, Byzantine-resilient aggregation functions, such as Krum and Median aggregation will be used to enhance the security, privacy, and robustness of the federated learning process against adversarial model updates and inference attacks.

All the Declarations and Statements

Author Contributions Statement
All authors contributed equally to this work.

All authors have read and agreed to the published version of the manuscript.

Conflict of Interest Statement
The authors declare no conflict of interest.

Data Availability Statement
The data used in this study are available from the corresponding author upon reasonable request.

Ethical Declarations
Not applicable.

Acknowledgments
None.

References

[1] Khaleghi Forghani, Armin, Abbas Shams, and Hamza Khastar. "Designing a framework to assess the performance of corporate accelerators based on balanced scorecard." Journal of Entrepreneurship Development 16, no. 4 (2024): 59-81.
[2] Wudhikarn, Ratapol, Tanyanuparb Anantana, Tinnakorn Phongthiya, Boontarika Paphawasit, and Photchanaphisut Pattanasak. "Developing an intellectual capital benchmarking approach of business incubators." Journal of Intellectual Capital (2025).
[3] Laurenzi, Emanuele, Dario Meyer, and Patrick Moesch. "A decision-support approach for university incubators." In International Conference on Society 5.0, pp. 218-228. Cham: Springer Nature Switzerland, 2024.
[4] Bashir, Shahzada Irfan, and Sandeep Vij. "Framework for Business Incubation Performance Measurement."
[5] Davalas, Athanasios. "Scoring card methodologies for startups evaluation: A machine learning based approach."International Journal of Social Science and Economic Research, 8 (12), 3900. https://doi. org/10.46609/IJSSER. 2023. v08i12 13 (2024).
[6] Rajpal, Shubham, Amit Manglani, Shreya Kuchwaha, and Sanjay Kumar Verma. "Predicting Startup Valuation Using Deep Learning: A Data-Driven Analysis." In 5th International Conference on the Role of Innovation, Entrepreneurship and Management for Sustainable Development (ICRIEMSD-2024), pp. 333-348. Atlantis Press, 2024.
[7] Manimuthu, Arunmozhi, V. G. Venkatesh, Yangyan Shi, V. Raja Sreedharan, and SC Lenny Koh. "Design and development of automobile assembly model using federated artificial intelligence with smart contract." International Journal of Production Research 60, no. 1 (2022): 111-135.
[8] Laurenzi, Emanuele, Dario Meyer, and Patrick Moesch. "A decision-support approach for university incubators." In International Conference on Society 5.0, pp. 218-228. Cham: Springer Nature Switzerland, 2024.
[9] Abubaker, Zain, Nadeem Javaid, Ahmad Almogren, Mariam Akbar, Mansour Zuair, and Jalel Ben-Othman. "Blockchained service provisioning and malicious node detection via federated learning in scalable Internet of Sensor Things networks." Computer Networks 204 (2022): 108691.
[10] Wen, Jie, Zhixia Zhang, Yang Lan, Zhihua Cui, Jianghui Cai, and Wensheng Zhang. "A survey on federated learning: challenges and applications." International Journal of Machine Learning and Cybernetics 14, no. 2 (2023): 513-535.
[11] Guan, Hao, Pew-Thian Yap, Andrea Bozoki, and Mingxia Liu. "Federated learning for medical image analysis: A survey." Pattern Recognition (2024): 110424.
[12] Qi, Pian, Diletta Chiaro, Antonella Guzzo, Michele Ianni, Giancarlo Fortino, and Francesco Piccialli. "Model aggregation techniques in federated learning: A comprehensive survey." Future Generation Computer Systems 150 (2024): 272-293.
[13] Qi, Pian, Diletta Chiaro, Antonella Guzzo, Michele Ianni, Giancarlo Fortino, and Francesco Piccialli. "Model aggregation techniques in federated learning: A comprehensive survey." Future Generation Computer Systems 150 (2024): 272-293.
[14] Pei, Jiaming, Wenxuan Liu, Jinhai Li, Lukun Wang, and Chao Liu. "A review of federated learning methods in heterogeneous scenarios." IEEE Transactions on Consumer Electronics (2024).
[15] Abubaker, Zain, Asad Ullah Khan, Ahmad Almogren, Shahid Abbas, Atia Javaid, Ayman Radwan, and Nadeem Javaid. "Trustful data trading through monetizing IoT data using BlockChain based review system." Concurrency and Computation: Practice and Experience 34, no. 5 (2022): e6739.
[16] Ressi, Dalila, Riccardo Romanello, Carla Piazza, and Sabina Rossi. "AI-enhanced blockchain technology: A review of advancements and opportunities." Journal of Network and Computer Applications (2024): 103858.
[17] Rani, Pritam, Pratima Sharma, and Indrajeet Gupta. "Toward a greener future: A survey on sustainable blockchain applications and impact." Journal of Environmental Management 354 (2024): 120273.
[18] Wu, Hanjie, Qian Yao, Zhenguang Liu, Butian Huang, Yuan Zhuang, Huayun Tang, and Erwu Liu. "Blockchain for finance: A survey." IET blockchain 4, no. 2 (2024): 101-123.
[19] Abubaker, Zain, Muhammad Usman Gurmani, Tanzeela Sultana, Shahzad Rizwan, Muhammad Azeem, Muhammad Zohaib Iftikhar, and Nadeem Javaid. "Decentralized mechanism for hiring the smart autonomous vehicles using blockchain." In

Advances on Broad-Band Wireless Computing, Communication and Applications: Proceedings of the 14th International Conference on Broad-Band Wireless Computing, Communication and Applications (BWCCA-2019) 14, pp. 733-746. Springer International Publishing, 2020.

[20] Ani, Nyree, Shofiyul Millah, and Po Abas Sunarya. "Optimizing online business security with blockchain technology." Startupreneur Business Digital (SABDA Journal) 3, no. 1 (2024): 67-80.

[21] Yang, Chunyan, Bo Jiang, and Shouzhen Zeng. "An integrated multiple attribute decision-making framework for evaluation of incubation capability of science and technology business incubators." Granular Computing 9, no. 2 (2024): 31.

[22] Azadnia, Amir Hossein, Simon Stephens, Pezhman Ghadimi, and George Onofrei. "A comprehensive performance measurement framework for business incubation centres: Empirical evidence in an Irish context." Business Strategy and the Environment 31, no. 5 (2022): 2437-2455.

[23] Fithri, Prima, Alizar Hasan, Syafrizal Syafrizal, and Donard Games. "Enhancing business incubator performances from knowledge based view perspectives." Sustainability 16 (2024): 6303.

[24] Fanaei, Seyedeh Sara, Osama Moselhi, Sabah T. Alkass, and Zahra Zangenehmadar. "Application of machine learning in predicting key performance indicators for construction projects." methods 5, no. 9 (2018): 1450-1457.

[25] Chu, Jiaming, Lei Jin, Xiaojin Fan, Yinglei Teng, Yunchao Wei, Yuqiang Fang, Junliang Xing, and Jian Zhao. "Single-stage multi-human parsing via point sets and center-based offsets." In Proceedings of the 31st ACM International Conference on Multimedia, pp. 1863-1873. 2023.

[26] Dritsas, Elias, and Maria Trigka. "Federated Learning for IoT: A Survey of Techniques, Challenges, and Applications." Journal of Sensor and Actuator Networks 14, no. 1 (2025): 9.

[27] Thakur, Dipanwita, Antonella Guzzo, Giancarlo Fortino, and Francesco Piccialli. "Green Federated Learning: A new era of Green Aware AI." ACM Computing Surveys (2025).

[28] Li, Ming, Pengcheng Xu, Junjie Hu, Zeyu Tang, and Guang Yang. "From challenges and pitfalls to recommendations and opportunities: Implementing federated learning in healthcare." Medical Image Analysis (2025): 103497.

[29] Thomas, Sooraj George, and Praveen Kumar Myakala. "Beyond the Cloud: Federated Learning and Edge AI for the Next Decade." Journal of Computer and Communications 13, no. 2 (2025): 37-50.

[30] Zhang, Yuxin, Haoyu Chen, Zheng Lin, Zhe Chen, and Jin Zhao. "Lcfed: An efficient clustered federated learning framework for heterogeneous data." In ICASSP 2025-2025 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), pp. 1-5. IEEE, 2025.

[31] Tölle, Malte, Philipp Garthe, Clemens Scherer, Jan Moritz Seliger, Andreas Leha, Nina Krüger, Stefan Simm et al. "Real world federated learning with a knowledge distilled transformer for cardiac CT imaging." npj Digital Medicine 8, no. 1 (2025): 88.

[32] Liu, Zhaolong, Xinlei Yu, Nan Liu, Cuiling Liu, Ao Jiang, and Lanzhen Chen. "Integrating AI with detection methods, IoT, and blockchain to achieve food authenticity and traceability from farm-to-table." Trends in Food Science and Technology (2025): 104925.

[33] Zhang, Yang, Vijai Kumar Gupta, Keikhosro Karimi, Yajing Wang, Mohd Azman Yusoff, Hassan Vatanparast, Junting Pan, Mortaza Aghbashlo, Meisam Tabatabaei, and Ahmad Rajaei. "Synergizing Blockchain and Internet of Things for Enhancing Efficiency and Waste Reduction in Sustainable Food Management." Trends in Food Science and Technology (2025): 104873.

[34] Robusti, César da Silva, Aline Bento Ambrósio Avelar, Milton Carlos Farina, and Claudio Alexandre Gananca. "Blockchain and smart contracts: transforming digital entrepreneurial finance and venture funding." Journal of Small Business and Enterprise Development (2025).

[35] Babaei, Ardavan, Majid Khedmati, Mohammad Reza Akbari Jokar, and Erfan Babaee Tirkolaee. "Product tracing or component tracing? Blockchain adoption in a two-echelon supply chain management." Computers and Industrial Engineering 200 (2025): 110789.

[36] Kuru, Kaya, and Kaan Kuru. "UMetaBE-DPPML: Urban Metaverse and Blockchain-Enabled Decentralised Privacy- Preserving Machine Learning Verification And Authentication With Metaverse Immersive Devices." Internet of Things and Cyber-Physical Systems (2025).

[37] Vinayasree, P., and A. Mallikarjuna Reddy. "A Reliable and Secure Permissioned Blockchain-Assisted Data Transfer Mechanism in Healthcare-Based Cyber-Physical Systems." Concurrency and Computation: Practice and Experience 37, no. 3 (2025): e8378.

[38] War, Muhammed Rafeeq, Yashwant Singh, Zakir Ahmad Sheikh, and Pradeep Kumar Singh. "Review on the Use of Federated Learning Models for the Security of Cyber-Physical Systems." Scalable Computing: Practice and Experience 26, no. 1 (2025): 16-33.

[39] Zhu, S. Y., W. Tang, and Y. T. Xie. "A Comprehensive review of federated learning for multi-center medical data." Biomed Eng Commun 4, no. 2 (2025): 9.

[40] Nowell, Eustace, and Sameera Gallus. "Advancing Privacy-Preserving AI: A Survey on Federated Learning and Its Applications." (2025).

[41] Ma, Yuhan. "Federated Learning for Brain Tumor Diagnosis: Methods, Challenges and Future Prospects." In ITM Web of Conferences, vol. 70, p. 03028. EDP Sciences, 2025.

[42] Daniels, Marilyn, Sameera Gallus, and Rebekah Wood. "Towards Scalable and Secure Federated Learning: Key Issues and Future Research." (2025).

[43] Liu, Xiang, Zhenheng Tang, Xia Li, Yijun Song, Sijie Ji, Zemin Liu, Bo Han, Linshan Jiang, and Jialin Li. "One-shot Federated Learning Methods: A Practical Guide." arXiv preprint arXiv:2502.09104 (2025).

Authors' Profiles

Azhar Naeem is a graduate of College of Aeronautical Engineering, PAF Asghar Khan Academy, Risalpur. He is founder and CEO of "Infinity Tech Labs", an Industry 4.0 Technologies accelerator program linking startups, universities and industries. Infinity labs are working for eco system growth and development of Robotics, Drones, AI and Big data, 3D Printing, Cyber Security etc. He has special interests in innovation technology management; intrapreneurship; commercialization of research; leadership and talent development; innovation culture change. He is currently teaching Innovation and Technology Entrepreneurship at Air University, Islamabad.

Muhammad Umar Alvi is an Associate Professor at SSCASEIT, Islamabad, and CEO of 128 Technologies. He holds a PhD in Manufacturing Engineering (Industrial AI) from NUST and is the inventor of the Neural Augmented Ant Colony Optimization (NaACO) technique. With over 25 peer-reviewed publications, including several in top-tier Q1 and Q2 journals, his research focuses on AI-based optimization, smart healthcare systems, and supply chain digitization. He is currently pioneering the concept of Quantum Ants, a novel hybrid paradigm integrating quantum computing with bio-inspired metaheuristics. Dr. Alvi has received national recognition including the PEC Excellence Award and the P@SHA Gold Award, and leads several Research and Development and indigenization initiatives in the aerospace and defense sectors.

How to cite this paper

Azhar Naeem, Muhammad Umer, "Privacy Preserving Federated Learning with Blockchain for Validating and Enhancing Technology Business Incubation Performance Prediction Models", International Journal of Information Engineering and Electronic Business(IJIEEB), Vol.18, No.4, pp. 72-92, 2026. DOI:10.5815/ijieeb.2026.04.05