Computer Modeling in Engineering & Sciences

Tech Science Press

DOI: 10.32604/cmes.2023.026691

ARTICLE

PoQ-Consensus Based Private Electricity Consumption Forecasting via Federated Learning

Yiqun Zhu[1], Shuxian Sun[1], Chunyu Liu[1], Xinyi Tian[1], Jingyi He[2] and Shuai Xiao[2,*]

[1]Marketing Service Center, State Grid Tianjin Electric Power Company, Tianjin, 300120, China

[2]School of Electrical and Information Engineering, Tianjin University, Tianjin, 300072, China

*Corresponding Author: Shuai Xiao. Email: xs611@tju.edu.cn

Received: 20 September 2022 Accepted: 22 November 2022

ABSTRACT

With the rapid development of artificial intelligence and computer technology, grid corporations have also begun to move towards comprehensive intelligence and informatization. However, data-based informatization can bring about the risk of privacy exposure of fine-grained information such as electricity consumption data. The modeling of electricity consumption data can help grid corporations to have a more thorough understanding of users' needs and their habits, providing better services for users. Nevertheless, users' electricity consumption data is sensitive and private. In order to achieve highly efficient analysis of massive private electricity consumption data without direct access, a blockchain-based federated learning method is proposed for users' electricity consumption forecasting in this paper. Specifically, a blockchain system is established based on a proof of quality (PoQ) consensus mechanism, and a multilayer hybrid directional long short-term memory (MHD-LSTM) network model is trained for users' electricity consumption forecasting via the federal learning method. In this way, the model of the MHD-LSTM network is able to avoid suffering from severe security problems and can only share the network parameters without exchanging raw electricity consumption data, which is decentralized, secure and reliable. The experimental result shows that the proposed method has both effectiveness and high-accuracy under the premise of electricity consumption data's privacy preservation, and can achieve better performance when compared to traditional long short-term memory (LSTM) and bidirectional LSTM (BLSTM).

KEYWORDS

Blockchain; consensus mechanism; federated learning; electricity consumption forecasting; privacy preservation

1 Introduction

Since the first decade of the 21st century, State Grid Corporation of China (SGCC) has put forward the plan for smart grid, intending to build a smart grid with the characteristics of informatization, intelligence, and interaction [1]. With the advent of technological innovation and electric power reform, the development and improvement of smart grid, such as automatic generation control (AGC), renewable energy integration (RGI) and electricity consumption forecasting (ECF), have received more and more attention [2,3]. Among them, ECF is an important topic in the construction

of smart grid. Accurate ECF and its modeling have important guiding significance for the grid-planning and decision-making of grid corporations [4]. At present, artificial intelligence (AI) has been widely applied for ECF to learn generic electricity consumption features and improve forecasting performance. Nevertheless, most of the existing artificial intelligence methods require data holders to upload raw data, which is sensitive and private, to a central server to train the models in a centralized fashion [5–10]. If the central server is attacked, the entire system has to face the risk of suffering from severe security problems, and this may easily result in privacy disclosure for the users [11]. The user's electricity data can reflect users' electricity consumption habits, from which users' outdoor time, consumption concept and economic level can be inferred. If the evildoers get these sensitive and private data, it will bring great security risks to the users. Therefore, it is necessary to explore how to achieve highly efficient use of private data under the constraints of data privacy preservation.

The emergence of federated learning (FL) brings a new approach to solving the above problems. As an emerging machine learning technology, the concept of federated learning was first proposed by McMahan et al. [12] in 2016 and quickly become a hot research topic in the field of privacy-preserving machine learning. FL is a learning mechanism in which multiple data holders (such as mobile phones, IoT devices, financial or medical institutions) collaborate to train the model without sharing data and only exchange the training parameters in the intermediate stage [13]. In this way, federated learning can break through the limitations of a single data holder in terms of data amount and data distribution, obtaining a high-quality model by training with data from multiple data holders. However, traditional federated learning may have some security vulnerabilities [14]. The centralized structure completely depends on the reliability of the central server, which makes the entire training process easy to be completely controlled by the attacker once the central server is maliciously occupied. In addition, how to deal with the situation where an attacker publishes fake or malicious data to poison the model is also an issue worthy of research.

In recent years, the characteristics of decentralized, traceable, tamper-proof and privacy-preserving of blockchain made blockchain technology receive extensive attention and study in various fields [15–17]. Blockchain is essentially a new decentralized distributed database based on cryptography. By using peer-to-peer (P2P) networking technology and hybrid communication protocols, blockchain is competent for handling the communication of heterogeneous devices so that the information in each isolated system can be effectively shared and integrated [18]. The blockchain system realizes the characteristics of non-tampering and easy tracking of data on the chain through the hash lock and timestamp mechanism and ensures trusted interaction of multi-source data based on the consensus mechanism, providing a secure and reliable approach for data sharing among multiple types of equipment or sensing devices [19].

Therefore, this paper mainly focuses on the privacy preservation of electricity consumption data by the combination of blockchain technology and federated learning mechanism, proposing a blockchain based private electricity consumption forecasting via federated learning. Considering the obvious periodicity of the electricity consumption, we build a multilayer hybrid directional long short-term memory (MHD-LSTM) network to handle both forward and backward dependencies of users' electricity consumption data. The parameters of MHD-LSTM network are shared by the proposed blockchain-based federated learning system, achieving highly efficient training without accessing the private electricity consumption data.

The main contributions of this study are as follows:

(1) An electricity consumption data sharing blockchain system that can achieve trusted interaction and privacy preservation is established on the basis of proof of quality (PoQ) consensus

mechanism. The update of the local network's model is verified by a set of trusted consensus nodes, avoiding the security risks caused by the centralized training of the central server.

(2) A blockchain-based federated learning mechanism for electricity consumption data forecasting is designed. Instead of sharing the private electricity consumption data directly, the participating nodes realize privacy preservation by using the data to perform the local network's model training and only sharing the parameters of the local network's model.

(3) In order to capture both the forward dependency and the backward dependency of users' electricity consumption data, an MHD-LSTM containing unidirectional and bidirectional structures is proposed for electricity consumption forecasting, according to the characteristics of electricity consumption data.

The rest parts of this paper are organized as follows. Section 2 briefly reviews the related work. In Section 3, the main theories and the proposed methods are elaborated. Section 4 shows the results and the discussion of this study, which is followed by conclusions in Section 5.

2 Related Works

Generally, electricity consumption data are highly coupled in the temporal domains, the current data forecasting methods can be mainly divided into classical methods, traditional methods and intelligent methods [20–22]. Based on the similarity of development trends, the classical forecasting methods include regression analysis methods and time series methods, which are simple, fast, but with low precision when the trend fluctuates greatly. When the dispersion of data is high, the traditional forecasting methods, including the exponential smoothing method and the grey forecasting method have their own shortcoming as well. Fortunately, the intelligent methods represented by deep learning can abstract high-level features from low-level features, thereby revealing the changing laws of the data accurately. Long short-term memory (LSTM) network is a kind of recurrent neural network used for time series processing, which can remember longer time series information through its cyclic structure and gating mechanism. Many researchers have conducted research in this field. Kim et al. [23] used the LSTM network to perform monthly electricity consumption forecasting. Su et al. [24] proposed a combined-LSTM to extract the hidden relationships between peak and valley volume. Ullah et al. [25] achieved better forecasting results by proposing a network M-BDLSTM. However, due to factors such as business competition and privacy preservation, the data interaction between different institutions is greatly hindered. The existence of an isolated data island makes it impossible to realize effective network model training, so the value of data cannot be fully utilized.

In order to solve the problem of isolated data island, many researchers have conducted research on federated learning [26], and many works using federated learning have been proposed in recent years. Aiming at the problem of model performance degradation caused by non-IID data, Jeong et al. [27] proposed a FAug method, which achieved the expansion of the client's local training set by training a CGAN on the server. Han et al. [28] proposed a part-federated learning (PFL) method by merging the advantages of split learning, which can not only reduce communication cost but also improve data privacy. This method only shares partial parameters of the local model with the FL server, and has better performance when dealing with non-IID data. To improve the diversity of tasks, Smith et al. [29] proposed a system-aware optimization method MOCHA for multi-task learning to solve the challenges related to communication, abnormal nodes, and fault tolerance, realizing personalized federated learning. Kumar et al. [30] proposed a privacy-encoding-based federated learning (PEFL) framework for intrusion detection to minimize the risk of data privacy disclosure,

which can efficiently identify the normal and the attack patterns during communication. All the above methods have their advantages, but they cannot play a superior performance in decentralized environment.

To overcome the above challenges, researchers recently turn their eyes to blockchain technology, which has become a research hotspot with the popularity of virtual currencies such as Bitcoin [31–33]. Blockchain technology was first proposed in 2008, solving the problem of decentralization without a trusted center by introducing consensus mechanisms such as proof of work (PoW), proof of stake (PoS), delegated proof of stake (DPoS), proof of authority (PoA), practical Byzantine fault tolerance (PBFT) and so on [34]. On the basis of the above technology, Kumar et al. [35] fused intrusion detection module, two-level privacy module and trustworthiness module to propose a trustworthy privacy-preserving secured framework (TP2SF), achieving the privacy preservation of smart cities. To have a securer use of distributed data, Arachchige et al. [36] proposed a framework PriModChain that amalgamated Ethereum blockchain, smart contracts, federated machine learning and differential privacy to improve the data privacy and trustworthiness. By combining blockchain with federated learning, Li et al. [37] proposed a crowdsourcing framework CrowdSFL that can realize higher security and less overhead during the implementation of crowdsourcing. Qu et al. [38] proposed an FL-Block scheme to balance the fog computing's performances and the subsequent inefficiency of privacy preservation, deriving the optimal block generation rate by considering computation cost, communication and consensus delays. Although these studies have addressed privacy preservation with good performances, none of them can be directly applied to electricity consumption forecasting.

3 Theory

3.1 Blockchain System Model

The blockchain used in this paper is developed based on Ethereum, whose type is a private chain. As shown in Fig. 1, the core architecture of the blockchain system mainly includes three parts, data layer, network layer and application layer. The data layer is mainly composed of the structure and algorithm for the storage of the blockchain, such as asymmetric encryption, SHA256 algorithm, Merkle tree and chain structure. Among them, SHA256 algorithm is a widely used hash algorithm, which can map the input value with arbitrary length to a 256-bit fixed-length binary value. Each block of the blockchain consists of the previous block hash, node index, timestamp, block storage nodes, current block hash, Markle root and content of metadata. All data is stored with a unique digital signature in the Merkle tree after the operations of twice SHA256 algorithm and asymmetric encryption, ensuring the integrity and the security of the transaction in the blockchain.

The network layer is the top priority of blockchain technology, including transaction pools, consensus mechanism, and block generation. The core problem to be solved by the consensus mechanism is how to reach a consensus even when there are malicious nodes in the chain and the consensus mechanism determines the efficiency and stability of the entire blockchain system. When the power of decision-making is more decentralized, the efficiency of the system reaching consensus is lower. On the contrary, when the decision-making power is more centralized, the system is more likely to reach a consensus but is more dictatorial.

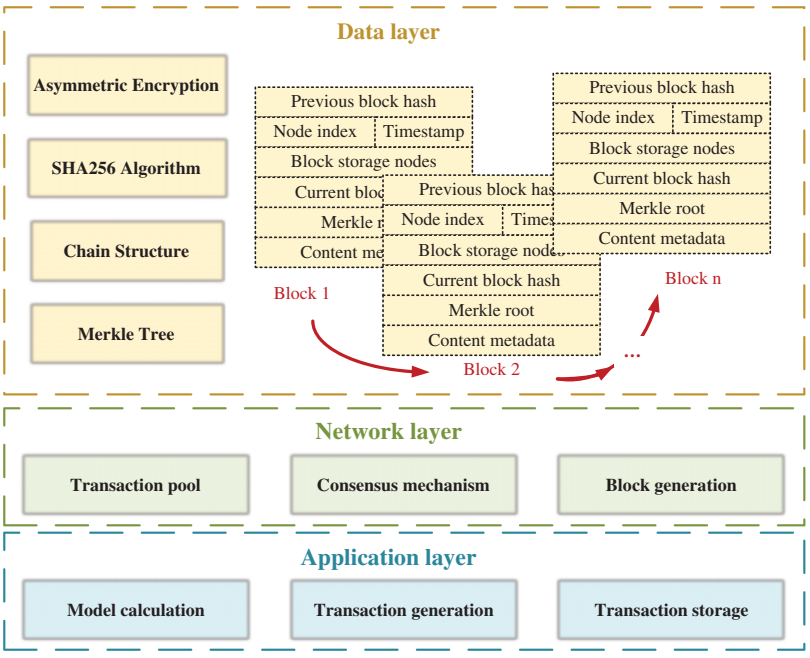

Figure 1: The core architecture of the blockchain system

In this paper, a PoQ consensus mechanism is adopted, which cannot only reduce the computing consumption when compared with the PoW consensus mechanism but also can break the restrictions of the node amount when compared with PBFT consensus mechanism. The role of the PoQ consensus mechanism is to ensure that the nodes are not tampered with and to improve the credibility of nodes with better parameters according to the quality value. By using the PoQ consensus mechanism, malicious attacks in the network can be largely resisted. Each node in the established blockchain system can provide a quality value $Q_{i\to j}^{final}$, which is assessed through the weighting of direct quality value and indirect quality value:

$$Q_{i\to j}^{final} = (1-\lambda)\cdot Q_{i\to j}^{direct} + \lambda \cdot Q_{i\to j}^{indirect} \tag{1}$$

where, $Q_{i\to j}^{direct}$ and $Q_{i\to j}^{indirect}$ are the direct quality value and indirect quality value of the node, respectively, representing the direct quality evaluation and indirect quality evaluation of worker j by task publisher i. The former mainly considers the interaction between the current node and the server while the latter takes other nodes' quality into account. λ is the weight of the quality value. The direct quality value and the indirect quality value can be calculated by:

$$Q_{i\to j}^{direct} = \sum_{y=1}^{Y} \gamma_y \cdot Q_{i\to j} / \sum_{y=1}^{Y} \gamma_y \tag{2}$$

$$Q_{i\to j}^{indirect} = \sum_{k\in K} \varphi_{i\to k} \cdot Q_{k\to j} / \sum_{k\in K} \varphi_{i\to k} \tag{3}$$

where, $\gamma_y = \eta^{Y-y}, \eta \in (0,1), y \in [1, Y]$ is a decay coefficient of freshness used to increase the weight of interaction events that are more recent in time. K indicates a collection of workers interacting with

the task publisher k. $Q_{i\to j}$ is the average test accuracy value of the trained model. The weight factor of indirect quality value $\varphi_{i\to k}$ can be expressed as:

$$\varphi_{i\to k}=\beta_{i\to k}\cdot\frac{\sum_{j\in C}\left(Q_{i\to j}^{direct}-\overline{Q_{i}^{direct}}\right)\cdot\left(Q_{k\to j}^{direct}-\overline{Q_{k}^{direct}}\right)}{\sqrt{\sum_{j\in\Pi}\left(Q_{i\to j}^{direct}-\overline{Q_{i}^{direct}}\right)^{2}}\cdot\sqrt{\sum_{j\in K}\left(Q_{k\to j}^{direct}-\overline{Q_{k}^{direct}}\right)^{2}}} \tag{4}$$

where, $\beta_{i\to k}(\beta_{i\to k}\in[0,1])$ is a constant, representing the weight of quality evaluation form task publisher i to task publisher k during the computation process. $\bar{\cdot}$ represents the operation of averaging. Π indicates a collection of workers interacting with the task publisher i. K indicates a collection of workers interacting with the task publisher k. C indicates a collection of workers interacting with both the task publisher i and the task publisher k. It can be seen that the greater the similarity between task publisher k and task publisher i, the higher the credibility of its quality evaluation.

The role of the application layer is to generate the transactions based on the parameters calculated by the model in a preset format, including training episodes, model accuracy, the size of the local training set, the final value of the quality, the parameters of the initialized global model, and the parameters of the local model, storing them in a transaction pool for on-chain trusted transmission through the digital signatures.

3.2 PoQ-Based Federated Learning

After establishing the electricity consumption data sharing blockchain system for trusted interaction under privacy preservation, we designed a PoQ-based federated learning mechanism by introducing the quality value $Q_{i\to j}^{final}$. Different from other learning frameworks which train network model centrally by accessing all raw data, federated learning is a distributed and privacy-preserving learning framework. In the framework of federated learning, each node can train a global model collaboratively by only using their local data instead of all nodes' raw data. In every episode during the process of federated learning, each node performs local training on top of the initialized global model. After updating the model according to the parameters of the previous node, each node continues to train the local model through its own private electricity consumption data and shares the fine-tuned parameters such as weights and biases through the chain. Algorithm 1 shows the optimization process of the network's model parameter based on federated learning.

Algorithm 1: PoQ-based federated learning

Require: learning rate α, network's model parameters θ, blockchain node p
Ensure: federated learning network's model parameters θ_n^{p+1}

for i = 0; i ≤ n; i++ **do**
  The node chooses a subset of data to train the local model based on the quality value;
The node shares the parameters of the local model to other nodes;
repeat
  $\theta_n^i=\theta_n^{i-1}-\alpha\cdot\nabla f(\theta_n^{i-1})$
until episode > max episode
$Q_{i\to j}^{final}=(1-\lambda)\cdot Q_{i\to j}^{direct}+\lambda\cdot Q_{i\to j}^{indirect}$
end for
$\theta_n^{p+1}=\sum_{i=1}^{n}P(Q_n^p)\cdot\theta_n^p/n$

3.3 MHD-LSTM for Electricity Consumption Forecasting

In order to avoid the gradient disappearance problem, Hochreiter et al. [39] improved the internal structure of the recurrent neural network (RNN), proposing a LSTM network that can handle long-term dependency. As shown in Fig. 2, the LSTM unit is consisted of forget gate, input gate and output gate, which can help the network accomplish the screening and the memory of data. The output of the forget gate is a value from 0 to 1, indicating the level of forgetting of the past time series information, 0 means complete forgetting, and 1 means complete retention. At time t, the forget gate, input gate, and output gate in the LSTM unit are respectively denoted as f_t, i_t, o_t, and their specific working mechanism and information flow calculation process can be expressed as follows:

$$f_t = \sigma\left(W_f x_t + U_f h_{t-1} + b_f\right) \tag{5}$$

$$i_t = \sigma\left(W_i x_t + U_i h_{t-1} + b_i\right) \tag{6}$$

$$o_t = \sigma\left(W_o x_t + U_o h_{t-1} + b_o\right) \tag{7}$$

where, h_{t-1} is the hidden state at time $t-1$, x_t is the input electricity consumption data at time t, W, U and b are the weights and biases of the gate structures, σ is the activation function which can be *sigmoid* or *tanh* [40]. The cell state is a storage unit in the hidden layer, whose input can be expressed as:

$$\widetilde{C}_t = \tanh\left(W_C x_t + U_C h_{t-1} + b_C\right) \tag{8}$$

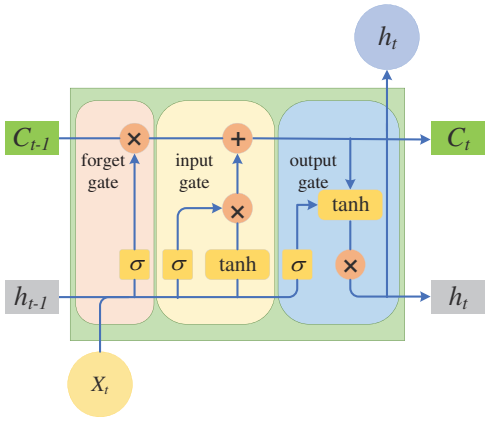

Figure 2: The structure of the LSTM unit

The output of the cell state and the hidden state can be calculated as follows:

$$C_t = i_t * \widetilde{C}_t + f_t * C_{t-1} \tag{9}$$

$$h_t = o_t * \tanh\left(C_t\right) \tag{10}$$

Because of the gate structure and the cell state, the LSTM unit can handle long-term dependencies, so that useful timing information is preserved and transmitted in the network. Considering that electricity consumption data has both forward time dependence and backward time dependence, which reflects the time correlation between the current data and the previous data as well as the subsequent data, a multilayer hybrid directional LSTM structure is used to fully extract the feature information of electricity consumption data. By fully using these two dependences closely related

to the user's habits and the environment, the user's electricity consumption data can be analyzed and forecasted more accurately. As shown in Fig. 3, the proposed MHD-LSTM network consists of two layers of bidirectional LSTM (BLSTM) and one layer of unidirectional LSTM. The former is used as the first few layers of the MHD-LSTM network to learn the bidirectional dependence of electricity consumption data, the latter is used as the output layer of the model to integrate the feature information learned by multiple BLSTM to obtain the final forecasted value.

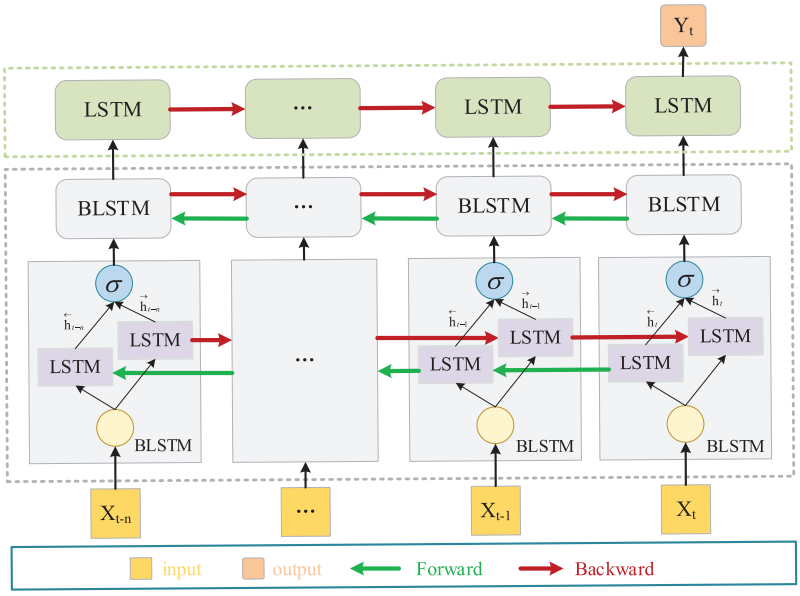

Figure 3: The architecture of MHD-LSTM

4 Results and Discussion

In this paper, all the experiments were conducted in Ubuntu 20.04 system on the server side, including five decentralized distributed nodes. Each node is equipped with a 12th Gen Intel® Core™ i7-12700K 3.6 GHz CPU, 128 GB of RAM, 4 TB hard drive and an NVIDIA GeForce RTX 3070 GPU. In order to verify the effectiveness of the proposed PoQ-based federated learning method in this paper, the users' electricity consumption data of a community in Tianjin from 2017 to 2019 was used. The data were sampled every four hours, and there were 6570 time points in total. More specifically, the electricity consumption data collected from 2017 to 2018 was divided into five parts to serve as the training set, and the data in January 2019 was used for testing. Each part of the training set was stored on a separate node and was assumed to come from a different data management department, which can help to locally train the global MHD-LSTM network's model. After the initialization of the global model was completed, the initialized network's model parameters were stored onto the blockchain by PoQ consensus mechanism, and then they were shared with other nodes. The process included model parameter download, local training update, and model parameter upload. Fig. 4 shows the comparison of the forecasted data with the real data, where the blue curve represents the real data, the red curve represents the forecasted data of MHD-LSTM, and the green curve represents the forecasted data of LSTM. It is not difficult to see that the data forecasted by the proposed MHD-LSTM network is closer to the real data.

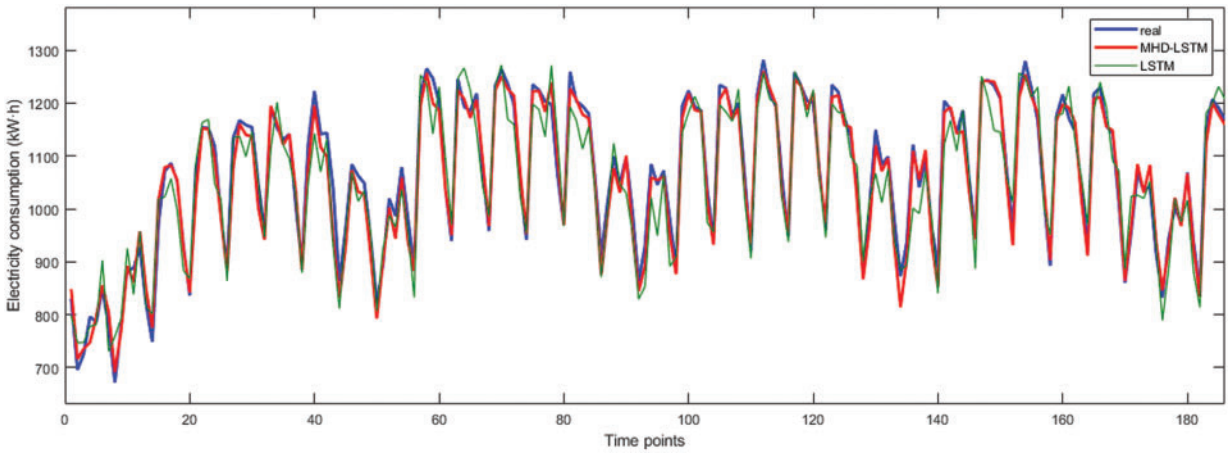

Figure 4: The comparison of the forecasted data with the real data

In order to obtain a more intuitive comparison, four indicators in Table 1 were used to evaluate the forecasting performance, namely: the root mean squared error (*RMSE*), the mean absolute error (MAE), the coefficient of determination (R^2) and the accuracy (*ACC*), which can be expressed as follows [41]:

$$RMSE = \sqrt{\frac{1}{N}\sum\nolimits_{n\in N}(ECD_f(n) - ECD_r(n))^2} \tag{11}$$

$$MAE = \frac{1}{N}\sum_{n\in N}|ECD_f(n) - ECD_r(n)| \tag{12}$$

$$R^2 = 1 - \frac{\sum_{n\in N}\left(ECD_f(n) - ECD_r(n)\right)^2}{\sum_{n\in N}\left(ECD_r(n)\right)^2} \tag{13}$$

$$ACC = 1 - \frac{||ECD_f(n) - ECD_r(n)||_2}{||ECD_r(n)||_2} \tag{14}$$

where, $ECD_f(\cdot)$ is the forecasted electricity consumption data and $ECD_r(\cdot)$ is the real electricity consumption data. It can be seen that, due to the multiple layer structure and the hybrid directional structure, the proposed MHD-LSTM network can fully extract the temporal correlation of the electricity consumption data, thus achieving better forecasting performance when it is compared with LSTM network and BLSTM network.

Table 1: The forecasting performance of LSTM, BLSTM and MHD-LSTM

	LSTM	BLSTM	MHD-LSTM
RMSE	43.3051	29.9655	**22.0157**
MAE	35.6966	24.0591	**17.3011**
R^2	0.9984	0.9992	**0.9996**
ACC	0.9597	0.9721	**0.9795**

In order to verify the defense ability of the proposed PoQ-based method against attacks. The level of attacked blockchain system was set to 10%, 20%, 30%, 40% and 50%, which means the corresponding percentage of the electricity consumption data will be maliciously tampered. Fig. 5 shows the ASR which was defined as attack success rate, under the different levels of malicious attack. The ASR corresponding to the five attack levels were 76%, 84%, 91%, 96%, and 99% respectively when in the absence of blockchain, which were 5%, 8%, 13%, 19% and 26% respectively with the existence of blockchain. We can see that the proposed method using blockchain technology was more robust. The reason why the ASR varied so greatly under the comparison of the two cases is whether blockchain was used. The PoQ consensus mechanism in the blockchain system can not only trace the local update of each node, but can identify attacks by malicious nodes as well, which resulted in much lower ASRs when the blockchain system was attacked maliciously. On the contrary, the method without using blockchain run into trouble in the face of malicious tampering attacks.

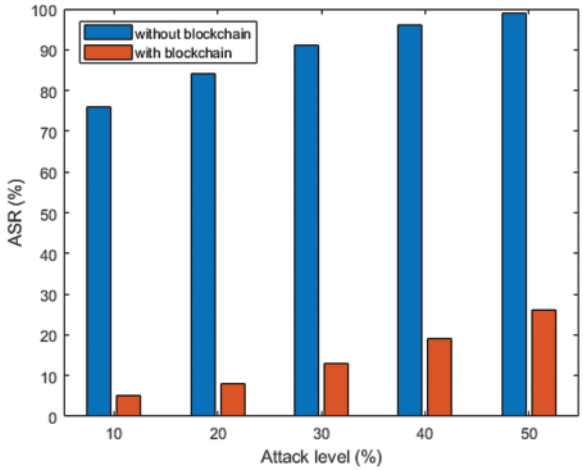

Figure 5: The attack success rate under different levels of malicious attack

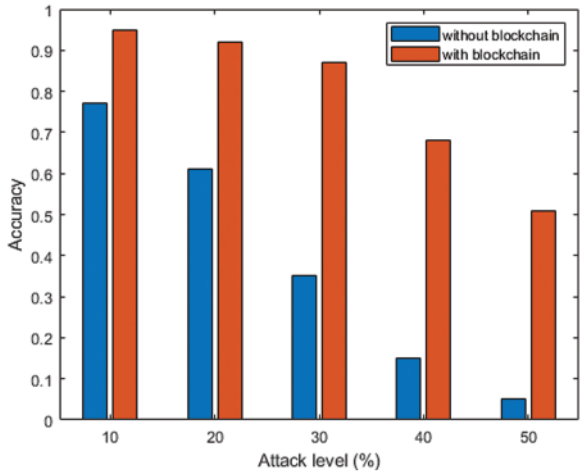

Figure 6: The forecasting performance under different level of attack

Then we conducted an experiment to reveal the impact of using blockchain technology on forecasting performance, demonstrating the superiority of the proposed algorithm. As shown in Fig. 6, the forecasting accuracy of the MHD-LSTM corresponding to the five attack levels were 0.77, 0.61, 0.35, 0.15, 0.05 respectively when there was no use of blockchain, which were 0.95, 0.92.0.87, 0.68 and 0.51 respectively with the use of blockchain. The proposed method can have higher forecasting accuracy than that without using blockchain technology. What's worse, the forecasting performance of the method without using blockchain technology decreased significantly as the level of attack increased.

5 Conclusions

This paper proposed a blockchain-based federated learning method for electricity consumption forecasting. Through the integration of blockchain technology and federated learning mechanism, the proposed method overcomes the privacy preservation problem by sharing the network parameters instead of the raw data itself. Besides, an MHD-LSTM network is applied to verify the performance of the proposed method. When the level of attack is not very high, the proposed method can still have high electricity consumption forecasting accuracy to ensure data privacy. In future works, we will try to deal with performance degradation when there is a high level of attack.

Funding Statement: This work is supported by the Technology Project of State Grid Tianjin Electric Power Company (KJ22-1-47).

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

1. Wang, Y., Chen, Q., Hong, T., Kang, C. (2019). Review of smart meter data analytics: Applications, methodologies, and challenges. *IEEE Transactions on Smart Grid, 10(3),* 3125–3148. https://doi.org/10.1109/TSG.5165411
2. Yuan, X., Du, Z., Li, Y., Xu, Z. (2021). Control strategies for permanent magnet synchronous generator-based wind turbine with independent grid-forming capability in stand-alone operation mode. *Electrical Energy Systems, 31(11),* e13117. https://doi.org/10.1002/2050-7038.13117
3. Yuan, X., Du, Z., Li, Y., Wu, G., Li, J. et al. (2021). Novel cascading scheme of VSC-HVDC with DC voltage synchronisation control for system frequency support. *IET Generation, Transmission & Distribution, 15(24),* 3502–3519. https://doi.org/10.1049/gtd2.12273
4. Wu, H., Zou, M., Ke, Y., Ou, W., Li, Y. et al. (2022). Effect evaluation and intelligent prediction of power substation project considering new energy. *Computer Modeling in Engineering & Sciences, 132(3),* 739–761. https://doi.org/10.32604/cmes.2022.019714
5. Loc, V., Alexander, H. (2021). Stochastic optimization methods in machine learning. In: *Reliability-based analysis and design of structures and infrastructure*, pp. 315–332. UK: CRC Press.
6. Li, Y., Yang, J., Wen, J. (2021). Entropy-based redundancy analysis and information screening. *Digital Communications and Networks*. https://doi.org/10.1016/j.dcan.2021.12.001
7. Zhu, C., Wang, L., Pan, D., Wang, Z., Wang, T. et al. (2023). Research on volt/var control of distribution networks based on PPO algorithm. *Computer Modeling in Engineering & Sciences, 134(1),* 599–609. https://doi.org/10.32604/cmes.2022.021052

8. Su, M., Zhong, Q., Peng, H., Li, S. (2021). Selected machine learning approaches for predicting the interfacial bond strength between FRPs and concrete. *Construction and Building Materials, 270,* 121456. https://doi.org/10.1016/j.conbuildmat.2020.121456
9. Su, M., Peng, H., Yuan, M., Li, S. (2021). Identification of the interfacial cohesive law parameters of FRP strips externally bonded to concrete using machine learning techniques. *Engineering Fracture Mechanics, 247,* 107643. https://doi.org/10.1016/j.engfracmech.2021.107643
10. Li, Y., Yang, J., Zhang, Z., Wen, J., Kumar, P. (2022). Healthcare data quality assessment for cybersecurity intelligence. *IEEE Transactions on Industrial Informatics, 19(1),* 841–848. https://doi.org/10.1109/TII.2022.3190405
11. Ge, J. (2020). ALCencryption: A secure and efficient algorithm for medical image encryption. *Computer Modeling in Engineering & Sciences, 125(3),* 1083–1100. https://doi.org/10.32604/cmes.2021.013039
12. Mcmahan, H., Moore, E., Ramage, D., Hampson, S., Arcas, B. (2016). Communication-efficient learning of deep networks from decentralized data. *The 20th International Conference on Artificial Intelligence and Statistics (AISTATS 2017)*, pp. 1–11. Fort Lauderdale, Florida, USA.
13. Lee, H., Kim, J., Hussain, R., Cho, S., Son, J. (2021). On defensive neural networks against inference attack in federated learning. *IEEE International Conference on Communications*, pp. 1–6. Montreal, QC, Canada.
14. Nandi, A., Xhafa, F. (2022). A federated learning method for real-time emotion state classification from multi-modal streaming. *Methods,* 1–8. https://doi.org/10.1016/j.ymeth.2022.03.005
15. Han, D., Chen, J., Zhang, L., Shen, Y., Gao, Y. et al. (2021). A deletable and modifiable blockchain scheme based on record verification trees and the multisignature mechanism. *Computer Modeling in Engineering & Sciences, 128(1),* 223–245. https://doi.org/10.32604/cmes.2021.016000
16. Yang, J., Wen, J., Jiang, B., Wang, H. (2020). Blockchain-based sharing and tamper-proof framework of big data networking. *IEEE Network, 34(4),* 62–67. https://doi.org/10.1109/MNET.65
17. Pal, S., Rabehaja, T., Hill, A., Hitchens, M., Varadharajan, V. (2020). On the integration of blockchain to the internet of things for enabling access right delegation. *IEEE Internet of Things Journal, 7(4),* 2630–2639. https://doi.org/10.1109/JIoT.6488907
18. Chen, J., Zhang, C., Yan, Y., Liu, Y. (2022). FileWallet: A file management system based on IPFS and hyperledger fabric. *Computer Modeling in Engineering & Sciences, 130(2),* 949–966. https://doi.org/10.32604/cmes.2022.017516
19. Suhail, S., Hussain, R., Jurdak, R., Hong, C. (2021). Trustworthy digital twins in the industrial internet of things with blockchain. *IEEE Internet Computing, 26(3),* 58–67.
20. de Silva, D., Yu, X., Alahakoon, D., Holmes, G. (2011). A data mining framework for electricity consumption analysis from meter data. *IEEE Transactions on Industrial Informatics, 7(3),* 399–407. https://doi.org/10.1109/TII.2011.2158844
21. Chou, J., Hsu, S., Ngo, N., Lin, C., Tsui, C. (2019). Hybrid machine learning system to forecast electricity consumption of smart grid-based air conditioners. *IEEE Systems Journal, 13(3),* 3120–3128. https://doi.org/10.1109/JSYST.4267003
22. Yang, J., Wen, J., Wang, Y., Jiang, B., Wang, H. et al. (2020). Fog-based marine environmental information monitoring towards ocean of things. *IEEE Internet of Things Journal, 7(5),* 4238–4247. https://doi.org/10.1109/JIoT.6488907
23. Kim, N., Kim, M., Choi, J. (2018). LSTM based short-term electricity consumption forecast with daily load profile sequences. *2018 IEEE 7th Global Conference on Consumer Electronics (GCCE)*, pp. 136–137. Nara, Japan.
24. Su, Y., Guo, N., Yang, H. (2019). Combined-LSTM based user electricity consumption prediction in a smart grid system. *2019 IEEE 1st International Conference on Civil Aviation Safety and Information Technology (ICCASIT)*, pp. 292–297. Kunming, China.

25. Ullah, F., Ullah, A., Haq, I., Rho, S., Baik, S. (2020). Short-term prediction of residential power energy consumption via CNN and multi-layer bi-directional LSTM networks. *IEEE Access, 8,* 123369–123380. https://doi.org/10.1109/Access.6287639
26. Abdulrahman, S., Tout, H., Ould-Slimane, H., Mourad, A., Talhi, C. et al. (2021). A survey on federated learning: The journey from centralized to distributed on-site learning and beyond. *IEEE Internet of Things Journal, 8(7),* 5476–5497. https://doi.org/10.1109/JIOT.2020.3030072
27. Jeong, E., Oh, S., Kim, H., Park, J., Bennis, M. et al. (2018). Communication-efficient on-device machine learning: Federated distillation and augmentation under non-IID private data. *The 32nd Conference on Neural Information Processing Systems (NIPS 2018)*, pp. 1–6. Montréal, Canada.
28. Han, C., Yang, T. (2021). Privacy protection technology of maritime multi-agent communication based on part-federated learning. *IEEE/CIC International Conference on Communications in China (ICCC Workshops)*, pp. 266–271. Xiamen, China.
29. Smith, V., Chiang, C., Sanjabi, M., Talwalkar, A. (2017). Federated multi-task learning. *31st Conference on Neural Information Processing Systems (NIPS)*, pp. 4427–4437. Long Beach, CA, USA.
30. Kumar, P., Gupta, G. P., Tripathi, R. (2022). PEFL: Deep privacy-encoding-based federated learning framework for smart agriculture. *IEEE Micro, 42(1),* 33–40. https://doi.org/10.1109/MM.2021.3112476
31. Amato, F., Cozzolino, G., Moscato, F., Moscato, V., Xhafa, F. (2021). A model for verification and validation of law compliance of smart contracts in IoT environment. *IEEE Transactions on Industrial Informatics, 17(11),* 7752–7759. https://doi.org/10.1109/TII.2021.3057595
32. Kumar, R., Kumar, P., Tripathi, R., Gupta, G. P., Islam, A. K. M. N. et al. (2022). Permissioned blockchain and deep learning for secure and efficient data sharing in industrial healthcare systems. *IEEE Transactions on Industrial Informatics, 18(11),* 8065–8073. https://doi.org/10.1109/TII.2022.3161631
33. Kumar, P., Kumar, R., Gupta, G. P., Tripathi, R. (2022). BDEdge: Blockchain and deep-learning for secure edge-envisioned green CAVs. *IEEE Transactions on Green Communications and Networking, 6(3),* 1330–1339. https://doi.org/10.1109/TGCN.2022.3165692
34. Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf
35. Kumar, P., Gupta, G. P., Tripathi, R. (2021). TP2SF: A trustworthy privacy-preserving secured framework for sustainable smart cities by leveraging blockchain and machine learning. *Journal of Systems Architecture, 115,* 101954. https://doi.org/10.1016/j.sysarc.2020.101954
36. Arachchige, P., Bertok, P., Khalil, I., Liu, D., Camtepe, S. et al. (2020). A trustworthy privacy preserving framework for machine learning in industrial IoT systems. *IEEE Transactions on Industrial Informatics, 16(9),* 6092–6102. https://doi.org/10.1109/TII.9424
37. Li, Z., Liu, J., Hao, J., Wang, H., Xian, M. (2020). CrowdSFL: A secure crowd computing framework based on blockchain and federated learning. *Electronics, 9(5),* 773. https://doi.org/10.3390/electronics9050773
38. Qu, Y., Gao, L., Luan, T., Xiang, Y., Yu, S. et al. (2020). Decentralized privacy using blockchain-enabled federated learning in fog computing. *IEEE Internet Things Journal, 7(6),* 5171–5183. https://doi.org/10.1109/JIoT.6488907
39. Hochreiter, S., Schmidhuber, J. (1997). Long short-term memory. *Neural Computation, 9(8),* 1735–1780. https://doi.org/10.1162/neco.1997.9.8.1735
40. Yang, J., Zhu, Y., Jiang, B., Gao, L., Xiao, L. et al. (2018). Aircraft detection in remote sensing images based on a deep residual network and super-vector coding. *Remote Sensing Letters, 9(3),* 229–236. https://doi.org/10.1080/2150704X.2017.1415474
41. Yang, J., Sim, K., Lu, W., Jiang, B. (2019). Predicting stereoscopic image quality via stacked auto-encoders based on stereopsis formation. *IEEE Transactions on Multimedia, 21(7),* 1750–1761. https://doi.org/10.1109/TMM.6046