Federated-Learning Based Privacy Preservation and Fraud-Enabled Blockchain IoMT System for Healthcare

Abdullah Iakhan, Mazin Abed Mohammed, Jan Nedoma, *Senior Member, IEEE*, Radek Martinek, *Senior Member, IEEE*, Prayag Tiwari, *Member, IEEE*, Ankit Vidyarthi, Ahmed Alkhayyat, and Weiyu Wang

***Abstract*—These days, the usage of machine-learning-enabled dynamic Internet of Medical Things (IoMT) systems with multiple technologies for digital healthcare applications has been growing progressively in practice. Machine learning plays a vital role in the IoMT system to balance the load between delay and energy. However, the traditional learning models fraud on the data in the distributed IoMT system for healthcare applications are still a critical research problem in practice. The study devises a federated learning-based blockchain-enabled task scheduling (FL-BETS) framework with different dynamic heuristics. The study considers the different healthcare applications that have both hard constraint (e.g., deadline) and resource energy consumption (e.g., soft constraint) during execution on the distributed fog and cloud nodes. The goal of FL-BETS is to identify and ensure the privacy preservation and fraud of data at various levels, such as local fog nodes and remote clouds, with minimum energy consumption and delay, and to satisfy the deadlines of healthcare workloads. The study introduces the mathematical model. In the performance evaluation, FL-BETS outperforms all existing machine learning and blockchain mechanisms in fraud analysis, data validation, energy and delay constraints for healthcare applications.**

***Index Terms*—Blockchain, cloud, federated learning, fraud-analysis, fog, healthcare, IoMT, privacy preservation.**

Manuscript received 19 January 2022; revised 22 March 2022; accepted 4 April 2022. Date of publication 8 April 2022; date of current version 6 February 2023. This work was supported by the Ministry of Education of Czech Republic under Projects SP2022/18 and SP2022/34. (*Corresponding authors: Prayag Tiwari; Ankit Vidyarthi.*)

Abdullah Iakhan is with the College of Computer Science and Artificial Intelligence, Wenzhou University, Wenzhou 325035, China (e-mail: abdullah@seu.edu.cn).

Mazin Abed Mohammed is with the College of Computer Science and Information Technology, University of Anbar, Anbar 31001, Iraq (e-mail: mazinalshujeary@uoanbar.edu).

Jan Nedoma is with the Department of Telecommunications, VSB-Technical University of Ostrava, 70800 Ostrava, Czech Republic (e-mail: jan.nedoma@vsb.cz).

Radek Martinek is with the Department of Cybernetics and Biomedical Engineering, VSB-Technical University of Ostrava, 70800 Ostrava, Czech Republic (e-mail: radek.martinek@vsb.cz).

Prayag Tiwari is with the Department of Computer Science, Aalto University, 02150 Espoo, Finland (e-mail: prayag.tiwari@ieee.org).

Ankit Vidyarthi is with the Department of CSE&IT, Jaypee Institute of Information Technology Noida, Noida 201309, India (e-mail: dr.ankit.vidyarthi@gmail.com).

Ahmed Alkhayyat is with the College of Technical Engineering, The Islamic University, Najaf 54001, Iraq (e-mail: ahmedalkhayyat85@iunajaf.edu.iq).

Weiyu Wang is with the Business School of Changzhou University, Jiangsu 213164, China (e-mail: weiyuwang001@gmail.com).

Digital Object Identifier 10.1109/JBHI.2022.3165945

I. Introduction

THE utilization of digital healthcare applications based on the Internet of Medical Things (IoMT) system has been increasing day by day [1]. The IoMT system collects different medical devices, wireless technologies, and fog and cloud nodes distributed throughout the network. The IoMT offers different services to digital healthcare applications and is generally called IoT-enabled digital healthcare applications. This digital healthcare consists of other applications in which IoT-enabled services provide ubiquitous connectivity to the users to monitor their healthcare 24/7. The digital healthcare IoT applications store and migrate user data via different connected nodes such as wireless technologies and fog and cloud computing nodes for processing. Artificial intelligence-enabled many dynamic methods help applications manage their execution and data storage in the IoT fog cloud network. Furthermore, existing artificial intelligence techniques are proposed to deal with the privacy preservation and fraud anomaly detection issues in the network. IoT applications with blockchain pursue various anomaly detection techniques on transactional network data of a public financial blockchain called bitcoin [2]. This blockchain-enabled solution is a prototype for a study that examines anomaly detection in the context of blockchain technology and its financial applications. It uses unsupervised machine learning techniques to remove transactional data from the bitcoin blockchain and analyze it for malicious transactions [3].

Federated learning is an artificial intelligence paradigm that concedes computing nodes to find out from a shared model collaboratively. It works by allowing individual model training on separate, independent IoMT data of applications while only sharing the trained models, which do not contain any personal data. The user devices train their applications data locally and shared to the global computing model for execution. This process is repeated for several iterations until a high-quality model is generated [3]. The decentralized blockchain is the technology

2168-2194 © 2022 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission.
See https://www.ieee.org/publications/rights/index.html for more information.

Authorized licensed use limited to: Deakin University. Downloaded on May 22,2024 at 07:34:40 UTC from IEEE Xplore. Restrictions apply.

that encourages the IoT applications to execute at different nodes in the fog-cloud network [4]. The blockchain technology can be implemented at the client-side and server-side with different schemes such as smart-contract, miners, consensus, and different fault-tolerant schemes [5]. However, static rules-based blockchain still suffers from dynamic frauds and scams, and the static learning process in existing blockchain systems did not work efficiently in the dynamic environment.

This paper formulates federated learning-based privacy preserving and fraud detection-enable blockchain IoMT system for healthcare applications in fog-cloud assisted network. The study suggests a new system that leverages different technologies such as federated learning and blockchain technology is a decentralized fog and cloud computing network. The research reduces the security risk, energy, delay, and deadline of applications. The study devises a new dynamic detection Federated Learning-Based Fraud Detection-Enable Blockchain System for IoT healthcare applications in Fog-Cloud. The study divides the learning process into local learning models at each fog node and then shared to the global master node to efficiently deal with the entire system. The study formulates this problem as the scheduling problem and makes the following efforts to solve the considered problem.

- The study devises a novel federated learning aware fraud-detection enables blockchain IoMT system where the fraud of data and validation of data and execution energy and delay being minimized as shown in Fig. 1. The system consists of different layers, such as an application layer consisting of interrelated applications that share data to process their goals in the network. The fog-node layer consists of varying fog nodes federated and fraud blockchain and trains the models at different nodes to avoid any attack on the storage between various transactions. The fog-cloud agent (FCA) is the master node that schedules all requested work based on shared models to the global federated learning model.
- The research devises the framework-based FL-BETS consisting of different heuristics to solve the problem in different sub-steps. The heuristics are fraud detection, blockchain scheme, and task scheduling in the framework. The goal is to process the entire workload of applications in a different process to validate their quality of service requirements.
- The study implemented fog nodes near the user applications to store and train the data to avoid dynamic fraud in blockchain-enabled with hashing and different primitive. The local train model shared their training model and the FCA's global train model to ensure the system's overall performance.
- The scheduler is the dynamic, iterative method that schedules all workloads' must be completed with their deadlines on to the different fog nodes based on their training model and blockchain requirements. The scheduler is non-preemptive, which will not interrupt any process during execution at the node. Rescheduling will be possible whenever any failure occurs in the system.

The manuscript has the subsequent sections. Section II shows the efforts of existing studies in literature state of the art.

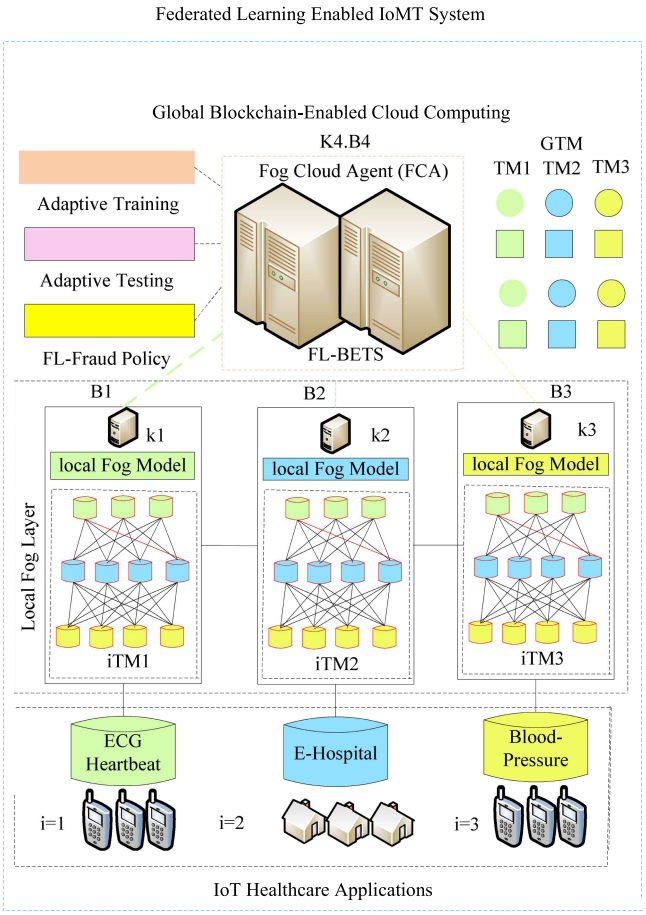

Fig. 1. Federated learning aware blockchain enabled IoMT for IoT healthcare applications.

Section III shows the problem-solution based on the proposed architecture, and section IV shows algorithm implementation based on heuristics steps. Section V determined the performances of the proposed schemes with the considered problem. Section VI summarizes the effort of the proposed work with the achievement of the results.

II. Existing Related Work of IoMT System

These days, Internet of Medial Things (IoMT) system enabled applications are growing progressively to solve different daily life issues. The most reason is that each traditional application is connecting to the web via different sensors and actuators. Whereas many traditional machine learning schemes supported supervised, unsupervised, and reinforcement learning are proposed to coach the models of IoT data within the fog cloud network. Blockchain technology is widely deployed at distributed fog-cloud networks. However, the traditional training model of machine learning suffered from overhead, lateness, accuracy, and lots of factors during the training of IoT workload within the system.

This work [1] devised the IoMT system based on different machine learning models for the applications. Recently, federated learning solved the matter of the normal machine learning model and trained the various models at local devices, and shared with the most servers as wiped out for the healthcare applications [6].

Authorized licensed use limited to: Deakin University. Downloaded on May 22,2024 at 07:34:40 UTC from IEEE Xplore. Restrictions apply.

The most goal of this studies to train the various models of applications at mobile devices during the processing of healthcare applications. The CNN and KNN based federated learning aware training models based suggested in studies [2]–[4]. The goal is to attenuate the energy consumption of devices during training the models locally and share them with the near fog servers for further manipulations. However, these studies still didn't consider the security of distributed computing.

Security and Privacy-aware federated learning supported blockchain suggested in [5], [7], [8] for smart-home applications in the mobile edge cloud and fog computing. The goal is to scale back the delay of applications and provide security to the sensitive data of applications during processing outside the devices. The energy optimization aware blockchain supported federated learning-based system suggested in [9]–[11]. The shared and native training models were considered because the objective with the minimization of energy consumption of mobile devices and communication networks. However, existing virtual machine-based systems are still affected by the delay.

The lightweight IoMT aware decentralized federated learning for E-healthcare applications suggested in [12]–[20]. The goal is to attenuate the wait delay, service delay and validate the info in several nodes. These studies suggested different machine learning algorithms like deep reinforcement learning schemes that supported Markov Model and optimized the multi-objective supported weighting and Pareto optimal. However, the proposed work is different from the state of art studies.

The studies [21]–[25] suggested the federated learning-enabled technology in the fog cloud-aware IoT system was devised for the different applications. These studies devised a blockchain-enabled, secure data-sharing architecture for multiple parties. These studies devised the privacy of data is well-maintained by sharing the data model instead of revealing the actual data. Finally, we integrate federated learning into the consensus process of permissioned blockchains so that the computing work for consensus can also be used for federated training. Numerical results derived from real-world datasets show that the proposed data sharing scheme achieves good accuracy, high efficiency, and enhanced security. However, these studies only considered the homogeneous fog and cloud nodes in their work. These studies considered intelligent transport applications and industrial applications with the only security constraint in their work. However, security, privacy, and deadlines for healthcare applications are widely ignored in work.

The study highlights the dynamic security and privacy challenges and their solutions in the manuscript to the state-of-the-art studies. The study devises federated learning-based blockchain-enabled task scheduling (FL-BETS) in the IoMT system for healthcare applications, which analyzes different constraints for optimization, such as validation, delay, and optimization under deadline for healthcare applications. The closely related studies [18]–[20] suggested trust and blockchian enabled for healthcare applications in the distributed network. However, they did not consider the delays, fraud, energy, and deadline constraints of the problem inside the formulation. These studies exploited traditional machine learning models for training and testing inside the fog and cloud nodes for healthcare IoT applications. However, these models have a lot of consumption of resources, energy, and time and often miss the deadlines for applications.

Federated-Learning Aware Training-Based Privacy Preservation and Fraud-Enabled Blockchain The IoMT System obtained authentication and authorization issues and threat attacks. The federated learning approach enables the different nodes to train and test their privacy and security models independently and share them with the global model node for processing. It is the more efficient mechanism used in the traditional privacy and security mechanisms of machine learning for IoMT applications.

III. Proposed Solution

The study devised the federated learning distributed training modeling enabled privacy preserving and fraud detection in blockchain enabled IoMT system for the Internet of Things (IoT) healthcare applications as shown in Fig. 1. The IoMT system consists of applications, fog nodes, and fog-cloud nodes with the container microservices. The system considered the I number of IoT applications such as E-Healthcare, E-Transport, and Smart-Homes. Each application i is coarse-grained and fully offloads the workload W_i to Fog-Cloud Agent (FCA) for further processing. The number of computing nodes K are geographically distributed at different places in the network. Each node k can train the data model of all IoT applications and can share with FCA and other nodes in the network. The FCA decides on the trained model at local fog nodes and achieves how to reduce applications' energy consumption and latency and execute them under their deadlines. The study devises FL-BETS algorithm framework that consists of different dynamic heuristics as shown in Algorithm 1 This research uses machine learning to implement multiple, self-improving, and maintainable fraud detection models. We demonstrate how to train supervised and unsupervised machine learning models on historical transactions to predict whether incoming transactions are fraudulent or not.

A. Problem-Formulation of Research

In the research problem, the model consists of I number of IoT healthcare applications, i.e., $\{i = 1, \ldots, I\}$, where $\{W_i = 1 \in I\}$ demonstrates their workloads under their deadlines D_i. The proposed model consists of I number of coarse-grained healthcare applications, e.g., $\{i = 1, \ldots iI\}$. For executing the workload, the study suggests the hybrid paradigm enabled fog and cloud nodes that are represented by $\{k = 1, \ldots, K\}$ with their different speed ζ_k and resources r. The blockchain technology with schemes implemented inside nodes with other blocks, e.g., $\{B = 1, \ldots, N\}$. Each blockchain blocks B inside the particular node k has various attributes such as current block number, current hashing, previous hashing, transaction data, fraud enabled, and validation schemes.

1) Security and Privacy Model: The study devised the symmetric based security model inside blockchain technology in which encryption and decryption done based on advance encryption standard (AES). The blockchain technology by default exploited SHA-256 security algorithm with the public key and private key during blockchian mechanism during distributed

Authorized licensed use limited to: Deakin University. Downloaded on May 22,2024 at 07:34:40 UTC from IEEE Xplore. Restrictions apply.

TABLE I
PROBLEM NOTATIONS

Notations	Aims and Definition
I	Set of healthcare coarse-grained applications
i	i^{th} workload of I applications
D_i	Deadline of the workload i as the hard constriant
W_i	Workload of application i
K	A set fog and cloud computing-nodes
k	The k^{th} computing-node of K
$k-watt$	Power consumption of node as the soft constraint
ϵ_k	Particular k resource
ζ_k	The processing speed of node k
N, B	A set of blockchains blocks and particular block
TM_i	Training and testing model of workload i
$x_{i,k,B}$	Assignment of workload one at a time

ledger data in fog cloud network. The study devised the privacy model and analyzed the fraud detection to avoid from any privacy issue in the work. The study train and test the model based on federated learning in the distributed blockchain technology.

2) Local Training Model and Blockchain: Initially, the system will decide offloaded workload from IoMT application finds particular node or not on the base of following equation.

$$x_{W_i,k} = \begin{cases} Assign & = 1, \\ NotAssigned & = 0. \end{cases} \tag{1}$$

Equation (1) determines the either offloaded workload has been assigned to any particular node or waiting for assignment in the system. After the workload assignment to any node, the training and testing analysis sets are divided into training, testing, and validation in the following way.

$$Training = \frac{W_i}{\zeta_k} \times \{w = 1, \ldots, W_i\}. \tag{2}$$

Equation (2) takes raw data (e.g., audio, video, image, text) and identify them based on pattern of data and similar pattern data store in the one cluster.

$$Valid = Training \times W_i. \tag{3}$$

Equation (3) validated the cluster workloads w_i of similar group based on their patterns in the system.

3) Global Model and Blockchain: The study introduces the local and global validation based on blockchain mechanism in the study. The goal is to reduce the security risk, delay and processing cost of applications in the system. Table I) defines the description of the symbols for the problem.

B. Placement of Fog and Cloud Nodes

The fog nodes are placed very near medical applications, such as fog nodes located at different hospitals and offering service at the localization. However, the centralized cloud is located multiple hops away from user applications and has high latency but less resource cost. The study considered the heterogeneous fog cloud nodes as the joint optimization resources for healthcare applications to keep the resource balance between fog nodes and cloud. All the fog and cloud nodes are decentralized they can share data with the blockchian hashing and make validation based on the proof of work method.

C. Multi-Constraints Optimization of the Problem

The study considers the different constraints to formulate the problem, such as data validation, accuracy, resource utilization which are sets of the delay and processing cost objectives functions.

D. Processing Delay

Initially, the study calculates the validation delay of data in the following way.

$$Validation - Delay = x_{W_i,k} \times Valid. \tag{4}$$

Equation (4) ensures the validation delay of the single workload in the system. The blockchain and execution are calculated in the following delay.

$$Execution - Delay = Hashing - time + \frac{W_i}{\zeta_k} \times x_{W_i,k} + Fraud - Analysis. \tag{5}$$

Equation (5) determines the execution delay of workload i.

$$Hashing - time = W_i \leftarrow k, B \leftarrow (SHA - 256). \tag{6}$$

Equation (6) determines the encryption and decryption inside blockchain for workload i.

$$Fraud - Analysis = W_i \leftarrow k, B \leftarrow Data - index. \tag{7}$$

Equation (7) determines the fraud analysis of workload i. The power consumption nodes depends upon the blockchain validation and fraud analysis for each workload to be determined in the following way. The total delay of workload to be determined in the following way.

$$Delay = Execution - Delay + Hashing - time + Fraud - Analysis. \tag{8}$$

Equation (8) to be determined the all delays of workload i.

$$Power - Consumption = Watt \times Delay. \tag{9}$$

Equation (9) determines the power consumption due to all execution, blockchain and fraud analysis process in the node for workload. The problem mathematically formulated as follows.

$$\sum_{i=1}^{I}\sum_{k=1}^{K}\sum_{B=1}^{N} \min Delay, Power - Consumption. \tag{10}$$

Subject To

$$\sum_{i=1}^{I}\sum_{k=1}^{K}\sum_{B=1}^{N} W_i, k, B \leq D_i, \forall i = 1, \ldots I. \tag{11}$$

All workloads executed under their deadlines as determined in equation (11).

$$\sum_{i=1}^{I}\sum_{k=1}^{K}\sum_{B=1}^{N} W_i, k, B \leq \epsilon_k, \forall k = 1, \ldots K. \tag{12}$$

All workloads executed under their resource limitation of nodes as determined in equation (12).

Authorized licensed use limited to: Deakin University. Downloaded on May 22,2024 at 07:34:40 UTC from IEEE Xplore. Restrictions apply.

Algorithm 1: FL-BETS Algorithm.

Input : I, W, TM, K ;
begin
  for *(i=1 to k=1 to K)* **do**
    Call Algorithm 2 order all workload based on their deadlines;
    Algorithm 2 accepts input at a time instead of random arrival in the system;
    Sorting $i \leftarrow W_i, \in I$;
    Searching and mapping $k \leftarrow \epsilon_k, D_i, \in K$;
    Call Algorithm 3 to train and test the data on different local nodes;
    Apply training and testing based on federated learning at different nodes k, W_i, TM;
    Call blockchain Algorithm 4 to store secure data at different nodes with adaptive validation;
  End Inner condition
End main

IV. Proposed FL-BETS Strategy Framework

In this section, the study shows the processes of FL-BETS framework which consists of different heuristics as shown in Algorithm 1. The FL-BETS consists of different processes and different schemes in the following way. The study considered the workload assignment problem which is to be solved in polynomial time that is workload deadline in the work. Generally, all the workload assignment problem are NP-Hard problem and to be solved within deadline.

Algorithm 1 takes the different constraints as the input, e.g., I, W, TM, K and process them into different phases. Algorithm 1 is the framework which consists of different strategies as discussed in problem description and solve the problem in different steps. Each strategy to be explained in different sub-sections.

A. Deadline Enabled Sorting and Scheduling

All the workloads have a fixed deadline and are known in advance in our work. All the workloads are submitted together in the system at a time. Therefore, all the workloads are sorted and scheduled based on our work's lowest deadline first scheduling method. In this paper, the deadline enabled scheduler which is the preemptive method that schedules the workload based on its deadline and privacy and security constraints. If the workload fails due to privacy or security issues, the scheduler will reschedule the workload on the different fog and cloud nodes highlighted in the manuscript.

Algorithm 2 sorts the all workloads based their deadlines. All the nodes are sorting according to their energy and delay constraints in network. All the workloads must be executed under the available resources of nodes until and unless the assigned workloads finished their executions.

B. FL-Fraud-Detection and Security Preserving Policy

Adaptive training and testing means training and testing different models on different fog nodes and sharing them with the centralized cloud for computation. Based on their training and testing models, all the trained and tested workloads avoid fraud attacks and privacy issues. The study devises the federated learning-enabled fraud detection (FL-Fraud) and privacy preserving policy in which training and testing progress on the healthcare workloads by analyzing the fraud detection in the fog cloud environment as shown in Fig. 2. The fog and cloud nodes are implemented at different layers where local federated models are trained on the fog nodes and shared to the global cloud computing for the blockchain-enabled storage in the system. FL-fraud trains the model to discover fraud patterns based on proposed adaptive training and testing model enabled federated learning-enabled policy. The model is self-learning; it can adapt to new and unexpected fraud patterns. The study categorized the fraud pattern into two mechanisms: known pattern and unknown pattern. The applications offload their workloads to the locally available fog nodes for further processing (e.g., training and testing) before execution to the global node. The proposed algorithm initially assigned the particular pattern to each workload and offloaded them to the respective available fog nodes. The existing proof of work and proof of stake consensus employ the smart-contract rule to practice the fraud on data and validation between nodes in the blockchain-enabled network. However, these are static rules; therefore, machine learning-enabled fraud detection based on random-forest has been implemented in the blockchain to handle the dynamic fraud in the network. However,

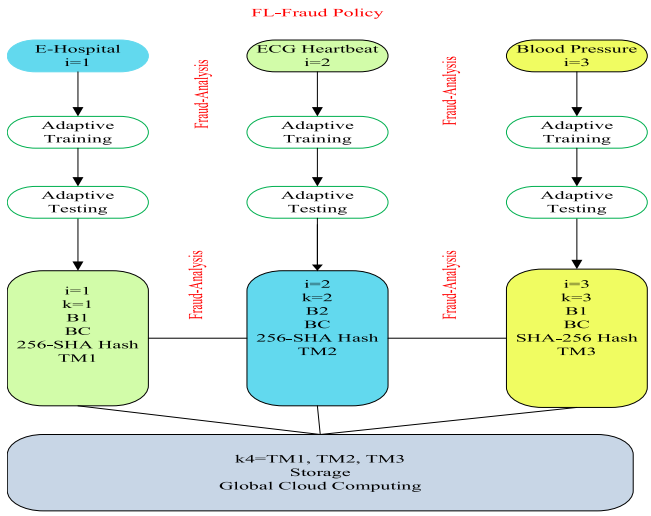

Fig. 2. Federated learning fraud-detection analysis and policy.

Algorithm 2: Delay, Energy and Deadline Efficient Scheduling.

Input : {i=1,..., I},{k=1,...,K}, $\{TM = 1, \ldots, TM\}$;
begin
  Schedule all workloads based on equation (5). Check the validation resources based on equation (12);
  Check the consumption of nodes based on equation (9);
  if *($W_i \leq \epsilon_k$)* **then**
    Apply Schedule-list[$i \leftarrow k \leftarrow TM$];

Authorized licensed use limited to: Deakin University. Downloaded on May 22,2024 at 07:34:40 UTC from IEEE Xplore. Restrictions apply.

Algorithm 3: Adaptive Training and Adaptive Testing.

Input : Schedule-list[$i = 1 \leftarrow k1 \leftarrow TM$ to $WI \leftarrow K \leftarrow GTM$], $Fraud[list]$;

```
begin
    foreach (i = 1 ← TM1.k1 to I ← K.GTM) do
        if (i ← TM.k.Matched.Fraud[list]) then
            Training-i ← TM.k ← 80%.status=Tempt;
            Test-i ← TM.k ← 20%.status=Tempt;
        else
            i ← TM.k.status=Success;
            i ← TM.k to GTM ∀k = 1, . . . , K;
End-Loop;
```

central machine learning fraud-detection algorithms based on random-forest, artificial neural network, and consensus validation has delay issue in the centralized training and testing model for the processing. Therefore, the proposed FL-Fraud policy delays optimal and accurate handling of known and unknown fraud in the system.

In the algorithm, GTM represents the global training model based on federated learning, whereas $k.TM$ is the federated learning model of fog node in the IoMT system. Algorithm 3 scheme determines any fraud if there are any chances of tempered data between different blocks in the blockchain network. Initially, all models train at other nodes and share the fraud details and the master node FCA in the system. This way, any dynamic fraud can detect easily in the system. Algorithm 3 uses machine learning to implement multiple, self-improving, and maintainable fraud detection models. Algorithm 3 demonstrates supervised and unsupervised machine learning models to train the local and global model on historical transactions to predict whether incoming transactions are fraudulent or not.

C. Federated Learning Enabled Fraud-Validation of Blockchain Process and Consensus Method

In this session, the study shows the fraud and validation enabled blockchain process and consensus method for workloads in the system. The existing blockchain consensus methods widely ignored the delay and energy aspects while evaluating the intrusion and validation of the nodes in the system. The study devises the lightweight blockchain consensus, which is delay and power-efficient and more effective to find the intrusion and delay with minimum consumption.

The study devises the privacy preserving mechanism in terms of malware detection in the system. The goal is to safe data or access control of nodes from malware attacks in the system. The time complexity of the method to be determined by n number of searching rounds and n of improvement during execution in the system. Therefore, it is equal to $log(n \times n)$ in the security and privacy method. Algorithm 4 determined the fraud and validation analysis of workload at different nodes and trained them locally and shared to the global node. As shown in Fig. 2, the study analyzes the fraud from local sensor data to local train fog node with the hashing pattern and fraud pattern. The initial pattern, e.g., pattern' design during adaptive local training and testing models (e.g., 80% training and 20%) in the model. Then further sharing to the remote cloud, the pattern" is matched on the original data without affecting any intrusion or attacks. If there is an attack from a list of intrusion data (e.g., data), the algorithm will recover them until it gets the original pattern of a particular node.

Algorithm 4: Federated Learning Enabled Fraud-Validation and Privacy Preserving of Blockchain Policy in Fog-Cloud Paradigms.

Input : Schedule-list[$i \leftarrow k \leftarrow TM$],$\{B = 1, \ldots B\}$, Data

```
begin
    Data=is fraud text to be included in original workload;
    Pattern= Pattern of the encrypted and decrypted data;
    Apply Encryption and Decryption based on equation (6);
    Pattern=k, B, W_i ← TM initial pattern of encrypted workload;
    Pattern'=k, B, W_i ← TM offloading from sensor to local fog node;
    if (Pattern≠ Pattern') then
        Apply security preserving;
        Determine the fraud based on equation (7);
        Pattern← Data (list of fraud or unknown attack);
        Determine the extra available resource based on equation (12);
        Determine the fraud analysis delay based under the deadline based on equation (8) and equation (11);
        Determine the power consumption of fraud analysis based on equation (9);
    else
        Train and validated Pattern on local fog nodes based on (3) and (3) equations;
    if (Pattern'≠ Pattern") then
        Analyze the fraud between local train models to cloud storage model based on first given condition;
```

V. Experimental Setting and Results

In this paper, the study devised the federated learning-enabled policy to minimize the energy of fog-cloud nodes and reduce the delay of applications in the blockchain-enabled network. Malfeasance systems are constantly rising in an IoT-enabled fog-cloud setting. Rule-based fraud detection systems have traditionally been used to mitigate online fraud, but they rely on a static collection of rules adaptive and intelligent experts. This research uses machine learning to implement multiple, self-improving, and maintainable fraud detection models. We demonstrate how to train supervised and unsupervised machine learning models on historical transactions to predict whether incoming transactions are fraudulent or not. We also explain how to deploy the models to a REST API to incorporate into

Authorized licensed use limited to: Deakin University. Downloaded on May 22,2024 at 07:34:40 UTC from IEEE Xplore. Restrictions apply.

TABLE II
NODES SPECIFICATION OF RESOURCES

K	$\epsilon_j(GB)$	Core	ζ_j(MIPS)	ϵ_k
k_1	2000000	1	10000	10000PW
k_2	500000	1	5000	1000PW
k_3	1000	1	1000	500PW
k_4	100000	4	10000	500000PW

an existing business software framework once trained. This paper widely exploits a demonstration of the method using an anonymized data transactions dataset.

A. Privacy Preservation Fraud Data Provider Healthcare Dataset for Experiment

One of the most severe issues facing Medicare is provider fraud. According to the government, Medicare spending grew tremendously due to Medicare claim fraud. Healthcare fraud is an organized crime where peers, providers, physicians, and beneficiaries, collaborate to file false claims. A thorough examination of Medicare data has revealed many doctors who commit fraud. They exploit vague diagnosis codes to justify the most expensive treatments and drugs. The most vulnerable institutions affected by these unethical acts are insurance companies. As a result, insurance companies have raised their prices, and healthcare is growing more expensive by the day. Fraud and abuse in the healthcare system can take various forms. The following are some of the most typical types of provider fraud: (i) Charging for services that are never rendered. (ii) Submitting a claim for the same service twice. (iii) Falsifying information about the service delivered. (iv) Billing for a more complicated or costly service than was supplied. (v) Billing for a covered service when the service was not performed.

This study aims to "predict possibly fraudulent suppliers" based on their claims. We will also find significant variables that will aid in the detection of possibly fraudulent providers' behavior. Furthermore, we will investigate fraudulent tendencies in provider claims to better predict provider behavior in the future. The Dataset's Introduction, We're looking at inpatient claims, outpatient claims, and beneficiary information for each provider for this project. Let's look at their specifics: (i) Inpatient Information reveals the claims filed for patients admitted to hospitals. It also includes information such as their admission and discharge dates, and they admit d diagnostic code. (ii) Outpatient Information. This information reveals the claims filed by patients who visit hospitals but are not admitted. (iii) Information on the Beneficiary information such as health conditions, region of residence, and so forth. Table II elaborate the resource specification of system with different configuration, such as speed, memory, and power consumption in study. The study exploited stratigraphic statistics tool to get the graphical results on the generated data in the work.

B. Medical Application Workload

The study gets the three different workload as the coarse-grained from Kaggle such as ECG heartbeat as images, E-Heart videos and images and blood pressure as the numeric text and process them in the system during execution. The detail of workload shown in Table III. Table III also configured the parameter setting of federated learning and its processing and validation time as the values TM for the simulation in the system.

TABLE III
IOMT APPLICATION WORKLOAD

i	Input	W_i(MB)	D_i	Federated-Learning
i=1	Images-Tasks	1000(MB)	1000 (ms)	TM1=500 (ms)
i=2	Videos-Tasks	1300(MB)	2000 (ms)	TM2=700 (ms)
i=3	Text-Tasks	1028(MB)	2800 (ms)	TM3=800 (ms)

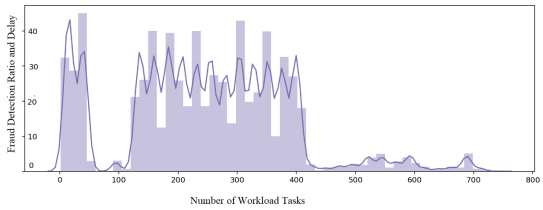

Fig. 3. Adaptive training and testing fraud data.

C. Federated Learning Training Model

The study suggested the federated learning aware training model with trained the different dataset of IoT applications on different fog nodes and shared with the main server fog-cloud agent (FCA). All nodes can train dataset model of all applications and easily shared to each other as shown in the following implementation. %beginlstlisting The source, as mentioned earlier code defined the blockchain implementation in IoT systems with different steps. The study implemented the following baseline approaches in the experimental part, which are closely similar to the proposed work and already discussed in the related work part.

- Baseline 1: These machine learning enable methods [1]–[3], [6] inside blockchain technology for fraud detection are widely exploited to train the healthcare model and e-transport and smart-home models. Data mining is used to classify automatically, cluster, and segment data and uncover relationships and rules in the data that may indicate intriguing trends, such as fraud tendencies. Expert systems that encode expertise in the form of rules for identifying fraud.
- Baseline 2: These dynamic machine learning methods [4], [5], [7]–[9] are widely exploited to train the healthcare model and e-transport and smart-home models. The study implemented all traditional machine learning training models and implemented blockchain, including scheduling and energy efficiency in fog-cloud methods.

D. Fraud Analysis

Fig. 3 shows the performances of the proposed algorithm on the fraud data in the system. From Fig. 3 it can be observed that, initially, the ratio of fraud and delay is high such as 60 to 80. After that, the system learns the adaptive training and testing and improves both the fraud ratio and delay with the minimum loss as shown in Fig. 3.

Authorized licensed use limited to: Deakin University. Downloaded on May 22,2024 at 07:34:40 UTC from IEEE Xplore. Restrictions apply.

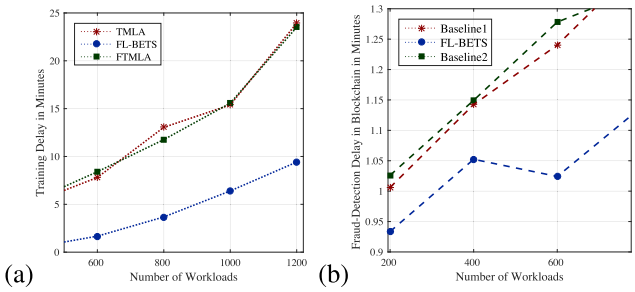

Fig. 4. Delay performance of IoMT applications with different numbers of tasks.

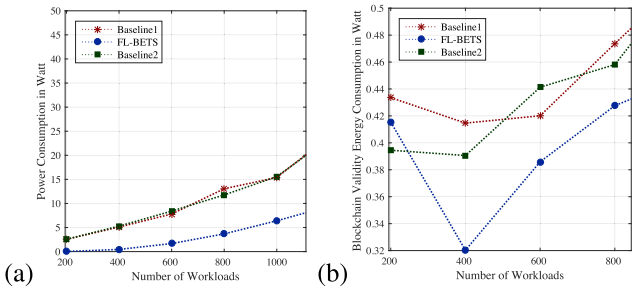

Fig. 5. Energy consumption of IoMT during fraud analysis and execution with different numbers of tasks.

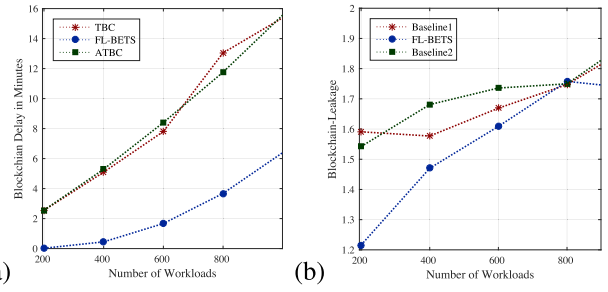

Fig. 6. Blockchain performances of IoMT applications with anomaly detection performances on different tasks.

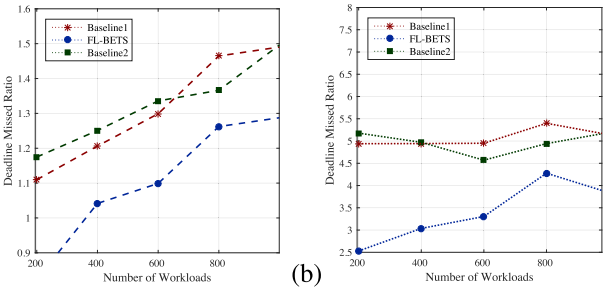

Fig. 7. Delay performance of IoMT applications with different numbers of tasks with anomaly detection.

E. Result Discussions and Performances of Proposed Schemes

The study conducted the experimental based on different components such as latency objective with the deadline, blockchain-enable accuracy and resource leakage performance of blocks, and energy efficiency of nodes during execution in the system. Fig. 4(a) shows the delay performances while using the proposed scheme FL-BETS as compared to baseline 1 and baseline 2 during the processing of IoT applications on the different computing nodes. The main reason is that all existing studies only focused on resource scalability instead of resource utilization while scheduling workloads on machines. Another perspective is that the FL-BETS trains the models at different fog nodes for each IoT workload, with a minimum training delay instead of a centralized training model. Therefore, federated learning-enabled distributed fog-cloud scheduling training optimally compared to a centralized machine learning training model in terms of delay. Fig. 4(b) the training delay performances of existing training machine learning algorithm (TMLA) for IoT applications with workload executions. In contrast, the Fully Training Machine Learning Algorithm (FTMLA) is widely used to train the offloaded data on single scalable nodes. However, these centralized nodes incur long train delays if the number of IoT applications increases in the system. Therefore, the FL-BETS distributed training model, e.g., federated learning model, gained optimal results compared to the existing training model in terms of delay in the system. Fig. 5(a) shows the power consumption due to fraud analysis and execution performances of the scheduling with the training model for IoMT applications in the system. Fig. 5(b) shows the power consumption during blockchain validation in nodes in both figures; the results show that the federated learning consumes less power for data training as compared to the existing centralized training model for IoMT applications. Fig. 6(a) and (b) shows the delay performance during blockchain verification and resource leakage in the distributed network. The existing traditional blockchain (TBC) algorithm and active traditional blockchain (ATBC) are widely exploited in the distributed fog-cloud network. However, they trained the fraud and security and proof of credibility, sake, and work cases on single centralized nodes in the peer-to-peer network. It will face a lot of delay for IoMT applications. Therefore, in this case, FL-BETS outperforms all existing schemes in terms of delay in the blockchain process in distributed fog-cloud for IoMT applications in the system. Besides energy consumption, delay, blockchain validation, privacy preservation and fraud-detection performance in the distributed fog-cloud nodes for IoMT, the deadline is also more critical in IoMT applications during scheduling in the system. Fig. 7(a) and (b) show the delay-performances of IoMT applications with the baseline approaches, e.g., baseline 1 and baseline and proposed scheme FL-BETS. At the same time, the delay of IoMT applications with the distributed federated enabled framework FL-BETS incurred lower end-to-end delay in the system as compared to existing schemes. The only reason is that, for each application, the FL-BETS train model at local nodes is shared to global nodes for further scheduling. This way, overall delay can be minimized for IoMT applications. Furthermore, Fig. 8(a) and (b) show the deadline performances of IoMT applications besides delay in the system. The results show that FL-BETS outperforms all existing schemes regarding missing deadlines and the satisfied deadline for IoMT applications in the system.

Authorized licensed use limited to: Deakin University. Downloaded on May 22,2024 at 07:34:40 UTC from IEEE Xplore. Restrictions apply.

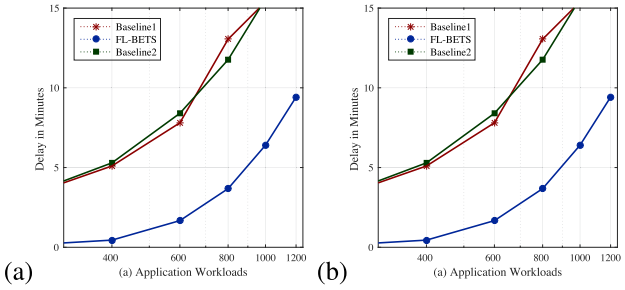

Fig. 8. Deadline performance of IoMT applications with different schemes in blockchain-enabled network.

F. Finding and Limitation

In the current proposed IoMT system, the study devised the federated learning-enabled distributed learning process in a blockchain-enabled IoMT system for different healthcare workloads. The objective is to minimize privacy and security issues with the minimum processing time and processing cost in IoMT work. The study devised the FL-BETS algorithm framework, which consisted of different methods and achieved the considered objective with optimal results. However, dynamic and run-time unknown attacks are more challenging for the IoMT and were not considered in this work. Our subsequent work will consider the adaptive malware-enabled federated learning method in the blockchain-aware IoMT system.

VI. Conclusion

As shown in the discussion section, the proposed (FL-BETS) framework minimized energy consumption by 41% and delay by 28%. The study introduced the mathematical model. In the performance evaluation, FL-BETS outperforms all existing machine learning and blockchain mechanisms in fraud analysis, data validation, energy and delay constraints for healthcare applications.

The study find the privacy and security issues with the minimum consumption of the resources in the proposed work as existing machine learning models did not achieve the effective utilization of resources in their model and incurred with the high energy, delay and cost in the system.

In future work, the study will focus on awareness of mobility fraud and anomaly detection for civil maritime applications in the blockchain-enabled fog-cloud network. The cost functions will be determined widely for the system's ubiquitous and distributed security constraints. Furthermore, the proposed system will consider the blockchain-enabled federated learning methods and the deep-learning decision model for both preemptive and non-preemptive aspects.

References

[1] P. Bhowal, S. Sen, J. H. Yoon, Z. W. Geem, and R. Sarkar, "Choquet integral and coalition game-based ensemble of deep learning models for COVID-19 screening from chest X-ray images," *IEEE J. Biomed. Health Informat.*, vol. 25, no. 12, pp. 4328–4339, Dec. 2021.

[2] Y. Zhou, B. Wang, X. He, S. Cui, and L. Shao, "DR-GAN: Conditional generative adversarial network for fine-grained lesion synthesis on diabetic retinopathy images," *IEEE J. Biomed. Health Informat.*, vol. 26, no. 1, pp. 56–66, Jan. 2022.

[3] Y. Qu *et al.*, "Decentralized privacy using blockchain-enabled federated learning in fog computing," *IEEE Internet Things J.*, vol. 7, no. 6, pp. 5171–5183, Jun. 2020.

[4] A. H. Sodhro *et al.*, "Towards ML-based energy-efficient mechanism for 6G enabled industrial network in box systems," *IEEE Trans. Ind. Informat.*, vol. 17, no. 10, pp. 7185–7192, Oct. 2021.

[5] R. Saha, S. Misra, and P. K. Deb, "FogFL: Fog assisted federated learning for resource-constrained IoT devices," *IEEE Internet Things J.*, vol. 8, no. 10, pp. 8456–8463, May 2021.

[6] Z. Lian, W. Wang, and C. Su, "COFEL: Communication-efficient and optimized federated learning with local differential privacy," in *Proc. IEEE Int. Conf. Commun.*, 2021, pp. 1–6.

[7] X. Wang, L. T. Yang, Y. Wang, L. Ren, and M. J. Deen, "ADTT: A highly efficient distributed tensor-train decomposition method for IIoT big data," *IEEE Trans. Ind. Informat.*, vol. 17, no. 3, pp. 1573–1582, Mar. 2021.

[8] S. Hosseinalipour, C. G. Brinton, V. Aggarwal, H. Dai, and M. Chiang, "From federated to fog learning: Distributed machine learning over heterogeneous wireless networks," *IEEE Commun. Mag.*, vol. 58, no. 12, pp. 41–47, Dec. 2020.

[9] H. Shao, M. Xia, G. Han, Y. Zhang, and J. Wan, "Intelligent fault diagnosis of rotor-bearing system under varying working conditions with modified transfer convolutional neural network and thermal images," *IEEE Trans. Ind. Informat.*, vol. 17, no. 5, pp. 3488–3496, May 2021.

[10] P. K. Sharma, J. H. Park, and K. Cho, "Blockchain and federated learning-based distributed computing defence framework for sustainable society," *Sustain. Cities Soc.*, vol. 59, 2020, Art. no. 102220.

[11] X. Lu, Y. Liao, P. Lio, and P. Hui, "Privacy-preserving asynchronous federated learning mechanism for edge network computing," *IEEE Access*, vol. 8, pp. 48 970–48 981, 2020.

[12] X. Zhao and C. Huang, "Microservice based computational offloading framework and cost efficient task scheduling algorithm in heterogeneous fog cloud network," *IEEE Access*, vol. 8, pp. 56 680–56 694, 2020.

[13] A. Lakhan and X. Li, "Transient fault aware application partitioning computational offloading algorithm in microservices based mobile cloudlet networks," *Computing*, vol. 102, no. 1, pp. 105–139, 2020.

[14] W. Dou, W. Tang, B. Liu, X. Xu, and Q. Ni, "Blockchain-based mobility-aware offloading mechanism for fog computing services," *Comput. Commun.*, vol. 164, pp. 261–273, 2020.

[15] A. Lakhan, M. Ahmad, M. Bilal, A. Jolfaei, and R. M. Mehmood, "Mobility aware blockchain enabled offloading and scheduling in vehicular fog cloud computing," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 7, pp. 4212–4223, Jul. 2021.

[16] P.-H. C. Chen, Y. Liu, and L. Peng, "How to develop machine learning models for healthcare," *Nature Mater.*, vol. 18, no. 5, pp. 410–414, 2019.

[17] Y. Zhang, Z. Zheng, H.-N. Dai, and D. Svetinovic, "Guest editorial: Special section on blockchain for industrial Internet of Things in IEEE Transactions on Industrial Informatics," *IEEE Trans. Ind. Informat.*, vol. 15, no. 6, pp. 3514–3515, Jun. 2019.

[18] S. Farshidi, S. Jansen, S. España, and J. Verkleij, "Decision support for blockchain platform selection: Three industry case studies," *IEEE Trans. Eng. Manage.*, vol. 67, no. 4, pp. 1109–1128, Nov. 2020.

[19] J. Lockl, V. Schlatt, A. Schweizer, N. Urbach, and N. Harth, "Toward trust in Internet of Things ecosystems: Design principles for blockchain-based IoT applications," *IEEE Trans. Eng. Manage.*, vol. 67, no. 4, pp. 1256–1270, Nov. 2020.

[20] G. Fortino, F. Messina, D. Rosaci, and G. M. Sarné, "Using blockchain in a reputation-based model for grouping agents in the Internet of Things," *IEEE Trans. Eng. Manage.*, vol. 67, no. 4, pp. 1231–1243, Nov. 2020.

[21] Y. Lu, X. Huang, Y. Dai, S. Maharjan, and Y. Zhang, "Blockchain and federated learning for privacy-preserved data sharing in industrial IoT," *IEEE Trans. Ind. Informat.*, vol. 16, no. 6, pp. 4177–4186, Jun. 2020.

[22] S. R. Pokhrel and J. Choi, "Federated learning with blockchain for autonomous vehicles: Analysis and design challenges," *IEEE Trans. Commun.*, vol. 68, no. 8, pp. 4734–4746, Aug. 2020.

[23] U. Majeed and C. S. Hong, "FLchain: Federated learning via MEC-enabled blockchain network," in *Proc. IEEE 20th Asia-Pacific Netw. Operations Manage. Symp. (APNOMS)*, 2019, pp. 1–4.

[24] D. C. Nguyen *et al.*, "Federated learning meets blockchain in edge computing: Opportunities and challenges," *IEEE Internet Things J.*, vol. 8, no. 16, pp. 12806–12825, Aug. 2021.

[25] Y. Lu, X. Huang, K. Zhang, S. Maharjan, and Y. Zhang, "Blockchain empowered asynchronous federated learning for secure data sharing in internet of vehicles," *IEEE Trans. Veh. Technol.*, vol. 69, no. 4, pp. 4298–4311, Apr. 2020.

Authorized licensed use limited to: Deakin University. Downloaded on May 22,2024 at 07:34:40 UTC from IEEE Xplore. Restrictions apply.