Blockchain-Enabled Contextual Online Learning Under Local Differential Privacy for Coronary Heart Disease Diagnosis in Mobile Edge Computing

Xin Liu, *Student Member, IEEE*, Pan Zhou, *Member, IEEE*, Tie Qiu, *Senior Member, IEEE*, and Dapeng Oliver Wu, *Fellow, IEEE*

***Abstract*—Due to the increasing medical data for coronary heart disease (CHD) diagnosis, how to assist doctors to make proper clinical diagnosis has attracted considerable attention. However, it faces many challenges, including personalized diagnosis, high dimensional datasets, clinical privacy concerns and insufficient computing resources. To handle these issues, we propose a novel blockchain-enabled contextual online learning model under local differential privacy for CHD diagnosis in mobile edge computing. Various edge nodes in the network can collaborate with each other to achieve information sharing, which guarantees that CHD diagnosis is suitable and reliable. To support the dynamically increasing dataset, we adopt a top-down tree structure to contain medical records which is partitioned adaptively. Furthermore, we consider patients' contexts (e.g., lifestyle, medical history records, and physical features) to provide more accurate diagnosis. Besides, to protect the privacy of patients and medical transactions without any trusted third party, we utilize the local differential privacy with randomised response mechanism and ensure blockchain-enabled information-sharing authentication under multi-party computation. Based on the theoretical analysis, we confirm that we provide real-time and precious CHD diagnosis for patients with sublinear regret, and achieve efficient privacy protection. The experimental results validate that our algorithm outperforms other algorithm benchmarks on running time, error rate and diagnosis accuracy.**

***Index Terms*—Blockchain, big data, Coronary heart disease diagnosis (CHD), contextual online learning, edge computing, local differential privacy.**

Manuscript received October 1, 2019; revised April 6, 2020 and May 26, 2020; accepted May 29, 2020. Date of publication June 2, 2020; date of current version August 5, 2020. This work is supported by Natural Science Foundation of China (NSFC) under Grant 61972448. *(Corresponding author: Pan Zhou.)*

Xin Liu and Pan Zhou are with the Hubei Engineering Research Center on Big Data Security, School of Cyber Science and Engineering, Huazhong University of Science and Technology, Wuhan 430074, China (e-mail: Liuxin_hust@hust.edu.cn; panzhou@hust.edu.cn).

Tie Qiu is with the College of Intelligence and Computing, Tianjin University, Tianjin 300350, China (e-mail: qiutie@ieee.org).

Dapeng Oliver Wu is with the Department of Electrical and Computer Engineering, University of Florida, Gainesville, FL 32611-6130 USA (e-mail: dpwu@ieee.org).

Digital Object Identifier 10.1109/JBHI.2020.2999497

I. Introduction

A. Motivation

THE most common type of heart diseases currently in the United States is coronary heart disease (CHD), which sometimes can cause heart attacks. As the survey shows [1], there are more than 3 70 000 deaths every year because of CHD, and it makes up 15.6% of all deaths globally [2]. And recent data indicates that by 2030, about 25 million people will die owing to the related heart diseases. CHD usually develops when cholesterol builds up on the artery walls that produces plaques. And these plaques make the coronary arteries too narrow to supply enough oxygen rich blood for the heart, which impacts the normal physical activities. There are many symptoms caused by CHD, such as indigestion, heartburn, weakness, nausea, and shortness of breath, etc.

With the CHD event happening frequently, the CHD prognosis has been an attractive field for clinical decision support systems. A number of tests may help with diagnosis and prognosis including: electrocardiogram, cardiac stress testing, coronary computed tomographic angiography, and coronary angiogram, among others [3]. However, in this big data era with universal health appealing and information sharing, there are some important issues about heart disease diagnosis that we should address as follows:

1) *Personalized diagnosis support:* Most diagnostic techniques keep low diagnosis accuracy with limited medical dataset. And different patients have different conditions and contextual information, which means the demand of personalized diagnosis. Utilizing the context from patients and incorporating them to reduce the uncertainty inherent for CHD diagnosis are important.
2) *High dimensional datasets:* The massive amounts of patients' electric health records are stored locally including symptom characteristics, historical diagnosis records, and personal information statistics, etc. Moreover, the missing value problem is also common in many clinical cases. How to manage the big data analysis and choose the reasonable features of patients to make accurate diagnosis is challenging.

3) *Clinical privacy concerns:* Due to the sensitivity of clinical data in the process of online learning, it is vital to ensure the privacy of patients and diagnosis records. Some malicious attackers or untrustworthy hospitals will put these sensitive information at a risk for financial incomes.
4) *Insufficient computing resources:* The traditional centralized computing structure cannot meet with the computation of massive clinical records and real-time response to patients in need. It is feasible to apply some advanced technologies with high computation capabilities to handle data processing and provide instant CHD diagnosis.

To solve the abovementioned problems, we propose a novel blockchain-enabled contextual online learning model under local differential privacy for CHD diagnosis in mobile edge computing. First, compared to the traditional classifiers [4]–[6] that only consider direct patients' symptoms to make diagnosis, our proposal is context-aware to utilize the comprehensive contextual information (e.g., lifestyle, medical history records, physical features, family history, etc) from patients similar to the approach of assessing the relevancy of contextual features in [7]. Thus, we can formulate our algorithm into solving a contextual multi-armed bandit (CMAB) problem [8] which is usually applied in recommendation scenarios and provide highly personalized diagnostic suggestions for different patients. Moreover, to handle big data analysis of massive patients' information in the clinical system, we use a top-down tree-based structure to support increasing dataflow for efficiently online learning. This tree structure is composed of infinite nodes that store the diagnosis records, and it can be adaptively partitioned and expanded by adding more new sub-nodes with updated diagnosis records arriving, which supports increasing datasets.

Next, to deal with the shortcomings of traditional centralized cloud computing and promote the feedback speed of CHD diagnosis, mobile edge computing (MEC) [9] is adopted and considered in our proposal to promote the computation capabilities. For example, in [10], the edge nodes cooperate with the terminals to analyze different big data in IoT for providing more help in diagnosing diseases. This technology reduces the latency through the medical network, increases the diagnostic stability, enlarges the storage capabilities and accelerates the online learning process. These nodes in the MEC network can share medical information with neighboring nodes while satisfying some specific conditions.

Finally, owing to the sensitivity of patients' context and diagnosis results, we utilize local differential privacy (LDP) [11] to guarantee patients' privacy and use blockchain technology [12] to achieve reliable information sharing and medical transactions simultaneously. As a privacy mechanism, LDP is at the user level locally without a trusted third party compared to global differential privacy [13]. In traditional global differential privacy, the noise is only added during the data processing to ensure the privacy of output. However, the noise under LDP is added to the input in the system model, so the privacy protection is guaranteed in the total process besides the outcome. As a result, LDP is used here to perturb the input medical records efficiently with randomized response mechanism [15] which can achieve random perturbation, disturb malicious attacks and ensure the patients' personal information safe. Blockchain is one kind of the security management tools, and we use it as an authentication mechanism to decide whether the nodes should cooperate with their one-step neighboring nodes. And it can ensure the security of the diagnostic process and record each medical transaction with multi-party computation (MPC), which provides a reliable secret sharing scheme [12].

Our main contributions are summarized as follows:

1) We propose a novel context-aware online learning algorithm for CHD diagnosis, which considers the heterogeneity of patients to guarantee the real-time personalized diagnosis for patients.
2) Our approach is based on an adaptively expanding tree structure to support increasing datasets of medical diagnosis records (MDR), which also ensures the accurate diagnosis recommendation results.
3) We adopt the local differential privacy method to prevent the privacy of patients from being attacked and utilize the blockchain-enabled model to guarantee the security of diagnosis records sharing and medical transactions.
4) Our proposal is in edge computing to reduce time consumption and space cost, which can process massive data from patients and accelerate the online learning process for CHD diagnosis simultaneously.

The reminder of this article is organized as follows. In Section II, we discuss the works related to our proposal. In Section III, we describe our system model in details. in Section IV, we propose our novel algorithm and analyze the performances. In Section V, we show our simulation and experimental results. In Section VI, we conclude this article.

II. Related Work

The major goal of our algorithm is to make accurate CHD diagnosis recommendation for different patients. A great number of efficient approaches have been devised to make accurate CHD prognosis and diagnosis. Tao *et al.* [4] apply support vector machines (SVM) to classify for patients with CHD or not. And in [5], the novel method utilizing the fitness function and a genetic function is presented to predict atherosclerosis, which depends on the receiver operator characteristics. Some applicable machine learning algorithms are also used for CHD prognosis to analyze the risk of heart diseases in [6], which mainly consider the image analysis and ultrasound detection. The authors in [14] apply the dynamic bayesian networks with temporal abstraction to represent the realistic probabilistic relationship between various risk factors and process the abstract data from patients to improve performances. The ultrasound image data is collected to make computer-aided diagnosis for predicting the risks of CHD caused by atherosclerosis in [6]. A novel binary particle swarm optimization algorithm in [16] is presented to detect heart disease, which improves the overall accuracy. But they all ignore patients' personal information and cannot guarantee the privacy of personal information.

Additionally, our proposal is derived from contextual multi-armed bandit (CMAB) framework [17], which takes patients' contextual information as the extracted context vector to

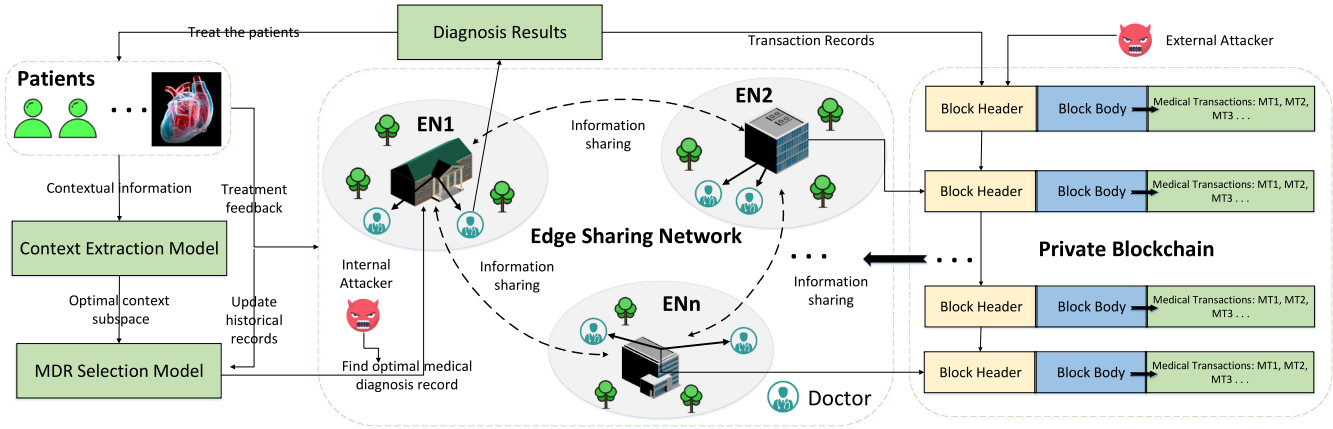


Fig. 1. Workflow of blockchain-enabled contextual online learning system in edge computing for CHD diagnosis.

provide personalized CHD diagnosis. However, static tree partition method is not appropriate in this case to support big data analysis. Thus, the bottom-up tree method [18] is proposed, while the number of arms must be told in advance. Our algorithm is based on the top-down tree structure, which expands in the patient level instead of only considering the single patient to adapt the increasing dataset.

Local differential privacy (LDP), as a novel technology in the local setting, is deployed in many conditions without a trusted third party. Take the Google applied randomized aggregatable privacy-preserving ordinal response (RAPPOR) [19], [20], it can ensure the high utility, efficient collection and privacy guarantees of real-world users' data. LDP can make the output from two identical individuals almost indistinguishable to a certain degree. Randomised response [23], as a method to eliminate bias, is usually combined with LDP to perturb the input dataset for protecting privacy. For example, in [21], the authors present optimized local hashing and unary encoding protocols to promote the utility of users' information based on randomised response. And we also apply randomised response in our algorithm to protect patients' privacy.

As for the privacy of diagnosis records, we utilize the blockchain, the decentralized data management framework [12], to ensure the security of online transactions authenticated by the cooperation of edge nodes. Actually, a blockchain consists of a list of records called blocks which are connected with previous blocks like a distributed ledger. Due to the computation of massive data, multi-party computation (MPC) [22] is the suitable distributed cryptographic solution for blockchains to jointly compute the authentication function without disclosing the privacy of inputs. Blockchain currently has been applied in many scenarios, such as Bitcoin [24], Ethereum [25], and Hyperledger Fabric [26], etc. Moreover, our proposed model relies on MEC, which guarantees the adding of new medical diagnosis records (MDRs) and reduces substantial computing resources for resource-limited terminal equipments. Xiong *et al.* [28] propose a novel framework of mobile edge computing with blockchain to manage the resources economically. And in [29], blockchain-inspired data contribution in EVCE computing is applied to solve the problems with energy allocation and

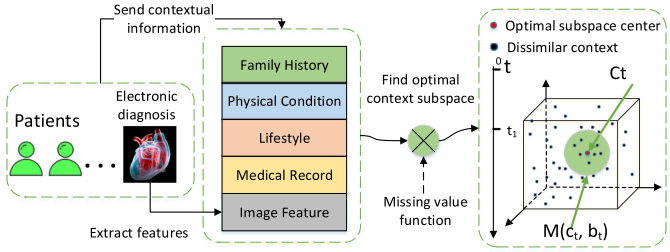


Fig. 2. Context extraction model.

security challenges. However, compared to above approaches, our algorithm can also provide personalized recommendations and support big data analysis.

III. System Model

As shown in Fig. 1, our proposed novel blockchain-enabled contextual online learning model under local differential privacy for CHD diagnosis in mobile edge computing is composed of four parts: context extraction model, MDR selection model with LDP, edge sharing network, and private blockchain. And the detailed descriptions are as follows.

A. Context Extraction Model

Each patient p with coronary heart disease, arrives with the corresponding contextual information as shown in Fig. 2, which is defined as a context vector $c \in \mathcal{C}$, where $\mathcal{C}$ is the patient context space containing all the patients' context. However, many missing values are existing in the clinical system, which affect the normal computation between different context vectors. Thus, we utilize maximum likelihood estimation as a missing value function to achieve value interpolation. We assume that each c in $\mathcal{C}$ is normalized to [0,1] and the space $\mathcal{C}$ is d_c-dimensional. Each dimension represents one feature related to one certain context (e.g., age, blood pressure, density of lipoprotein, whether smoke or not, smoking habit, family history, level of fibrinogen, previous medical records, electronic image diagnosis, etc). For instance, if $d_c = 4$, and a context vector $c = [0.3, 0.6, 0, 0.5]$

arrives in the space, where $c_1 = 0.3$ means the patient is about 36 years old if the maximum is 120 with a high level of blood pressure ($c_2 = 0.6$), who dislikes smoking ($c_3 = 0$) and has a family in which five persons have the coronary heart disease ($c_4 = 0.5$) with a maximum of ten persons.

To select the optimal context subspace for recommending more suitable MDRs, we equip each space $\mathcal{C}$ with a dissimilarity function $\mathcal{F}_{\mathcal{C}}$. And $\forall c, \vec{c} \in \mathcal{C}$, we have $\mathcal{F}_{\mathcal{C}}(c, \vec{c}) \geq 0$ and $\mathcal{F}_{\mathcal{C}}(c, c) = 0$. To evaluate the similarity between different contexts, we introduce the $\mathcal{F}_{\mathcal{C}}$-ball indexed by the function $M(c_t, b_t)$ to measure the distance between them, where c_t is the center and b_t means the radius. The maximum dissimilarity distance between two context vectors is $\mathcal{D}(c_1, c_2) = \sup_{c_1, c_2 \in \mathcal{C}} \mathcal{F}_{\mathcal{C}}(c_1, c_2)$. We build the context ball space with the radius $b_t^C = (\frac{\ln t}{t^2})^{\beta}$, where the value of β can control the context exploration speed. We can see the radius of ball decreases with time increasing, and eventually we can find the optimal context space to retrieve suitable MDR.

B. MDR Selection Model With LDP

The MDR selection tree, built with various patients' historical medical records and condition feedbacks, is defined as $T^{\mathcal{R}}$, where $\mathcal{R}$ represents the corresponding space containing diagnosis records. As a tree-based structure, this model is composed of many MDR nodes, which cache different diagnosis records r (e.g., blood testing results, pressure analysis, heart rate, heart CT scans, etc). We denote the m-th node at depth $h \geq 0$ as (h, m), and m is constrained by $1 \leq m \leq 2^h$. Hence, each parent node (h, m) can be represented by two child nodes $(h+1, 2m-1)$ and $(h+1, 2m+1)$. Furthermore, each subspace $\mathcal{R}_{h,m}$ containing the selected node (h, m) should satisfy some constraints: $\forall h \geq 0, 1 \leq m, \vec{m} \geq 2^h, \mathcal{R}_{0,1} = \mathcal{R}, \mathcal{R}_{h,m} \cap \mathcal{R}_{h,\vec{m}} = \oslash, \mathcal{R}_{h,m} = \mathcal{R}_{h+1,2m-1} \cap \mathcal{R}_{h+1,2m+1}$. Due to the limited size of nodes, we should bound the maximum and minimum size, and then partition them adaptively as the arrival medical information increases. Thus, we utilize the following assumption to support our analysis:

Assumption 1 (MDR selection tree structure): $\exists \beta_1, \beta_2 > 0$, $0 < \alpha < 1$, and we define the maximum distance in $\mathcal{R}$ among any nodes $(h, m) \in T^{\mathcal{R}}$ as $\mathcal{D}(\mathcal{R}_{h,m})$, then we have: $\beta_1 \alpha^h \leq \mathcal{D}(\mathcal{R}_{h,m}) \leq \beta_2 \alpha^h$.

According to this assumption, we bound the nodes' size and can divide it into more precious sub-nodes for providing more accurate diagnosis results with the increase of system working rounds. However, once the optimal node including the most appropriate medical records is selected, the internal curious attackers will use some program analytic skills to disguise as doctors in the clinical hospital to acquire the personal diagnosis results. Therefore, we use the LDP here to guarantee patients' privacy. We introduce the randomised response mechanism $\mathcal{M}$ to achieve ε-local differential privacy by perturbing the MDR r and ε is non-negative, and then we have to satisfy:

$$\sup_{q \in \mathcal{Q}, r, \vec{r} \in \mathcal{R}} \frac{\mathcal{M}(q|r)}{\mathcal{M}(q|\vec{r})} \leq \exp^{\varepsilon}, \tag{1}$$

where $\mathcal{Q}$ is a n-dimensional output after randomised perturbation, and q belongs to it. Let $\mathcal{Q} = \{q_1, q_2, \ldots, q_n\}$ and $\mathcal{R} = \{r_1, r_2, \ldots, r_n\}$. We define a multi-dimensional design matrix [15] $\mathbb{P} = \{p_{qr}\}$ to achieve the data perturbation, and the sum of each column is 1:

$$\begin{pmatrix} p_{q_1 r_1} & p_{q_1 r_2} & \cdots & p_{q_1 r_n} \\ p_{q_2 r_1} & p_{q_2 r_2} & \cdots & p_{q_2 r_n} \\ \vdots & \vdots & \vdots & \vdots \\ p_{q_n r_1} & p_{q_n r_2} & \cdots & p_{q_n r_n} \end{pmatrix}, \tag{2}$$

where $p_{q,r}$ means the probability that the perturbed output is q while the original record is r. Moreover, to evaluate the utility of the perturbed records while ensuring the local differential privacy, we use a reconstruction probability event $\vec{\mathbb{P}}(r_i = r \to \vec{r}_i = r) = \sum_{q_i \in \mathcal{Q}} \mathbb{P}(q_i = q | r_i = r) \mathbb{P}(\vec{r}_i = r | q_i = q)$, which means the probability that we correctly reconstruct the individual's records r from the perturbed data. When the reconstruction probability is maximum and this model satisfies the condition $p_{qr}/p_{q\vec{r}} \leq \exp^{\varepsilon}$, where the original records $r \in \mathcal{R}$, and the perturbed records $\vec{r} = \mathcal{R}/r$, and thus we can achieve the optimal utility and guarantee the patients' privacy.

C. Edge Sharing Network

There are $|W|$ edge nodes (ENs) in the edge sharing network, which are indexed by the set $W = \{1, 2, \ldots, |W|\}$. We introduce a graph $N(W, E)$ to model the connected ENs in the clinical network, where E represents the set of edges. And the structure of the network is featured by an adjacent matrix $e(x, y), x, y \in W$. We set $e(x, y) = 1$ if node x is y's one-step neighbor, otherwise $e(x, y) = 0$. As shown in Fig. 1, we observe that $e(1, 2) = 1, e(1, n) = 1, e(2, n) = 0$. Due to the sufficient computing capabilities of ENs, they can store massive patients' medical diagnosis records. Besides, as the components in the sharing network, the ENs can share medical information with each other to achieve cooperative CHD diagnosis. The diagnosis record of the patient p is sent instantly to the most experienced doctor with low latency bypassing the edge sharing network for further diagnosis. According to the realistic conditions and historical medical records, the doctor will provide a final diagnosis result to treat the patient efficiently. However, to guarantee the security of medical transactions and reliable information sharing, we utilize the modified blockchain to set a sharing correctness threshold Θ calculated by our proposed authentication algorithm, to determine whether the current EN is trustworthy.

D. Private Blockchain Model

The private blockchain is composed of chained blocks, which stores some references to the medical transactions as a decentralized hash sub-table in the block body, and block head which contains different parameters (e.g., timestamp, nonce, Merkle root, version number, difficulty value, etc) control the dataflow, ensure the block immutable and achieve most basic functions. In this model, secure multi-party computation (MPC) makes sure that the data is split to be computed discretely and thus every party cannot infer any meaningful medical information from

the unreliable adjacent ENs. To protect the patients' medical diagnosis transactions, we generalize the multi-party secure CHD diagnosis recommendation problem into MPC, and then introduce the linear secret-sharing scheme [12] to achieve the linear combination of different secret records. We denote N_u as the number of parties, and utilize a random N_m degree polynomial $\Upsilon(n)$ to share the personal records r as

$$\Upsilon(n) = k_0 + k_1 n + k_2 n^2 + \cdots + k_{N_m} n^{N_m}, \quad k_0 = r, \tag{3}$$

where $k_i \sim B(N_u, p), i \in \{1, \ldots, N_u\}$, and $N_m + 1$ represents the minimum number of parties required to reconstruct the medical records r. Besides, we define $[r]_{p_i} = \Upsilon(i)$ as the shared records, and then given any $N_m + 1$ shares, we can reconstruct the original record r by using $r = \Upsilon(0)$. Therefore, based on the cryptosystem, we can defend the attacks of passive external adversaries, protect the privacy of personal medical records and achieve reliable information sharing.

To guarantee the correctness of information sharing and decide which EN is suitable to cooperate with, we devise a protocol using somewhat homomorphic encryption (SHE) based on MPC [27] to generate sharing randomness and evaluate the level of correctness. The sharing protocol represents each shared record by its MAC address and additive share, which is modified as

$$\langle r \rangle_{p_i} = ([\theta(r)]_{p_i}, [r]_{p_i}), \quad \text{s.t.} \quad \theta(r) = \rho r, \tag{4}$$

where ρ means the immutable MAC key, and $\langle r \rangle$ represents the sharing scheme which can support superposition homomorphism of different medical records. Using this modified scheme, we can calculate the sharing correctness Θ between different records stored in different ENs and achieve efficient cooperative medical diagnosis.

E. Workflow of System Model

We let n represent the round in our time-slotted system model. Initially, 1) the CHD patient p arrives with contextual information at timestamp t_n, 2) the context extraction model extracts the patient's context and electronic diagnosis image features into the context space $\mathcal{C}$ through missing value function. Furthermore, the space can be partitioned into a smaller ball $M(c_t, b_t)$ to select the most relevant contextual information. 3) While finding the optimal context subspace, it will be sent to the MDR selection model to retrieve the tree structure by adaptively online learning and further partition to select the most suitable MDRs r in the chosen cluster. 4) The optimal record r faces with the attacks from internal passive adversaries, we utilize the LDP mechanism to guarantee patient's privacy. Next, the record r is stored in the adjacent ENs, which can be conveyed to the most experienced doctors. 5) In the edge sharing network, different ENs can cooperate with each other to achieve information sharing according to the calculated threshold Θ from the private blockchain to judge whether the one-step neighboring node is reliable. 6) The related medical record r is sent to the corresponding doctor and he/she makes the final diagnosis decisions. To prevent the transactions being exposed, this medical transaction is recorded in the block header by the blockchain to ensure the safety of transactions between doctors and patients. 7) Next, the patient p will receive the diagnosis results and obtain the most reasonable treatment. 8) Finally, the patient p sends current treatment feedback to MDR selection model to update the medical records in the tree and the related feedback is also stored in the edge sharing network for next diagnosis.

F. CHD Diagnosis Recommendation Problem

To evaluate the performance of CHD diagnosis, we introduce the *regret* and *error rate (ER)*. The regret is from the gap between the optimal diagnosis feedback and realistic feedback, and then ER is composed of the number of false negative (FN) examples which means the benign outcome is diagnosed as negative and false positive (FP) examples which means the malicious outcome is diagnosed as positive. Furthermore, the feedback $f_{r,p}$ of patient p with the medical records r is constrained by [0,1], which is calculated by both explicit and implicit feedbacks. Explicit feedback represents the treatment effects and subjective description of patient p. And the implicit feedback is gained from the doctors' diagnosis results and optimal medical diagnosis records by online learning. We define the expected feedback of patient p as $\mu_{r,p} = \mathbb{E}[f_{r,p}]$ based on the MDR r. The optimal medical record is selected randomly from the most suitable node (h^*, m^*) which is the m-th node at depth h in the MDR selection tree, and actually varies over time. Therefore, we denote $r_n^* = \arg\max_r \mu_{r,p}(n)$ as the record with the optimal expected feedback. Additionally, similar MDRs are usually recommended to the patients who have similar disease conditions, so we need an assumption to consider this case:

Assumption 2 (Lipschitz conditions): For $\forall (h, m), (\vec{h}, \vec{m}) \in T^{\mathcal{R}}$, $\exists L > 0$, we assume that the MDR r in node (h, m) is recommended to the patient p, and the MDR $\vec{r}$ in node $(\vec{h}, \vec{m})$ is recommended to the patient $\vec{p}$. Then we have: $|\mu_{r,p} - \mu_{r,\vec{p}}| \leq L||r, \vec{r}||, |\mu_{r,p} - \mu_{\vec{r},p}| \leq \max\{\mathcal{D}(\mathcal{R}_{h,m}), |\mu_{r,p}^* - \mu_{\vec{r},p}|\}$.

The Lipschitz constant L is useful in the regret analysis process. The regret between optimal feedback and empirical feedback is defined as $\triangle(t_n) = \mu_{r,p}^* - f_{r,p}$. As a result, the n-steps cumulative expected regret can be defined as:

$$\begin{aligned} \mathbb{E}[CR(t)] &= \mathbb{E} \sum_{r \in T^{\mathcal{R}}} \sum_{j=1}^{n} [\triangle(t_j)] \\ &= \mathbb{E} \sum_{r \in T^{\mathcal{R}}} \sum_{j=1}^{n} [\mu_{r,p}^*(t_j) - f_{r,p}(t_j)], \end{aligned}$$

where $\mu_{r,p}^*(t_j)$ is the optimal expected feedback at time t_j from patient p according to medical records r. Our goal is to minimize the error rate and guarantee that the regret is sublinear which ensures the regret can converge to a small level. Therefore, the CHD diagnosis recommendation problem can be formulated as:

$$\begin{aligned} &\text{minimize} \quad \mathrm{ER} = \mathrm{FP} + \mathrm{RP}, \\ &\text{subject to} \quad \mathbb{E}[\mathrm{CR(t)}] \quad \text{is sublinear}, \end{aligned} \tag{5}$$

where ER depends on the number of both false positive examples and false negative examples.

Algorithm 1: LCOL.

Input: $d_c > 0$, $f_{r,p} \in (0,1)$, $L, \beta_1, \beta_2, \alpha > 0$, content space $(\mathcal{R}_{h,m})_{h\geq 0, 1\leq m\leq 2^h}$.
Initialize: $n = 1, W_{\mathcal{C}} = 0, t_n = 0, T^{\mathcal{R}} = \{(0,1),(1,1),(1,2)\}, \mathcal{G}_{0,1}(t) = \mathcal{G}_{1,1}(t) = infinity$.
Auxiliary Function: MSP, SCB.
loop
  The patient p arrives with the context c at time t_n in the system model, then extract contextual information and electronic diagnosis features into context space $\mathcal{C}$ bypassing a missing value function.
  Find the optimal context subspace $M(c_t, b_t)$, and then send it to the MDR selection model.
  $P_n \leftarrow \mathtt{MSP}(T^{\mathcal{R}}, M(c_t, b_t))$.
  Select the optimal medical diagnosis record (MDR) r according to the path P_n.
  Design a randomised response matrix $\mathbb{P} = \{p_{qr}\}$, and then maximize the reconstruction probability event $\vec{\mathbb{P}}(r_i = r \to \vec{r}_i = r) = \sum_{q_i \in \mathcal{Q}} \mathbb{P}(q_i = q | r_i = r)\mathbb{P}(\vec{r}_i = r | q_i = q)$ and guarantee $p_{qr}/p_{q\vec{r}} \leq \exp^{\varepsilon}$. Furthermore, the perturbed record r is stored in EN a and the doctor rely on the record to make the final diagnosis decision.
  $\vec{r} \leftarrow \mathtt{SCB}(a, r, N_u, N_m, \rho)$.
  Recommend the final medical diagnosis records $\vec{r}$ to the patient p. After the treatment, the patient's feedback $f_{r,p}$ is sent to update the MDR selection tree and utilized to calculate the regret to evaluate the total diagnostic performance.
  Update $f_{r,p}, \mu_{r,p}, \mathcal{G}_{h,m}$.
  Go to time slot $t_n = t_n + 1$.
  $W_{\mathcal{C}} \leftarrow W_{\mathcal{C}} + 1$.
  if $W_{\mathcal{C}} \geq \tau_t = (\frac{\ln t_n}{t_n^2})^{\beta}$ **then**
    Partition the subspace $\mathcal{C}$, and then store the current subspace $M(c_t, b_t)$.
  end if
  if $(h_t, m_t) \in leaf(T^{\mathcal{R}})$ AND $\mathcal{E}_{h_t,m_t}(t) \geq \frac{2\ln t}{(\beta_2 \alpha^{h_t})^2}$ **then**
    Divide (h_t, m_t) into $(h_t + 1, 2m_t - 1)$, $(h_t + 1, 2m_t)$, and set each $\mathcal{G}$ value of them is infinity.
  end if
end loop

IV. Proposed Algorithm

In this section, we describe our proposed novel blockchain-enabled contextual online learning algorithm under local differential privacy for CHD diagnosis in mobile edge computing. It utilizes the massive medical records which are cached in ENs to support accurate diagnosis recommendation, and we can make big data analysis based on the MDR selection tree structure.

A. Algorithm Descriptions

First, we define the number of times that node (h, m) is selected till round n as $\mathcal{E}_{h,m}(t) = \sum_{t=1}^{n} \mathbb{I}\{h_t = h, m_t = m, c_t \in \mathcal{C}\}$, where $\mathbb{I}$ is the indiction function. Therefore, the empirical feedback from (h, m) is defined as:

$$\vec{\mu}_{r,p}^{h,m}(t) = \frac{1}{\mathcal{E}_{h,m}(t)} \sum_{t=1}^{n} f_{r,p}(t)\mathbb{I}\{h_t = h, m_t = m, r \in (h_t, m_t)\}, \tag{6}$$

which represents the average value of realistic feedbacks. However, if we select the node (h^*, m^*) with the highest retrieval

Algorithm 2: The MSP Function.

Input: Tree $T^{\mathcal{R}}$, $M(c_t, b_t)$.
Initialize: $(h, m) \leftarrow (0,1)$, $P_n \leftarrow (0,1)$, $\tau_0(t) = 1$.
while $\mathcal{E}_{h,m}(t) \geq \tau_h(t) = \frac{2\ln t}{(\beta_2 \alpha^h)^2}$, (h, m) contains history records with context from $M(c_t, b_t)$ AND $(h, m) \notin leaf(T^{\mathcal{R}})$ **do**
  Append P_n with node (h, m).
  if $\mathcal{G}_{h+1,2m-1} \leq \mathcal{G}_{h+1,2\,m}$ **then**
    Add $(h + 1, 2\,m)$ as (h, m)'s child.
  else
    Add $(h + 1, 2m - 1)$ as (h, m)'s child.
  end if
end while
Output: P_n.

feedback $\vec{\mu}_{r,p}^{h,m}(t)$, we might repeatedly select some nodes but ignore to exploit other potential nodes in the tree, and thus we introduce the parameter $\mathcal{G}$ to achieve the trade-off between exploitation and exploration. Actually, $\mathcal{G}$-value denotes the upper bound of the estimated feedback and it is calculated at level (h, m) as follows:

$$\mathcal{G}_{h,m}(t) = \begin{cases} \vec{\mu}_{r,p}^{h,m}(t) + \beta_2 \alpha^h + \sqrt{\frac{2\ln t}{\mathcal{E}_{h,m}(t)}} + \lambda_t L & \mathcal{E}_{h,m}(t) > 0, \\ \text{infinity}, & \text{otherwise}, \end{cases}$$

where λ_t means the maximum value of the radius in the context space $\mathcal{C}$. The first term here is estimated based on the historical records. The second term represents the maximum size of node containing medical diagnosis records. The third term means the fluctuation of estimate $\mu_{r,p}(t)$ while using $\vec{\mu}_{r,p}^{h,m}(t)$. And the last term is derived from the uncertainty of context space's size. We observe that the upper confidence of $\mathcal{G}_{h,m}(t)$ decreases with the round increasing, which means that once we select one optimal node for many times, its $\mathcal{G}$-value will decrease and then give more chances to exploit other suboptimal nodes. In short, our proposed algorithm includes three stages: 1) Find optimal MDRs. 2) Information sharing and privacy protection. 3) Historical records update and store.

1) *Find Optimal MDRs:* Initially, the patient p arrives, and then the contextual information and electronic image features are extracted as context vectors into context space to find the optimal subspace $M(c_t, b_t)$ as mentioned before. The subspace is utilized to retrieve the MDR selection tree and find the suitable path to select the most accurate record r. Once the number of node (h, m)'s selected times $\mathcal{E}_{h,m}(t)$ exceeds the threshold $\frac{2\ln t}{(\beta_2 \alpha^h)^2}$ and there are some existing records with context from $M(c_t, b_t)$, which means the node is reliable, and then we can add the current node into the path till the leaf node is selected. Retrieving on the path, we can select the optimal MDR node (h^*, m^*) at the end, and choose an appropriate record r randomly inside it. As shown in Fig. 3, the optimal path chooses the node (4,7), but the current path selects the node (5,13) as the appropriate node instead of finding the realistic optimal node. Moreover, the partition of different MDR nodes is corresponding to the division of MDR space $\mathcal{R}$. To guarantee the privacy of the records, we design a randomised response matrix $\mathbb{P}$, and thus the

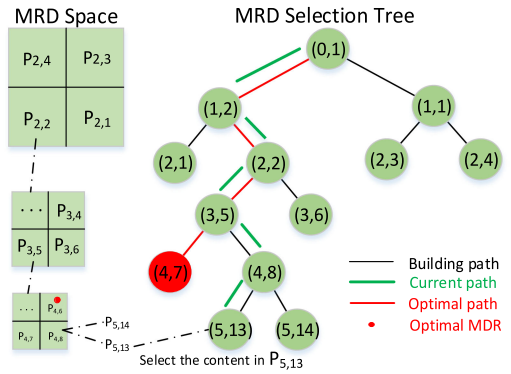


Fig. 3. Medical diagnosis record (MDR) selection tree model.

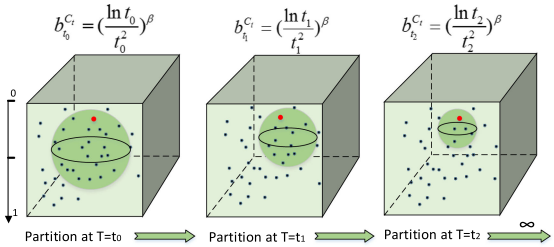


Fig. 4. Context space partition process.

output can be randomly perturbed and satisfy the LDP-condition to prevent the attacks from the internal curious ENs.

2) *Information Sharing and Privacy Protection:* To achieve medical information sharing, we introduce the linear secret-sharing scheme $\Upsilon(n)$ to share different medical records through blockchain. However, some nodes are malicious nd untrustworthy, and thus we use the private blockchains to calculate the correctness to judge whether the one-step EN is reliable. First, we use the function $\theta(r)$ to construct the address of different records in EN x except the selected node a in the edge sharing network. Then, the sharing protocol $\langle r\rangle_{p_i} = ([\theta(r)]_{p_i}, [r]_{p_i})$ can measure the relation value between its MAC and additive shares. Finally, if the value exceeds 0, it means the current record in EN x is reliable and the correctness value Θ will increase. Once the correctness Θ_x in EN x exceeds Θ_a in EN a, it must be worthwhile of cooperating with EN x to achieve medical information sharing. After the cooperative diagnosis, the new record $\vec{r}$ is reconstructed from $\Upsilon(n)$ and sent to the patient p.

3) *Historical Records Update and Store:* The patient p will provide a feedback $f_{r,p}$ to evaluate the diagnosis recommendation performance. In Algorithm 1, we can observe that the upper bound of estimated feedback $\mathcal{G}_{h,m}(t)$ and related parameters are updated. Due to the limited size of context space, if the number of context vectors in $\mathcal{C}$ exceeds $(\frac{\ln t_n}{t_n^2})^\beta$, the space should be partitioned preciously for more accurate recommendations. We can see in Fig. 4 that at timestamp t_0, the radius of partitioned ball is $b_{t_0}^{c_t} = (\frac{\ln t_0}{t_0^2})^\beta$. With the time increasing, at timestamp t_2, the level of radius in the new ball decreases to $b_{t_2}^{c_t} = (\frac{\ln t_2}{t_2^2})^\beta$, which achieves the more accurate division. Similar to context space, the node in the selection tree can also be divided if it is the leaf node or the number of the node (h, m)'s selected times exceeds $\frac{2\ln t}{(\beta_2 \alpha^{h_t})^2}$.

Algorithm 3: The SCB Function.

Input: EN a, r, N_u, N_m, ρ.
Initialize: $\Theta_x = 0$.
Build the random polynomial $\Upsilon(n) = k_0 + k_1 n + k_2 n^2 + \cdots + k_{N_m} n^{N_m}$, $k_0 = r$, to share the record r in EN a, where $k_i \sim B(N_u, p)$, $i \in \{1, \ldots, N_u\}$.
for any one-step neighboring node of EN a in the edge sharing network **do**
  if the shared different records r_x in EN $x \neq \emptyset$ **then**
    $\theta(r_x) = r_x \rho$,
    $\langle r_x\rangle_{p_i} = ([\theta(r_x)]_{p_i}, [r_x]_{p_i})$.
    if $\langle r_x\rangle_{p_i} \geq 0$ **then**
      $\Theta_x = \Theta_x + 1$.
    end if
  end if
  if $\Theta_x \geq \Theta_a$ **then**
    Cooperate with EN x and achieve information sharing.
  end if
end for
Reconstruct $\vec{r}$ from $\Upsilon(n)$
Output: $\vec{r}$.

B. Privacy Analysis

In this subsection, we analyze the requirements of local differential privacy based on the randomized response.

Theorem 1: To maximize the utility of the perturbed medical record r, and ensure the randomized response satisfies ε-local differential privacy, we have $\varepsilon > \ln \max_{q=\{q_1,q_2,\ldots,q_n\}} \frac{\max_{r=\{r_1,r_2,\ldots,r_n\}} p_{q,r}}{\min_{r=\{r_1,r_2,\ldots,r_n\}} p_{q,r}}$, and we get the optimal design matrix $\mathbb{P}$:

$$p_{q,r} = \begin{cases} \frac{\exp^\varepsilon}{n-1+\exp^\varepsilon}, & \text{if } q = r, \\ \frac{1}{n-1+\exp^\varepsilon}, & \text{if } q \neq r, \end{cases}$$

Proof: See proof of Theorem 1 in [37]. ■

Remark 1: From Theorem 1, there is a trade-off between records' utility and privacy which is controlled by ε. Our goal is to ensure the medical records are useful and accurate for patients while respecting the privacy. It must satisfy $\varepsilon \geq 0$, and if $\varepsilon = 0$, each value in the matrix is identical, so 0-local differential privacy makes the output distribution similar to the input, hence we cannot ensure its utility. However, if $\varepsilon = \infty$, the output is the same as the input, and thus its privacy cannot be protected.

Theorem 2 [30]: For the LDP protocol with the optimal design matrix $\mathbb{P} = p_{q,r}$, to account for the impact of randomized response, we can compute the frequency estimation of q in the aggregation technique as:

$$\Omega(q) = \frac{\sum_{q\in\mathcal{Q}} \mathbb{I}_{\mathbb{P}}(q) - N p_{q,r}(q \neq r)}{p_{q,r}(q = r) - p_{q,r}(q \neq r)},$$

where $\sum_{q\in\mathcal{Q}}\mathbb{I}_{\mathbb{P}}(q)$ means that the number of times that q occurs in the set $\mathcal{Q}$ and N is the number of patient in the system. And the variance of the unbiased estimation is

$$Var[\Omega(q)] = \frac{n-2+\exp^{\varepsilon}}{(\exp^{\varepsilon}-1)^2}\cdot N.$$

Remark 2: From Theorem 2, we can see the accuracy of our privacy protection protocol will decrease with n increasing, since the perturbed output can be various although the original record r is unchangeable, which means the distribution of the perturbation is more complicate. Similarly, when the number of patients increases over time, it will cause the data congestion and impact the efficiency of perturbing inputs.

C. Regret Analysis

In the recommendation process, there is always inaccuracy produced by the following two reasons: 1) Select the suboptimal MDR nodes. 2) Randomized response noise from the design matrix. The following lemmas show some details:

Lemma 1: Note that $Var_{h,m}(t)$ is the measurement of noise bypassing the randomized response matrix added to the $\mathcal{G}$-value of cluster (h,m), we let $\psi_{h,m}=\min\{\tau\le t:\mathcal{E}_{h,m}(\tau)\ge \kappa_{h,m}=\lceil\frac{8\ln tVar_{h,m}}{(\Delta_{h,m}-\beta_2\alpha^h)^2}\}\rceil$ for any suboptimal node. We define (h^*,m^*) as the optimal MDR node, we have:

$$\mathbb{P}\{\mathcal{G}_{h,m}(t)>\mathcal{G}_{h^*,m^*}(t),\forall t\ge\psi_{h,m}\}\le 2t^{-4},$$

$$\mathbb{E}[\mathcal{E}_{h,m}(t)]\le\frac{8\ln t(n-1+\varepsilon)}{\varepsilon^2(\Delta_{h,m}-\beta_2\alpha^h)^2}+\frac{\pi^4}{45},$$

where n means the domain range of perturbed output q.

Proof: See proof of Lemma 1 in [37]. ■

And Lemma 1 limits the expected number of records that patient can access. With ε increasing, we can see the upper bound of the number of selected suboptimal nodes will decrease gradually, since it cannot ensure the privacy of selected nodes, and then more selections will cause more risks for privacy.

Theorem 3: The final accumulative regret of LCOL is bounded as:

$$\mathbb{E}[CR(t)]\le 4t\left(\frac{\ln t}{t^2}\right)^{\beta}(\varrho+1)+$$
$$\left(\frac{4\ln t}{\alpha\beta_2\beta_1^{d_0}}+\frac{128\ln t}{\alpha^2}\right)\left(1+\frac{1}{\varrho}\right)\left(\frac{\varrho L_c\sqrt{d_c}}{\beta_2}\right)^{-d_0}$$
$$\cdot(4\pi\ln t)^{\frac{d_0}{d_c(1+\zeta)}}\cdot t^{\frac{-d_0}{d_c(1+\zeta)}}+\frac{128(\varepsilon+n)\ln t\varrho^2L^2d_c}{\varepsilon^2\alpha^2\beta_2\beta_1^{d_0}}\left(1+\frac{1}{\varrho}\right)$$
$$\left(\frac{\varrho L\sqrt{d_c}}{\beta_2}\right)^{-d_0}\cdot(4\pi\ln t)^{\frac{2+d_0}{d_c(1+\zeta)}}\cdot t^{\frac{2-d_0}{d_c(1+\zeta)}}. \quad (7)$$

where $\varrho=\frac{\beta_2\alpha^h}{\lambda_t L}$ is balance factor between context space $\mathcal{C}$ and MDR nodes, and ζ is a positive constant related to context space. Note that d_0 is the near-optimality dimension of context space, and in most of the cases $d_0=0$.

Proof: See proof of Theorem 3 in [37]. ■

Remark 3: In Theorem 3, there are three terms about the regret, each term represents different meanings. The first and second terms are derived from the selection of suboptimal nodes. And the third term comes from the combination of perturbation from randomized response and selection of next optimal nodes for medical records. With the value of ζ increasing, the patients' contextual information will be more similar, which impacts the MDR selection model to make accurate diagnosis. However, the value of ζ cannot be too small. When ζ decreases to a certain low level, the context space will be partitioned too fast, which makes it difficult to select optimal context subspace $M(c_t,b_t)$ and then causes the diagnostic results inaccurate. Notice that the third term follows the highest time order, due to $1>\frac{2-d_0}{d_c(1+\zeta)}>0$ when we let $d_c(1+\zeta)>2$, and thus we achieve a sublinear regret while minimizing the error rate. Meanwhile, the time complexity of cumulative regret equals to $\mathcal{O}(t^{\frac{2-d_0}{d_c(1+\zeta)}})$, which is lower than $\mathcal{O}(t)$. As a result, the computation cost of our method is acceptable in the real-world scenario for real-time diagnosis.

V. Experimental Results

A. Dataset Description

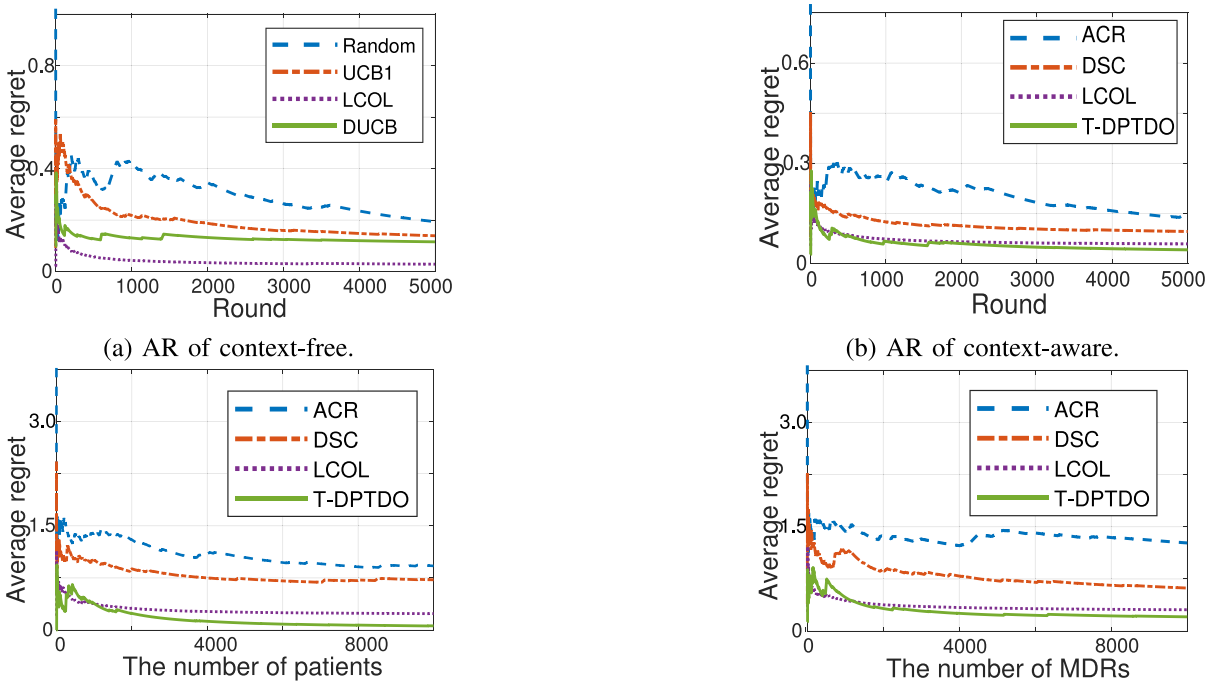
Similar to [36], we utilize the real-world dataset from the patients with coronary heart diseases, which is provided by the Tongji Medical College from Huazhong University of Science and Technology. The causes of the selected CHD patients typically attribute to the fatty deposits of plaque built up in the injury site, and then lead to atherosclerosis. We select 4,241 patients randomly in the dataset, and the medical diagnosis records mainly include four types: 1) Medications (e.g., angiotensin-converting enzyme inhibitors, beta-blockers, statins, calcium channel blockers, etc). 2) Surgery (e.g., laser surgery, coronary bypass surgery, angioplasty and stent placement, etc). 3) Prevention advice (e.g., exercise more, limit alcohol, avoid tobacco, etc). 4) Diagnosis test results (e.g., electrocardiogram, stress tests, CT scans, etc). Our goal is to recommend reasonable and accurate diagnosis records for patients based on their contextual information. There are 16 different contexts in our dataset, and we only consider some representative features: gender (male or female), age, the number of cigarettes each day, prevalent hypertension (yes or no), the value of total cholesterol, heart rate, the value of diastolic blood pressure, the value of systolic blood pressure, the amount of glucose, and the number of historical CHD records within ten years. To specify the parameters in the experiment which is performed on our university's computing platform whose CPU reaches 18.46 TFlops and SSD cache is 1.25 TB, we let $d_c=10$ firstly, and $\zeta=10$ to control the exploitation speed.

B. Comparison With Online Learning Algorithm

To evaluate the average regret (AR) of our algorithm, we compare it with some context-free algorithm first to show the importance of patient's context on the system performance.

1) Random: This algorithm selects one medical diagnosis record randomly each round, which is regarded as the benchmark for other algorithms.

2) UCB1 [31]: As a classical multi-arm bandit algorithm, it can perform well while recommending the optimal medical records for patients without considering personalization.



(a) AR of context-free.

(b) AR of context-aware.

(c) The impact of the number of patients.

(d) The impact of the number of MDRs.

Fig. 5. Comparison with context-free and context-aware algorithms on average regret.

3) DUCB [32]: This distributed online learning system can share information through the network and works similar to the UCB1 algorithm.

In Fig. 5(a), we can observe that our algorithm LCOL outperforms other context-free algorithms largely, since without context, it can only predict based on the historical medical records instead of utilizing the specific patient's contextual information. And we can see that our proposal converges faster than others, which means that context-aware algorithms can achieve more efficient online learning and obtain more accurate recommendations. Notice that there are some fierce fluctuations at the initial stage, which is common as the cold start problem in the recommendation algorithms, but context-free algorithms experience more serious impacts on performances. Next, to measure the total performance, we further compare LCOL with some context-aware algorithms.

1) DSC [33]: As a distributed system, it utilizes the static context space which is built and partitioned in advance to make proper decisions.

2) ACR [34]: This is a centralized contextual algorithm with fixed MDRs, and cannot learn from other resources online.

3) T-DPTDO [35]: This algorithm can support big data analysis, ensure the patients' privacy with exponential mechanism in differential privacy and also consider the network structure in its system model.

While comparing with context-aware algorithms in Fig. 5(b), it is similar to the above conditions, but AR of context-aware algorithms are usually lower than that of algorithms without context. It also shows that AR of T-DPTDO and LCOL is almost same, since LCOL works with local differential privacy which should satisfy more strict requirements compared to the differential privacy mechanism in T-DPTDO and then LCOL will sacrifice some performances. To analyze the adaptation of our algorithm in the big data condition, we use the varied number of patients and MDRs to measure the total performances on AR in Fig. 5(c)–(d). Due to the adaptive tree structure for selecting related medical records in the nodes and efficient partition of context space, our proposal and T-DPTDO can quickly reduce losses with the constantly increasing dataset and achieve a low level of AR. However, the impact on the AR of ACR and DSC is huge. This is mainly because these algorithms are with static and fixed information space, once the dataset expands, they cannot store more information and support massive data analysis, and then cause more regret each round. The results show that LCOL achieves 72.1% and 45.6% performance gains over that of ACR and DSC when the number of MDRs is 8000 in Fig. 5(d). To further demonstrate the advantages of our system model, we evaluate the response time with other related algorithms in Fig. 6. We can see the time consumption of LCOL is evidently optimal, and when the number of patients reaches to 8×10^4, the total time of ACR is 2.45, 1.96, and 1.23 times higher than that of LCOL, T-DPTDO, and DSC. Since our model stores records in the network which supports information sharing, and the MDR selection tree can be partitioned adaptively, LCOL achieves optimal performances.

C. Evaluation of Other Performances

1) Error Rate When the Regret Is Sublinear: When we guarantee the regret is sublinear, we can just focus on minimizing

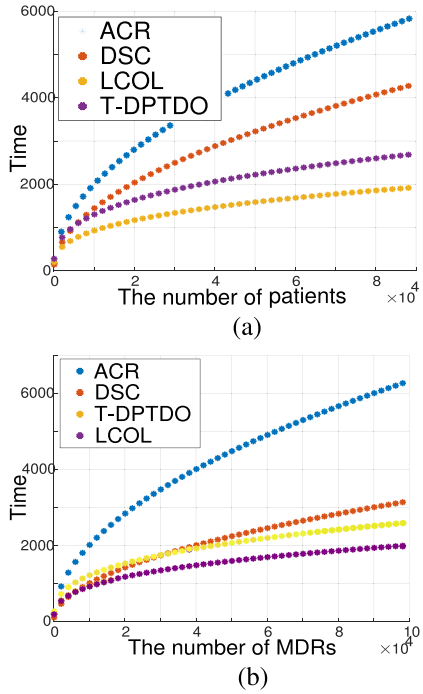


Fig. 6. Comparison with context-aware algorithms on time.

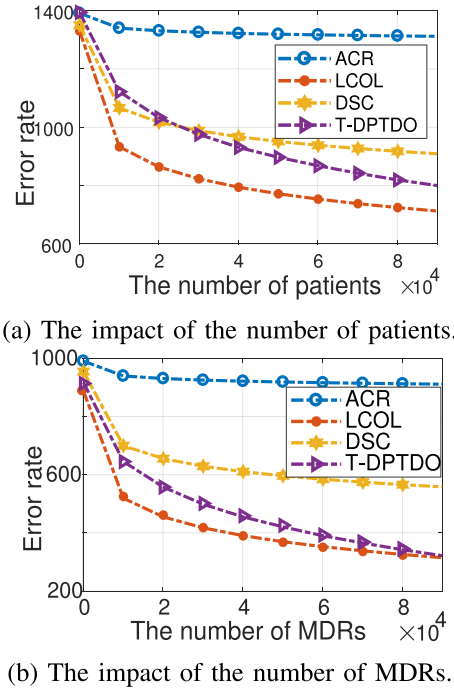


Fig. 7. Comparison of error rate while the regret is sublinear.

the error rate. As shown in Fig. 7, in the beginning, the curve of LCOL has a larger reduction slope than any other algorithms, and it means that our algorithm can efficiently utilize the dataset to make more accurate medical recommendations, so the number of successful diagnosis increases dramatically. However, ER of ACR almost keeps unchangeable, since its MDR space is

TABLE I
THE IMPACT OF d_c ON THE AVERAGE REGRET

d_c	Time Rounds $\times 10^4$								
	2	4	6	8	10	12	14	16	18
$d_c = 3$	0.82	0.71	0.64	0.56	0.48	0.43	0.40	0.37	0.35
$d_c = 6$	0.75	0.67	0.58	0.50	0.43	0.35	0.32	0.30	0.28
$d_c = 9$	0.70	0.63	0.55	0.45	0.38	0.30	0.28	0.26	0.24
$d_c = 12$	0.63	0.57	0.50	0.43	0.36	0.29	0.24	0.21	0.19
$d_c = 15$	0.43	0.38	0.32	0.30	0.28	0.27	0.22	0.17	0.15
$d_c = 16$	0.40	0.35	0.30	0.26	0.24	0.21	0.19	0.17	0.14

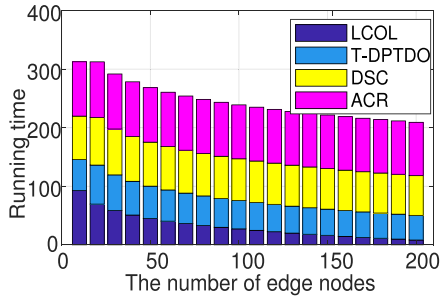


Fig. 8. The impact of the number of edge nodes on running time.

fixed and cannot learn some new information to support more demands by online learning. We can observe the gap of ER between ACR and other algorithms become increasingly larger. As for DSC, it uses the static context space to make predictions, so the increase of patients has more impacts on it than the increase of MDRs. Furthermore, the ER in Fig. 7(b) is lower than that in Fig. 7(a), so it represents that the increase of MDRs is more beneficial for reducing the performance losses than that of patients, which is reasonable in the real-world scenario.

2) Impact of Context Space Dimension d_c: As shown in Table I, we set $d_c = 3, 6, 9, 12, 15$, respectively, and measure the variety of average regret. In terms of row, with a fixed d_c, the AR is decreasing with time rounds increasing, and the speed of decreasing becomes lower since it can converge fast by online learning. In terms of column, if the value of d_c keeps increasing when round n does not vary, which represents that more contextual information can be extracted to accelerate the process of online learning and make the diagnosis recommendation more precious, and then our algorithm will achieve lower regret as expected.

3) The Number of Edge Nodes: In this part, we measure the running time when the number of edge nodes varies in [0,200]. As shown in Fig. 8, the running time of LCOL decreases the fastest as the number of edge nodes increases. The reason is that more edge nodes can offer more chances for cooperation between nodes to make the diagnosis more accurate. However, the time consumption of ACR, DSC, and T-DPTDO initially is shorter than that of LCOL, since they only should select the optimal results as the output, but LCOL with LDP will consume some time to randomly perturb the input bypassing the design matrix. As the number of edge nodes exceeds a threshold, the running time of our algorithm will keep in a low level compared to other algorithms. Furthermore, in Fig. 9, we consider the impact of the number of edge nodes on the value of

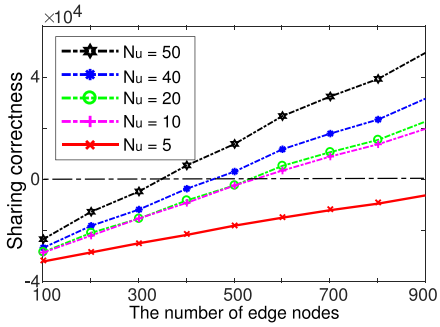


Fig. 9. The impact of the number of edge nodes on correctness.

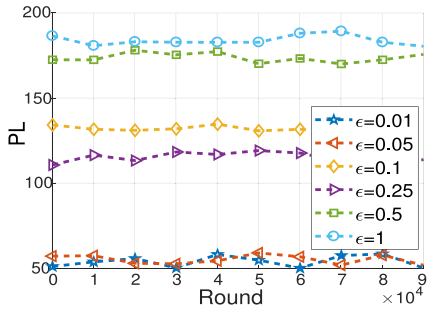


Fig. 10. The impact of different levels of ε on privacy leakage.

correctness in the privacy blockchains. If the number of parties N_u is fixed, we can see that correctness Θ is increasing with the number of edge nodes increasing, since more nodes will make sure the information sharing easier. Moreover, if the number of edge nodes is fixed, when N_u increases, more parties are involved in the sharing secret computation, so it can achieve better information sharing (i.e., Θ increases).

4) Local Privacy-Preserving Level (LPL): We know there is a trade-off between LPL and AR, because when LPL increases, the distribution of data perturbation becomes more evenly and it makes the privacy protection more reliable, but it causes the utility of records decreases and thus produces more regret. Therefore, to measure the LPL, we use privacy leakage $PL = \ln \max_{q=\{q_1,q_2,\ldots,q_n\}} \frac{\max_{r=\{r_1,r_2,\ldots,r_n\}} p_{q,r}}{\min_{r=\{r_1,r_2,\ldots,r_n\}} p_{q,r}}$. In Fig. 10, we can see when the value of ε decreases, the PL also decreases (LPL increases), which accords with our theoretical analysis in Theorem 1. However, we cannot achieve 0-local differential privacy, since we cannot ensure complete data privacy for big data analysis. Similarly, if ε exceeds a certain level, the outcome of privacy protection is slight. Therefore, there should be a range of ε to ensure local differential privacy.

VI. Discussion

In our future work, we would like to operate our system model in other real-world scenarios to improve the total performances of online learning and consider more factors (e.g., environment, social relationship, etc) to improve the accuracy. Actually, the application scenario is not only for CHD in the hospital, but also feasible for other privacy-preserving disease diagnosis (e.g., lung cancer, genetic disease).

Besides, to satisfy the experimental conditions, it needs lots of works. First, there should be enough medical diagnosis records for online learning accuracy. Next, we need some mobile devices modelled as ENs to send and receive medical records with information sharing, and some devices as containers to store basic information like the block body and block head in blockchains. Finally, to ensure the privacy of personal information, the randomized response for data perturbation and the blockchain for secure medical transaction must be only accessible in the model level. However, there are some potential drawbacks of our approach, like that the model needs the positive cooperation of different technologies, otherwise causing negative results, and the amount of shared information between ENs is limited.

VII. Conclusion

In this article, we present a novel blockchain-enabled contextual online learning algorithm under local differential privacy for CHD diagnosis in mobile edge computing supporting big data analysis. Our detailed theoretical analysis and comparison with existing algorithms verify the optimal performances of our algorithm. Specifically, our proposed algorithm outperforms related context-aware privacy-preserving approaches by about 21% in terms of error rate when the regret is sublinear and 31% in terms of running time.

References

[1] C. Nordqvist, "What to know about coronary heart disease,"Jul. 2019. [Online]. Available: https://www.medicalnewstoday.com/articles/184130.php
[2] GBD 2015 Mortality and Causes of Death Collaborators, "Global, regional, and national life expectancy, all-cause mortality, and cause-specific mortality for 249 causes of death, 1980-2015: A systematic analysis for the Global Burden of Disease Study 2015," London, vol. 388, pp. 1459–1544, 2016.
[3] "How Is Coronary Heart Disease Diagnosed?" U.S. Department of Health & Human Services, Sep. 2014.
[4] S. Hongzong *et al.*, "Support vector machines classification for discriminating coronary heart disease patients from non-coronary heart disease," *WestInd. Med. J.*, vol. 56, no. 5, pp. 451–457, 2007.
[5] H. D. Liang, J. A. Noble, and P. N. T. Wells, "Recent advances in biomedical ultrasonic imaging techniques," *Int. Focus*, vol. 1, no. 4, pp. 475–476, 2011.
[6] S. G. Mougiakakou, S. Golemati, I. Gousias, A. N. Nicolaides, and K. S. Nikita, "Computer-aided diagnosis of carotid atherosclerosis based on ultrasound image statistics, laws' texture and neural networks," *Ultrasound Med. Biol*, vol. 33, no. 1, pp. 26–36, 2007.
[7] L. Song, W. Hsu, J. Xu, and M. van der Schaar, "Using contextual learning to improve diagnostic accuracy: Application in breast cancer screening," *IEEE J. Biomed. Health Inform.*, vol. 20, no. 3, pp. 902–914, May 2016.
[8] C. Tekin, S. Zhang, and M. van der Schaar, "Distributed online learning in social recommender systems," *IEEE J. Sel. Topics Signal Process.*, vol. 8, no. 4, pp. 638–652, Aug. 2014.
[9] T. X. Tran, A. Hajisami, P. Pandey, and D. Pompili, "Collaborative mobile edge computing in 5G networks: New paradigms, scenarios, and challenges," *IEEE Commun. Mag.*, vol. 55, no. 4, pp. 54–61, Apr. 2017.
[10] M. Du, K. Wang, Y. Chen, X. Wang, and Y. Sun, "Big data privacy preserving in multi-access edge computing for heterogeneous internet of things," *IEEE Commun. Mag.*, vol. 56, no. 8, pp. 62–67, Aug. 2018.
[11] J. C Duchi, M. I. Jordan, and M. J. Wainwright, "Local privacy and statistical minimax rates," in *Proc. IEEE 54th Annu. Symp. Found. Comput. Sci.*, 2013, pp. 429–438.
[12] G. Zyskind, O. Nathan, and A. Pentland, "Enigma: Decentralized computation platform with guaranteed privacy," in *New Solutions for Cybersecurity*, MIT Press, 2018, pp. 425–454.

[13] A. C. Y. Tossou and D. Christos, "Achieving privacy in the adversarial multi-armed bandit," *Thirty-First AAAI Conf. Artif. Intell.*, pp. 2653–2659, 2017.
[14] K. Orphanou, A. Stassopoulou, and E. Keravnou, "DBN-extended: A dynamic Bayesian network model extended with temporal abstractions for coronary heart disease prognosis," *IEEE J. Biomed. Health Inform.*, vol. 20, no. 3, pp. 944–952, 2015.
[15] Y. Wang, X. Wu, and D. Hu, "Using randomized response for differential privacy preserving data collection," in *Proc. EDBT/ICDT Workshops*, 2016, pp. 1–12.
[16] M. N. Elbedwehy, H. M. Zawbaa, N. Ghali, and A. E. Hassanien, "Detection of heart disease using binary particle swarm optimization," *Federated Conf. Comput. Sci. Inf. Syst.*, Wroclaw, 2012, pp. 177–182.
[17] C. Tekin and M. van der Schaar, "Distributed online learning via cooperative contextual bandits," *IEEE Trans. Signal Process.*, vol. 63, no. 14, pp. 3700–3714, Jul. 2015.
[18] L. Song, C. Tekin, and M. van der Schaar, "Online learning in large-scale contextual recommender systems," *IEEE Trans. Serv. Comput.*, vol. 9, no. 3, pp. 433–445, May/Jun. 2016.
[19] U. Erlingsson, V. Pihur, and A. Korolova, "Rappor: Randomized aggregatable privacypreserving ordinal response," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, 2014, pp. 1054–1067.
[20] G. Fanti, V. Pihur, and U. Erlingsson, "Building a rappor with the unknown: Privacypreserving learning of associations and data dictionaries," in *Proc. Privacy Enhancing Technol.*, vol. 2016, no. 3, pp. 41–C61, 2016.
[21] T. Wang, J. Blocki, N. Li, and S. Jha, "Locally differentially private protocols for frequency estimation," *26th USENIX Security Symp.*, 2017, vol. 17, pp. 729–745.
[22] D. Bogdanov, S. Laur, and J. Willemson, "Sharemind: A framework for fast privacy-preserving computations," *Eur. Symp. Res. Comput. Secur.*, Heidelberg, 2008, pp. 192–206.
[23] S. L. Warner, "Randomized response: A survey technique for eliminating evasive answer bias." *J. Amer. Statistical Assoc.*, vol. 60, pp. 63–69, 1965.
[24] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash," *J. Syst.*, 2008.
[25] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger" *J. Ethereum Project Yellow Paper*, 2014, pp. 1–32.
[26] C. Cachin, "Architecture of the hyperledger blockchain fabric," *Workshop Distrib. Cryptocurrencies Consensus Ledgers*. 2016.
[27] I. Damgard, M. Keller, and E. Larraia, "Practical covertly secure MPC for dishonest majority-or: Breaking the SPDZ limits," *Eur. Symp. Res. Comput. Secur.*, Heidelberg, pp 1–45, 2013.
[28] Z. Xiong, Y. Zhang, D. Niyato, P. Wang, and Z. Han, "When mobile blockchain meets edge computing," *IEEE Commun. Mag.*, vol. 56, no. 8, pp. 33–39, Aug. 2018.
[29] H. Liu, Y. Zhang, and T. Yang, "Blockchain-Enabled Security in Electric Vehicles Cloud and Edge Computing," *IEEE Netw.*, vol. 32, no. 3, pp. 78–83, May/Jun. 2018.
[30] T. Wang, N. Li, and S. Jha, "Locally differentially private frequent itemset mining," *IEEE Symp. Secur. Privacy*. 2018, pp. 127–143.
[31] P. Auer, N. Cesa-Bianchi, and P. Fischer, "Finite-time analysis of the multiarmed bandit problem," *J. Mach. Learn.*, vol. 47. no. 2–3, pp. 235–256, 2002.
[32] S. Buccapatnam, A. Eryilmaz, and N. B. Shroff, "Multi-armed bandits in the presence of side observations in social networks," *IEEE Conf. Dec. Control*. pp. 7309–7314, 2013.
[33] C. Tekin and M. Van der Schaar, "Distributed online big data classification using context information," *51st Annu. Allerton Conf. Commun., Control, Comput.*, 2013, pp. 1435–1442.
[34] L. Song, C. Tekin, and M. van der Schaar, "Online Learning in Large-Scale Contextual Recommender Systems," *IEEE Trans. Services Comput.*, vol. 9, no. 3, pp. 433–445, 1 May/Jun. 2016.
[35] P. Zhou, K. Wang, J. Xu, and D. Wu, "Differentially-private and trustworthy online social multimedia big data retrieval in edge computing," *IEEE Trans. Multimedia*, vol. 21, no. 3, pp. 539–554, Mar. 2019.
[36] C. Tekin, O. Atan, and M. Van Der Schaar, "Discover the expert: Context-adaptive expert selection for medical diagnosis," *IEEE Trans. Emerg. Topics Comput.*, vol. 3, no. 2, pp. 220–234, 2014.
[37] X. Liu *et al.*, "Supplementary: Blockchain-enabled contextual online learning under local differential privacy for coronary heart disease diagnosis in mobile edge computing," Oct. 2019. [Online]. Available: https://www.dropbox.com/s/hy1blzknni4p6cn/JBHI_supp.pdf?dl=0