PMHE:A Wearable Medical Sensor Assisted Framework For Health Care Based On Blockchain And Privacy Computing

Jindong Zhao
Yantai University
Wenshuo Wang (wangwsh202121@163.com)
Yantai University https://orcid.org/0000-0002-1645-1549
Dan Wang
Yantai University
Chunxiao Mu
Yantai University

Research Article

Keywords: Blockchain, Homomorphic encryption, Smart contracts, Privacy computing, Smart medical.

Posted Date: December 29th, 2021

DOI: https://doi.org/10.21203/rs.3.rs-1121236/v1

Abstract

Nowadays, smart medical cloud platforms have become a new direction in the industry. However, because the medical system involves personal physiological data, user privacy in data transmission and processing is also easy to leak in the smart medical cloud platform. This paper proposed a medical data privacy protection framework named PMHE based on blockchain and fully homomorphic encryption technology. The framework receives personal physiological data from wearable devices on the client side, and uses blockchain as data storage to ensure that the data cannot be tampered with or forged; Besides, it use fully homomorphic encryption method to design a disease prediction model, which was implemented using smart contracts. In PMHE, data is encoded and encrypted on the client side, and encrypted data is uploaded to the cloud platform via the public Internet, preventing privacy leakage caused by channel eavesdropping; Smart contracts run on the blockchain platform for disease prediction, and the operators participating in computing are encrypted user data too, so it avoids privacy and security issues caused by platform data leakage. The client-to-cloud interaction protocol is also designed to overcome the defect that fully homomorphic encryption only supports addition and multiplication by submitting tuples on the client side, to ensure that the prediction model can perform complex computing. In addition, the design of the smart contract is introduced in detail, and the performance of the system is analyzed. Finally, experiments are conducted to verify the operating effect of the system, ensuring that user privacy is not leaked without affecting the accuracy of the model, and realizing a smart medical cloud platform in which data can be used but cannot be borrowed.

1 Introduction

In recent years, with the application of new technologies such as smart healthcare and mobile healthcare, medical data, such as electronic health records, clinical measures,personal health status records perceived by wearable sensors, have all shown explosive growth [1,2]. In online medical system, the procedure of authorization distribution, transmission and processing of data involve not only data exchange and transmission technology, but also the privacy security of data source [3,4] and the trust of multiple nodes participating in data sharing [5]. Furthermore, in the mobile and health medical service system, People's awareness of data privacy protection is weak, and attackers tend to connect users' medical data with network behaviors, which makes the impact of medical privacy disclosure more serious [6].

With the development of blockchain technology, it has gradually been applied in the medical field. The main application areas of blockchain include the secure sharing and privacy protection of medical data, among which the privacy protection of medical and health data is the research focus [7]. The essence of blockchain technology is decentralization, which ensures that medical data will not be manipulated or damaged in an environment of mutual distrust. The encryption algorithm provides anonymity for blockchain and protects the privacy of patients' information. In view of the privacy disclosure and information islands of medical data, the decentralized, distributed storage, anonymity and other features of blockchain not only guarantee the privacy and security of medical data, but also provide possibilities

for the safe transfer of medical data,which has attached extensive attention of researchers in the medical field.

Blockchain ensures that data cannot be tampered with or forged. However, on the smart medical cloud platform deployed on Internet, users need to upload physiological data to the cloud platform through the public link, and then be computed on cloud platform using the preset model to predict diseases and monitor health. There is a risk of data leakage during this process. In addition, models on cloud platforms require user data as raw formation for computing. Cloud platforms are untrusted third parties, and data may be leaked on cloud platforms.

In this paper, we present a smart medical cloud platform framework based on privacy computing, and its abbreviation is PMHE. The platform calculate users' physiological data that is encrypted on client side, and use the results to predict diseases. It can protect users' privacy in communication and computing. Although the data is encrypted, the accuracy of the model is not affected.

1.1 Contributions

PMHE utilizing blockchain and fully homomorphic encryption technology builds an intelligent medical data and privacy protection framework to solve many problems. Those problems include privacy disclosure and data tampering caused by data loss and hacking.

The advantages mentioned above enable the data consumers and data providers to realize the trust transaction of medical data on the platform without the trust endorsement of the third-party platform [8]. People can enjoy the disease prediction, health monitoring and other medical services provided by the platform securely. The main contributions in this paper can be summarized as follows:

- Proposed the PMHE framework. This is a privacy protection scheme of smart medical data based on blockchain technology and fully homomorphic encryption technology. Compared to most existing schemes, PMHE does not rely on any trusted third party or tamper-proof hardware, but only involves portable wearable medical devices, blockchain and (untrusted) clouds. In terms of storage and computing costs, PMHE also makes significant improvements to existing medical data management solutions based on blockchain.
- Design interaction protocols with desired functionality for PMHE under the universally compostable framework. Generally, the computing model in the cloud involves complex operations, but holomorphic encryption algorithm only supports addition and multiplication. The interaction protocol allows any computation to participate in homomorphic evaluations.
- Implement PMHE scheme based on Hyperledger Fabric, and conduct comprehensive experiments to evaluate its performance. The experimental results show that PMHE increases affordable communication costs and storage costs while providing safe, full-featured disease prediction and health monitoring functions.

1.2 Structure

This paper is divided into seven parts.Section 1 introduces the research motivation and contribution, Section 2 introduces correlational researches and preparatory knowledge, Section 3 and 4 introduce the process and results of implementing PMHE, Section 5 deeply studies the privacy security of PMHE, and Section 6 carries out specific experiments and analyzes experimental data .Finally, the thesis is summarized in Section 7.

2 Related Works And Preparation

2.1 Related Works

With the advent of blockchain, many privacy protection scheme of medical data based on blockchain have been proposed. In 2019, Hylock et al. proposed a mixed-block blockchain framework to support immutable logging and editable patient blocks[9]. This framework utilized smart contracts to share patient-generated accumulated data through blockchain, which enhanced interoperability and security of healthcare data. Ruijin Wang et al. in 2019 put forward a model of decentralized medical data sharing based on blockchain [10], This model uses ring signature technology in blockchain to construct a private data storage protocol, which can protect the privacy of medical data and patient identity. Besides, smart contract was used in this model to execute preset access control commands automatically and guarantee the confidentiality of medical privacy data. In 2021, Jingwei Liu et al. proposed a privacy-preserving medical data sharing scheme based on consortium blockchain [11]. This scheme uses on-chain-off-chain storage model to reduce the storage burden of blockchain, in which only the metadata of electronic medical records was recorded, while the patient's medical data was encrypted and stored in the cloud. Zhou Zhengqiang et al. proposed a medical data security sharing scheme based on consortium blockchain in 2021[12]. The scheme used consortium blockchain to store metadata and cloud storage to store ciphertext of medical data. In addition, the combination of time-limited smart contract and ciphertext-policy attribute-based encryption (CP-ABE) technology realized fine-grained access control and secure storage of medical data.

2.2 Blockchain and Smart Contract

The structural concept of blockchain was proposed as early as in the 1990s, and it was not until 2008 that Satoshi Nakamoto put forward the concept of blockchain for the first time in his published paper [13]. Blockchain can be regard as a decentralized database of blocks that can be added continuously, a self-referential data structure that is open, transparent, immutable, and traceable. Blockchain is not one new technology, but is implemented through a combination of technologies such as cryptography, distributed networks and consensus algorithms.

Smart contract, known as Chaincode in Hyperledger, is essentially a program that runs on blockchain, and its code and data are stored on blockchain too. It solves the problem of limited flexibility by allowing authorized participants to manipulate applications and reach consensus on the blockchain. Due to the openness and immutability of blockchain, once a smart contract is deployed on it, any information on the smart contract will be open and transparent, and cannot be modified by traditional methods. Therefore,

smart contracts should not contain too much external logic and confidential information. If a smart contract involves confidential information, the confidential information should be encrypted before writing. In addition, since the preparation of a complete smart contract involves many aspects such as privacy, security, legal issues and mechanism design [14], it is a key issue for practical application to design a safe smart contract which is fair, reliable and complies with specifications.

2.3 Fully Homomorphic Encryption

As early as 1978, Rivest et al. first proposed the idea of Fully Homomorphic Encryption (FHE) [15,16]. Since then, the study of Fully Homomorphic Encryption algorithm has been listed as a research difficulty in the field of cryptography. It was not until 2009 that Gentry constructed the world's first fully homomorphic encryption scheme based on lattice cryptography [17], which was homomorphic for fixed number of operation operations (usually called circuit depth). Then researchers began to improve on the basis of Gentry's work, and developed more perfect homomorphic encryption algorithm. CKKS homomorphic encryption scheme was proposed by Cheon et al. in 2017[18]. It supports approximate floating-point operations and is one of the most important and suitable similar algorithms in homomorphic encryption field.

Fully homomorphic encryption scheme supports both homomorphic addition and multiplication, and the number of operation rounds is unlimited. At present, homomorphic encryption technology plays an important role in privacy security of cloud computing system. After encoding and encrypting, the user stores the ciphertext in blockchain. Without the user's private key, the real plaintext data of the user cannot be obtained [19].In operation procedure, encrypted plaintexts are involved in homomorphic evaluations. After completion of operation using ciphertext, user can decrypt the result using his/her private key, and the output of decryption operation is almost the same as computation result on original data. The detail process of full homomorphic encryption is shown in Fig. 1.

In the cloud computing system, the functions in the left box are implemented in client side, while the functions in the right box are implemented in cloud system.

Homomorphic encryption (HE) is a cryptographic scheme that enables homomorphic operations on encrypted data without decryption. For arbitrary function f and message m, holomorphic encryption has the following properties [6]:

$$Dec(f(Enc(m1), Enc(m2), \ldots, Enc(mn))) = f(m1, m2, \ldots, mn) \quad (1)$$

In our proposal, users use homomorphic encryption algorithm to encrypt medical data before uploading it, and then upload the encrypted medical data to the blockchain. Because homomorphic encryption algorithm has homomorphism, smart contracts on blockchain can directly bring ciphertext into AI model to calculate. Homomorphism means that two plaintext m_1 and m_2 satisfy the property $Dec(f(Enc(m_1) \oplus Enc(m_2)) = m_1 \otimes m_2$. *Enc* refers to the encryption algorithm, *Dec* refers to the decryption algorithm, $\oplus$ refers to the operations on encrypted data, and $\otimes$ refers to the operations on the plaintext data. When $\otimes$

represents addition, it means that the algorithm supports homomorphic addition operation. When ⊗ represents multiplication, it means that the algorithm supports homomorphic multiplication operation. Based on the characteristics mentioned above, we combine blockchain, deep learning and homomorphic encryption technology to obtain a scheme that can analyze medical data in blockchain network. The scheme uses homomorphic encryption technology to ensure both the privacy and availability of medical data.

Homomorphic encryption technology is a reliable tool and security basis for users to conduct data mining and analysis calculation in blockchain network [20]. In PMHE, blockchain technology is combined with homomorphic encryption technology, and CKKS encryption algorithm for approximate arithmetic is introduced to realize homomorphic evaluations on shared data.

2.4 CKKS

Unlike other LWE-based encryption schemes, rescaling is introduced in CKKS scheme for managing the magnitude of plaintext [14]. After multiplication of encrypted message, the plaintext encrypted divided by an integer. By taking advantage of the rounding feature of floating-point number and scientific notation in approximate arithmetic, some imprecise lower bits in the plaintext are removed. And the size of message remains the same before and after encoding. Besides, the maximum ciphertext module required by the scheme increases linearly with the depth of the operation circuit, which greatly improves the efficiency of the scheme and promotes the practical development of the scheme.

In PMHE framework, the cloud system is divided into cloud server and blockchain according to functions. The basic Web application is implemented on the cloud server, and the disease prediction AI model written by smart contract is run on the blockchain. The homomorphic operations in AI model are implemented with CKKS encryption scheme. CKKS uses *Ecd*, *Dcd* and scaling factor Δ to map messages to plaintext. For example, the message is complex number, and the plaintext is an element on the cyclotomic polynomial ring $R = Z[X]/(\Phi M(X))$. *Dcd* first divides the plaintext polynomial $m(X)$ by factor Δ, then computes the function value of the plaintext polynomial at the root of the cyclotomic polynomial ring $\Phi M(X)$, and rounds numbers to get the final complex number vector of message. *Ecd* is the inverse transformation of *Dcd* [21].

3 System Architecture And Security Model

This section describes the system architecture and security model in terms of desired functionality firstly, then, the design goals of the privacy-protected solution defined with the desired functionality in PMHE is introduced.

3.1 System Architecture

As shown in Fig. 2, the PMHE framework involves five types of entities: portable wearable medical devices, client apps, cloud servers, disease prediction models, and the blockchain with smart contracts.

- Portable wearable medical devices. Portable wearable medical devices mainly refer to portable electronic devices that can be directly worn in clinical or daily health monitoring [6]. The intelligent medical devices mainly used in this paper include smart bracelets, smart watches and ECG underwear. Portable wearable medical devices can continuously collect physiological data of the human body at anytime, anywhere and in any environment. It mainly collects such data as heart rate, ECG, respiration and blood pressure through sensors arranged in body surface, so as to prediction of diseases later.
- Client APP. It is used to receive data from wearable devices, perform preliminary filtering on original data, then encode and encrypt the filtered data, and finally upload the ciphertext to the cloud platform. In addition, it receives the resulting message after homomorphic operations returned from the cloud platform, then decrypts the results to get the plaintext, and shows the corresponding health status for user. Last but not least, it generates public/private key pairs for secure communication and signature generation, and interacts with the server through the protocol to determine the format of the data to be uploaded.
- Cloud server. The cloud server, which does not need full trust, is responsible for receiving and processing the user's health data and returning the resulting message after homomorphic operations to the client. Model selection server deployed on the cloud server. The server determines the data format that the client needs to provide according to model selection algorithm. Besides, because the client does not know the meaning of plaintext results after decryption operation, the server also needs to send the specific meaning of each part of the plaintext results to the client.
- Disease prediction model. Disease prediction models are written using smart contracts and run on blockchain. The model uses specific AI algorithm to analyze and calculate encrypted health data, so as to realize early warning and health monitoring. Through machine learning and deep learning algorithm, the disease prediction model can not only be used for the monitoring and early warning of heart disease or hypertension, but also can be widely used for other field such as pregnant women care, the early warning of lung disease and Alzheimer's disease.
- The blockchain with smart contracts. Smart medical care involves a large amount of personal health data. Traditional cloud storage uses traditional database systems to manage user information, which is easy to be tampered and forged by malicious users, posing a great threat to data security. In PMHE, consortium blockchain isused to store user data,and AI prediction algorithms are written using smart contract. Medical data and the program will be stored synchronously at different nodes on the blockchain network,which ensure the failure of a single node will not cause the collapse of the entire system. Smart contracts also ensure the security and reliability of the AI model. Blockchain and smart contract can avoid data loss, program change, data leakage and other problems, greatly ensuring data and function security.

3.2 Security Model

In cloud computing system, user data faces two risks of privacy disclosure. One is that offline data may be eavesdropped during network transmission, while another is that data leakage will happen in the

cloud.

- Network eavesdropping. Network eavesdropping is a kind of passive attack. The cloud system communicates with the client via the public link over Internet. Attackers can obtain user data by eavesdropping communication channel between the client and the cloud system. The most powerful way to and then transmit ciphertext over the Internet.
- Data leakage. If the cloud server is not fully trusted, it may expose users' personal medical data. Or the cloud system could be trusted, but an attacker could still gain access to user data by hacking into the cloud system. Encryption is the most suitable solution to this security problem. In the cloud system, ciphertext is received and the AI model uses ciphertext for calculation. In the absence of a secret key, even if an attacker has access to the data, he or she cannot know the user's privacy.

The PMHE framework can achieve the following security objectives:

- Security. In the process of data up-chain and AI model calculation, the data is in ciphertext form, which ensures the safety of data processing.As for data storage, data is stored using blockchain to ensure data storage security.
- Privacy. Even if the data is eavesdropped during transmission or leaked in the cloud, the attacker can only obtain the ciphertext encrypted with the user's public key. Without knowing the user's private key, the attacker cannot obtain the valuable information contained in the data.

4 The Framework Of Pmhe

PMHE is a cloud computing framework for smart medical systems based on blockchain and homomorphic encryption technology. The wearable medical device transmits the collected physiological data of the user to the client, and then the client encodes and encrypts the data. The encrypted plaintexts is transmitted to the blockchain and triggers a smart contract on the blockchain. The AI prediction model written using smart contract calculates the ciphertext and predicts the results. The client receives the resulting message after homomorphic operations from the cloud server, and finally gets the predictive plaintext by homomorphic decryption. According to the plaintext information, the client can predict the user's disease or evaluate the user's health status. The Program framework of PMHE with CKKS Supporting in Fig. 3.

The basic idea of PMHE is to use CKKS encryption algorithm to encrypt plaintext into ciphertext during medical data transmission, calculation, and storage. And the entire process of computing is encrypted to ensure data integrity, privacy and security. Therefore, it is necessary to improve each stage in order to use ciphertext to achieve its function. Table 1 lists the symbols involved in PMHE.

4.1 The Design of Data Tuple

CKKS encryption algorithm only supports addition and multiplication, but AI model involves some functional operations which do not meet homomorphism characteristic, such as exponential function, logarithmic function , square root function etc. Although some functions can be converted to addition and multiplication by polyfit (for example, sigmod can be fitted using polynomial approximation), a lot of ciphertext operations need to be performed in blockchain network. These extra operations will not only result in a loss of efficiency, but will more likely exceed the CKKS multiplication limit.

In PMHE, the AI model algorithm is converted into the formation of the data and their polynomial, so that the number of multiplications meets the CKKS limit. The cloud and the client interact by protocol. The server notifies the client to provide basic functions or basic functions' combination of the original data. The client encrypts the original data and the corresponding function values, and then sends them together to the server in the form of data tuple, so as to the server can perform homomorphic addition and multiplication operations. The AI model can calculate these encrypted data efficiently and conveniently. The protocol using in PMHE is described as follows:

1). the server sends the tuple template to the client.

$$P=(\{x, y, z, w, F_1(x\ y\ z\ w), \ldots, F_n(x\ y\ z\ w)\}) \longrightarrow C \qquad (2)$$

Where *x, y, z, w* are the original data of the client. is the meta function of the original data. The original data of the independent variable is not all empty.

2). The client responds to the server, encodes the original data and value of meta functions required by the server as operation factors, encrypts them into ciphertext *M* in the form of tuples, and sends them to the server.

$$(x, y, z, w) \xrightarrow{E} \{B_x, B_y, B_z, B_w, B_1, \ldots, B_n\}$$

$$\xrightarrow{Enc} \{M_x, M_y, M_z, M_w, M_1, \ldots, M_n\} = M \qquad (3)$$

$$P \longrightarrow M \longrightarrow S \qquad (4)$$

Where $B_x = E(x)$, $B_i = E(F_i)$, $M_x = Enc(B_x)$, $M_i = Enc(B_i)$, $1 \le i \le n$.

3). While the server receives the ciphertext data, it uploads them to the blockchain, where the AI prediction model can directly perform approximate calculations on ciphertext and eventually send the prediction results to the client.

$$Q = F(x, y, z, w) \qquad (5)$$

$$Z = F(M) \qquad (6)$$

$$Q \approx D(Dec(Z)) \qquad (7)$$

4.2 PMHE Scheme

In PMHE, a data tuple is generated on the client side firstly and then submits the tuple data using CKKS homomorphic encryption to hide valuable information. An ideal property of the CKKS scheme is that the ciphertext can be computed directly without prior decryption of the ciphertext. Therefore, privacy security, data authorization distribution and secure transmission of personal data are ensured.

TABLE 1. PMHE symbol definition

Symbol	*Definition Description*
Enc	Cryptographic operations
Dec	Decryption operation
E	Encoding operation
D	Decoding operation
P	Original data
B	Plaintext
M	Encrypted plaintext
Q	Unencrypted computation on original data
Z	Resulting message after homomorphic operations
S	Server
C	Client
x	Heart rate
y	Diastolic blood pressure
z	Systolic pressure
w	Respiratory rate
F	Disease prediction AI algorithm

1) INITIALIZATION. In the initialization phase, the user registers with the client APP, connects the client to the wearable device, and generates the public/private key pair. The public key represents the unique identity and is used to protect data in homomorphic encryption algorithms. The private key is used to sign the submitted data, verify the user's identity, and decrypt the calculation results returned by the cloud.

2) SUBMIT.AI model is deployed on the blockchain and implemented as a smart contract.The client obtains the physiological data collected by the wearable device, encrypts them with the public key after coding, and submits them to the cloud application. The cloud calls the corresponding smart contract, performs the data calculation, and saves the data to the blockchain.

3) PREDICTION. Based on the physiological data collected by wearable devices, ciphertext is calculated in the AI model. After the calculation, the result Z is obtained. In the calculation process of AI model based on homomorphic encryption technology, the valuable information contained in the data cannot be observed, which ensures the privacy of user data.

4) REPORT. Transforming physiological indicator data collected by wearable devices into disease prediction results with medical value provides users with low-cost, high-quality and high-precision medical information. For example, intelligent heart health assessment algorithm can efficiently and accurately predict whether a person has coronary heart disease, and is not affected by the individual ability of the doctor. However, the results in encrypted formation cannot be used for diagnostics, so the server cannot understand it and sends the results to the client.

5) DIAGNOSIS. After the client receives the operation result of the ciphertext, it decodes and decrypts it with the private key to get the unencrypted AI model result *Q*, and then compares the model reference criteria to give the diagnostic result.

4.3 Smart Contract

Smart contracts can be used to accomplish more complex business logic when more business and application requirements need to be fulfilled in the blockchain. Essentially, smart contracts are pieces of executable code that run in a blockchain, so they have the same decentralized and autonomous characteristics as blockchain. In the PMHE framework, the principle of full homomorphic encryption based on smart contracts is as follows[22]:

1) *setup*(*m*):It refers to the function that selects AI model according to parameter *m*.

2) *receive*(List(*tuple*)):It refers to receiving a list of encrypted data tuples from the client

3) *issue*(*result*):It refers to issue the results of the AI model operation on encrypted data to the client

4) *add(pk, ciphertext1, ciphertext2)*:It refers to the homomorphic function of addition, which can be used by users to perform addition calculations on ciphertext data

5) *mult(pk, ciphertext1, ciphertext2)*:It refers to a homomorphic function of multiplication that users can use to multiply on ciphertext data.

The formal description of the FHE-Contract algorithm is as follows:

- Input: The encrypted dataset uploaded by the client
- Output: The results of the homomorphic calculation on the encrypted data. The specific algorithm description is shown in Fig. 4.

5 Discussion And Analysis

In this section, we first gives a formal security proof of privacy under the universally composable framework, and then analyzes PMHE performance from a communication and computing perspective.

5.1 Privacy Security

Unlike traditional cloud computing application frameworks, PMHE consists of three components: client, cloud system and blockchain. By using the CKKS algorithm,the system realizes the function of data security protection in communication and calculation. The task of client is to generating keys, selecting CKKS algorithm parameters. Besides,it is responsible for encoding and encrypting user data. All those operations ensure the security of data transmitted over the Internet, and the user data participate in operation of the AI model are encrypted too. The server sends the calculation results on cryptographic state to the client. The client gets an approximation which is extremely close to the real results. By comparing the results with the reference criteria, we can get a diagnosis.

In the entire process of data processing, encrypted data is transmitted on the public link between the server and the client. Cloud server and smart contract are all deal with ciphertext. As a result, user privacy and medical data are protected furthest.

5.2 Performance Analysis

Compared with the traditional smart medical cloud platforms, PMHE ensures data security, and the data is encoded to meet the CKKS algorithm which cause an increasing of data size. In the calculation process, each multiplication involve rescale and re-linearize operation[23], which result in more calculated workload. According to the interaction protocol, the tuple transmitted in PMHE is several times larger than the original data. As a result, PMHE adds additional overhead in terms of communication, computing, and storage.

Suppose there are three items in user physiological indicator, referred as X:

$$X = \{x_1, x_2, x_3\} \quad (8)$$

Each physiological indicator in the original data is a 32-bit single-precision floating-point number, then an entire user data need 12 bytes for a triple. In CKKS, assuming that the polynomial modulus is 8192 and the coefficient modulus is {60, 40, 40, 60}, the plaintext will have 32756 elements and the encrypted plaintext will have 65536 elements. A total of 262144 bytes are consumed after the triple is encoded and encrypted on client side.

Communacation Cost. At communication stage, the first interaction between the medical device and the cloud requires setting interaction parameters for each other, and users only upload medical data in the rest of the time. Wearable devices usually upload data at a frequency of from 1 time per minute to 1 time per 10 minutes, depending on the user's physical condition. Even at the highest frequency, we assume that the data tuple contains three physiological indicators, and each of them carry four meta functions. The system need upload approximately 1MB bytes per minute, and the network speed requirement is about 136kbps, which is generally acceptable in the WiFi environment or 4G environment.

Computing Cost. In PMHE, computing tasks are assigned to the client device and the blockchain. Encoding, encryption, decryption and decoding of user data are completed on the client, while the AI model runs on smart contract of blockchain. During client initialization, the operation of generating key pair causes extra computation time. In addition, each sensor data and its basic operators need to be encoded as plaintext (encoded message).The length of plaintext is polynomial modulus times longer than original data. After encrypting, the length of encrypted plaintext is twice as long as plaintext. Compared with traditional clients in cloud computing system, each data upload costs more computing time, but the interval of one minute for uploading data can be ignored.

The AI model perform homomorphic operations on encrypted data [18] on blockchain network, and most of these operations are multiplication. Since the operators are polynomial, and the operations such as rescaling and relinearize are required for each multiplication, the computational complexity is greatly increased. However, blockchain itself is a distributed system, made up of many nodes, which allows computing to take place without centralization. The structural characteristics of blockchain can effectively relieve the computational stress.

Storage Cost. In PMHE, the cloud server system only records the user's basic information and the model parameters used by the user, but does not record specific user data. Therefore, the storage performance of cloud servers is not high.

User data is stored in blockchain (Hyperledger Fabric's state database). In each uploaded tuple, what we need to store is only four pieces of basic user data, because the other elements are function values of the basic data. Each data consists of 8192 floating-point numbers(equivalent to *polynomial_modulus*). Assuming that the user needs to upload data 100 times each time they use the service, the total storage required is about 800KB bytes, which is quite acceptable.

6 Experiment And Evalution

The PMHE prototype has been implemented on Hyperledger Fabric and conducted comprehensive experiments to evaluate its feasibility and performance in storage and computation.

6.1 Experiment Setting

Latigo-ckks[24] is a CKKS framework implemented with GO language, which is also the preferred language for smart contract on Hyperledger Fabric development.

In the experiment, the *DELL R720* was used as the server and 8 virtual machines were built with virtualization technology. One is used as a Web application server to manage user information, receive user data, and invoke smart contracts on blockchain.The others are used to build a Hyperledger Fabric environment.

Hardware server configuration:

- CPU: E5-2697 v3 @ 2.60GHz
- Memory:256GB 1600-MHz DDR3

Virtual Machine configuration:

- OS: Centos8.0
- CPU: 4 vCPUs
- Memory: 16G,

The client has not been tested using mobile phones, but is currently implemented using laptop computers.

The configuration of laptop is as follows:

- OS: macOS Mojave 10.14.6
- CPU: 2.8 GHz Quad-core Intel Core i7
- Memory: 16GB 2133MHz DDR3

The implementation of the PMHE scheme consists of five parts: portable wearable medical device, client, cloud server, blockchain and smart contract which implements disease prediction model. The computing results of AI model are used to predict or diagnose the health status of users. Because the model implemented with CKKS executes approximate arithmetic, there is an error between the output of decryption algorithm and the real results. Therefore, the focus of the experiment is the computational efficiency of the client, the execution efficiency of the smart contract and the error between the output of decryption algorithm and the real results.

CKKS is a public key encryption system, which has all the characteristics of public key encryption system, such as public key encryption, private key decryption, etc. Therefore, the following components are needed in the program:

- Keygenerator: Generating the key
- Encryptor: Encrypting data with a public key

- Decryptor:Decrypting ciphertext with a private key
- Evaluator: Executing homomorphic evaluations

According to the design of PMHE, the first three modules are realized in the client, and the evaluator module is the AI model essentially.

CKKS requires three preset parameters: *poly_modulus_degree,coefficient_modulus*,

and *scale.*

Parameter *poly_modulus_degree* must be a number of powers of 2, such as 1024, 2048, 4096, 8192, 16384, 32768. Larger values supports to perform more complex calculations, but will increase the size of the ciphertext.After multiply operation,we must execute rescaling to manage the magnitude of plaintext[14],and the frequency of rescaling depends on the number of *coeff_modulus* parameter. In other words, it determines the number of multiplication operations that can be performed.

The experiment was carried out twice with different parameters:

Paramers1:

$$poly\_module\_degree = 8196;$$

$$coeff\_modulus = \{60, 40, 40, 60\};\ scale = 2^40$$

Paramers2:

$$poly\_module\_degree = 8196;$$

$$coeff\_modulus = \{50, 30, 30, 30, 50\};\ scale = 2^30$$

In the experiment, the experimental data is triples, each containing four elements.

Client Testing. The size of public and private key file, the length of plaintexts after encoding and the length of encrypted plaintexts are highly related to the *poly_modulus_degree* and the *coefficientt_modulus*.The larger the *poly_modulus_degree*, the higher the security is, but the time of key generation, encoding and encryption will increase. The time statistics for clients to generate key, encoding, and encryption are shown in Table 2.Table 2 shows that client operations do not add much time consumption.

Table 2
Computing time of every stage on client

Procedure	*Time(Microsecond)*	
	Paramerts1	**Paramerts2**
Generating the private key	77	204
Generating the public key	34140	41922
Generating encryptor	53	70
Generating encoder	1628	1734
Generating decoder	116	135
Encoding	26718	32295
Encryption	272171	345132
Decryption	5047	8469
Decoding	4854	15201
Total	30	30

AI Model Testing. In PMHE framework, the AI model is implemented by smart contract, and the algorithm is transformed into a polynomial that contains only addition and multiplication. Each of the polynomial is the multiplication of user data ciphertext and polynomial coefficients ciphertext .In encoding procedure, the client scales floating-point number according to scale parameter. After every multiplication, the scale of the ciphertext will double.Thus,the rescaling operation need to be executed to reduce it,and the length of the prime number used for modulus reduction is determined by *coeff_module*s parameters. The Scale should not be too small. Although a large scale will increase the computation time, it can ensure that the noise is removed correctly during the modulus reduction process without affecting the correctness of decryption.

Before each operation, we should ensure that the data participating in the operation is on the same "level". Since the ciphertext is polynomial, multiplication will lead to larger scale. Relinearize operation will be performed after the ciphertext multiplication, which will lower the "level" of the data, and then rescaling operation will be performed. The key of relinearize is generated according to CKKS algorithm in the model algorithm.The addition does not require rescaling operation, so it does not change the "level" of data. Because the "level" of data can only be lowered rather than raised, the order of calculation in model design is very important. The parameters selected in the experiment can only be multiplied twice, that is, it can achieve the fourth power at most.To pull data from different "levels" to the same "level", we can use multiplying 1.0 to pull the higher level operands to the lower "level" to achieve the cubic calculation. More complex algorithm need to adjust the parameter *coeff_modules.*The AI model running time statistics are

shown in Table 3.Table 3 show that the total computing time of invoking the AI model once on the blockchain is still relatively idea.

Table 3
Encryption time statistics

Procedure	*Time(Microsecond)*	
	Paramerts1	**Paramerts2**
Generating the secret key of relinearize operation	121565	200155
Single addition operation	10792	10987
Multiplication operation between ciphertexts	34941	49108
Multiplication operation between ciphertext and plaintext	11288	12203
Square operation of ciphertext	34339	48247
The time of relinearize operation	121497	187206
Total	282587	425543
Count the number of times	30	30

6.2 The Result and Analysis of AI Model

The core function of the smart medical system is disease prediction and health monitoring, and finally diagnosis is made according to the outputs of decryption algorithm. CKKS algorithm based on approximate arithmetic ,and noise is introduced into the operations. As a result, there is an error between final results and real value. To figure out the error size, we divided the original data into three groups, one-digit, double-digit,and three-digit. Because the number of multiplications in the AI model exceeds three times, paramters1 does not meet the calculation requirements and we select paramters2 .Each experiment was repeated fifty times. The experimental results are shown in Fig. 5. Figure 5 show that the error between the final results and the real results is very small, and the maximum error is no more than 0.02%, which can fully meet the needs of disease prediction and health monitoring.

7 Summary And Conclusion

Medical and health data are of great value both in the scientific research and medical field, such as clinical auxiliary diagnosis and health management, but they faced the risk of privacy disclosure [22]. This paper first introduces the research background and significance of medical and health data privacy protection, and then illustrates the development of blockchain technology in the privacy protection of medical data by investigating the related work world widely. Then it introduces blockchain smart contract technology and homomorphic encryption algorithm. On this basis, aiming at the privacy disclosure problems faced by medical data in the disease prediction model, this paper introduces homomorphic

encryption technology to propose blockchain-based privacy protection method of medical and health data. Based on this method ,we design and implement a privacy protection framework of smart medical data based on blockchain and homomorphic encryption, named PMHE. In the entire process of data processing, no matter network transmission, model calculation, or data storage, involveddataintheseprocedureisall ciphertext encrypted with public key. On the premise of not affecting the accuracy of calculation, PMHE realizes the security of the data on the chain, protecting the privacy of the user. In other words,PMHE truly achieves that the data is available but uncollectable.

In summary, the proposed solution can be used in following fields:

- The ciphertext results generated by the disease prediction model can be used in other health big data industries, such as health monitoring, nursing homes and medical institutions. Compared with traditional big data analysis, this greatly protects users' privacy.
- Encrypted messages can be used to exchange relevant data with healthcare providers, and ultimately provide high-quality, low-cost and safe solutions for smart medical products. The disease pattern database formed by data exchanged can be used as health big data, providing reference for disease diagnosis and contributing to social health.

PMHE is a exploration of using blockchain and privacy computing for smart medical application, there are still some problems to be further solved in the future:

- The prototype experiment results of the scheme proposed in this paper are satisfactory,but its efficiency needs to be further verified when it is used in large-scale applications with high real-time requirements.
- Because the AI model in this paper mainly operates on multiplication and addition, it is easy to implement with CKKS.However, the calculation model of many problems is more complex, and the degree of fitting polynomials is too high to exceed the “level” limit of CKKS. Therefore, the next step is not only to optimize the model design, but also to optimize the CKKS algorithm itself to improve its universality.

Declarations

Acknowledgements

None

Authors' contributions

J.Z.,W.W.,D.W. and C.M. developed the idea, protocol design, and wrote the original draft. J.Z and W.W. improved the scheme, provided useful advice, and performed the experiment. All authors have read and agreed to the published version of the manuscript.

Funding

This research is funded by Shandong Provincial Natural Science Foundation, China,grant number ZR2020MF148.Besides, This is also a part research accomplishment of the project “61972360”, which is supported by National Natural Science Foundation, China.

Availability of supporting data

The datasets generated and analyzed during the current study are available from the corresponding author on reasonable request.

Ethics Approval and Consent to participate

Not applicable

Consent for publication

Not applicable

Competing interests

The authors declare that they have no competing interests.

References

1. Zhang Y,Qiu M,Tsai C, Hassan M, Alamri A(2017) Health-CPS: healthcare cyber-physical system assisted by cloud and big data.IEEE Syst J 11(1):88-95.
2. Zhang X, Zhang J, Hang C,TANG W (2021) Verifiable statistical analysis scheme for encrypted medical data in cloud storage.Comput. Eng 47(6):3237+43.
3. She W, Chen J, Liu Q, Hu Y, Gu Z, Tian Z,Liu W (2019) New blockchain technology for medical big data security sharing.Journal of Chinese Computer System 40(7):1449-1454.
4. Sovova O (2019) Electronization in health care and privac-y protection.Journal of Sustainable Development 9(23): 72-80.
5. Price W,Cohen I (2019) Privacy in the age of medical big data.Nat. Med. 25(1)37-43.doi:10.1038/s41591-018-0272-7.
6. Wang S (2020) Research on medical data privacy protection application based on homemorphic encryption. Dissertation,ShenYang Aerospace University.
7. Huang J,Jiang Y,Li Z,Fan L (2018) Application prospect of blockchain in medical industry.J. Med. Inf. 39(2):1-8.doi:10.3969/j.issn.1673-6036.2018.02.001.
8. Niu G (2020) Research and implementation of trusted sharing platform for medical data based on blockchain. Dissertation, Harbin Institute of Technology.
9. Hylock R,Zeng X (2019) A blockchain framework for patient-centered health records and exchange (HealthChain): Evaluation and proof-of-concept study.J Med Internet Res 21(8).doi: 10.2196/13592.

10. Wang R,Yu S,Li Y,Tang Y, Zhang F (2019) Medical blockchain of privacy data sharing model based on ring Signature. J. Univ. Electron. Sci. Technol. China 48(6):886-892.
11. Liu J,Liang T,Sun R,Du X,Guizani M(2020)A privacy-preserving medical data sharing scheme based on consortium blockchain.in: GLOBECOM 2020-2020 IEEE Conference and Exhibition on Global Telecommunications.IEEE, Taipei.
12. Zhou Z,Chen Y,Li T,Ren X,Qing X (2021) Medical data security sharing scheme based on consortium blockchain.J. Appl. 39(1):123-134.doi: 10.3969/j.issn.0255-8297.2021.01.011.
13. Nakamoto S(2008) Bitcoin: A Peer-to-Peer Electronic Cash System.https://bitcoin.org/bit-coin.pdf.
14. OuYang L,Wang S,Yuan Y,Ni X,Wang F (2019) Smart contracts: architecture and research progresses.Acta Autom. Sin. 45(3):445-457.doi: 10.16383/j.aas.c180586.
15. Rivest R.L,Adleman L,Dertouzos M.L (1978) On data banks and privacy homomorphisms.Found. Secure Comput. 4(11):169–180.
16. Rivest R.L,Shamir A,Adleman L (1978) A method for obtaining digital signatures and public-key cryptosystems. Assoc. Comput. Mach. 21(2):120-126.
17. Gentry C (2009) Fully homomorphic encryption using ideal lattices.in: Proc. 41st ACM Symp. Theory Comput. (STOC), pp. 169-178.doi: https://doi.org/10.1145/1536414.1536440
18. Cheon J.H, Kim A, Kim M , Song Y (2017) Homomorphic encryption for arithmetic of approximate numbers.in: International Conference on the Theory and Application of Cryptology and Information Security,pp. 409-437.
19. Liu Y,Xia Q,Li Z,Xia H, Zhang X,Gao J (2020) Research on secure data sharing system based on blockchain. Big Data Research 6(5):92-105.
20. Zhao C, Zhao S,Zhao M,Chen Z,Gao C,Li H,Tan Y (2019) Secure multi-party computation: theory, practice and applications, "Inf. Sci.,vol.476,pp.357-372.
21. Zheng S,Liu X, Zhou T,Yang X (2021) Optimized CKKS scheme based on learning with errors problem. Journal of Computer Applications 41(6):1723-1728.dio: 10. 11772/j. issn. 1001-9081. 2020091447.
22. Chen J (2020) Research on privacy protection method of medical and health data based on blockchain .Dissertation, Zhengzhou university.
23. Xu H,Yang X,Zhang X (2021) Protection of face feature information based on fully homomorphic encryption in cloud computing environment. Guizhou Daxue Xuebao(Ziran Kexueban) 38(3):83-91.dio: 10.15958/j.cnki.gdxbzrb.2021.03.12.
24. Lattigo v2.2.0.http://github.com/ldsec/lattigo.

Figures

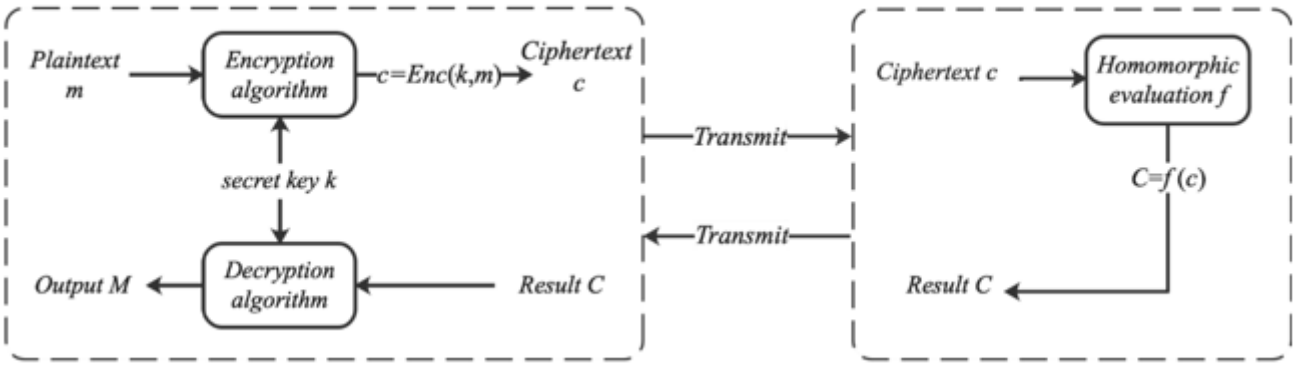

Figure 1

Privacy homomorphic encryption

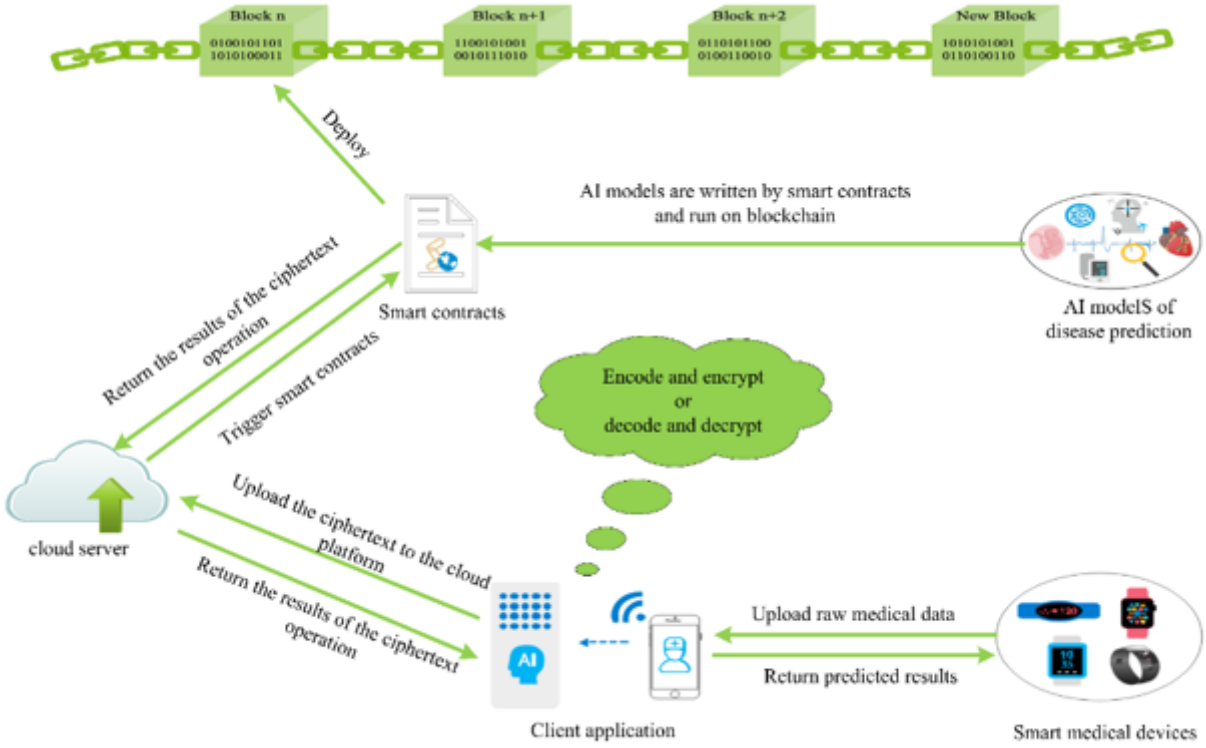

Figure 2

The architecture of PMHE system

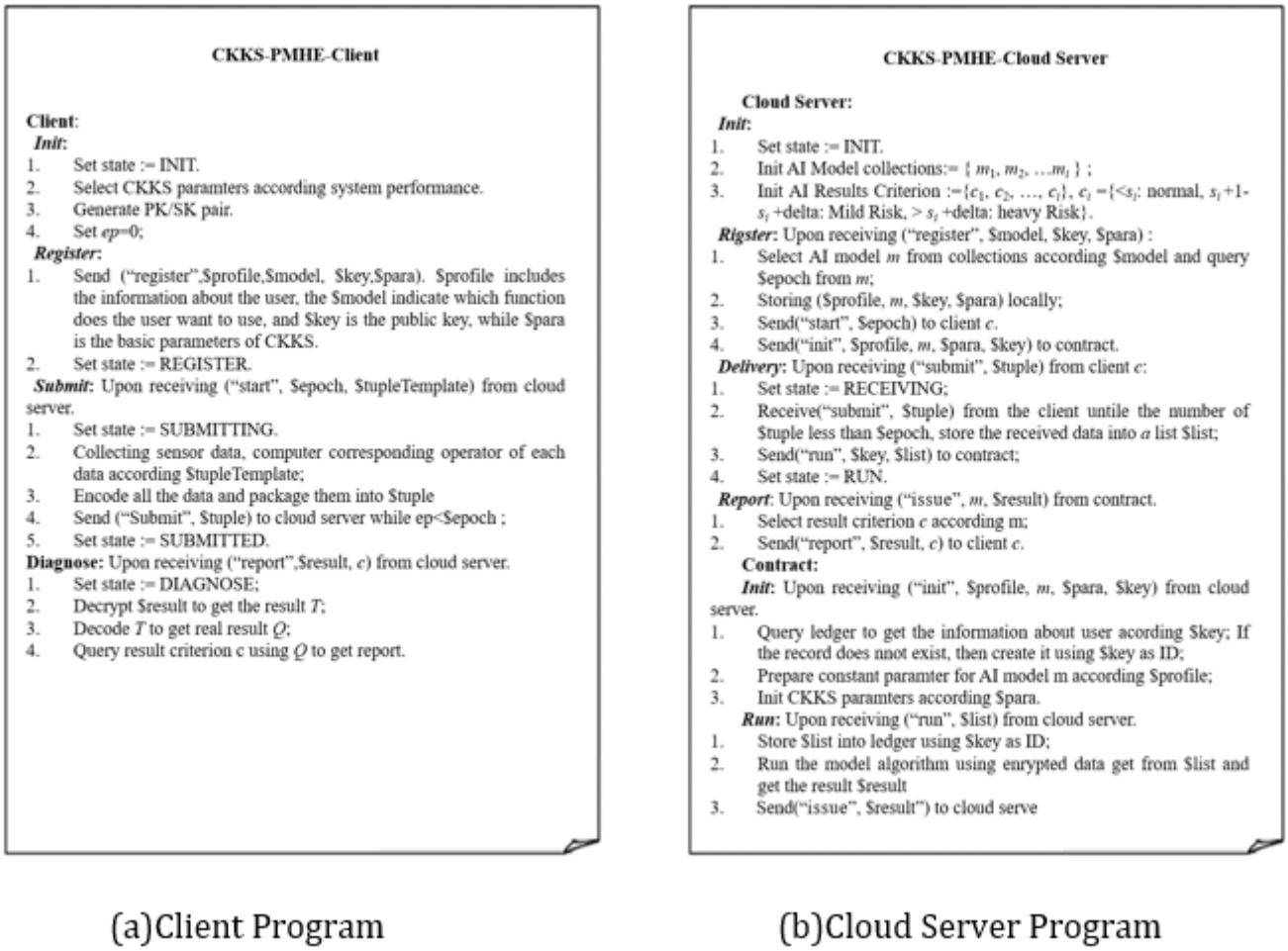

Figure 3

The program framework of PMHE with CKKS supporting

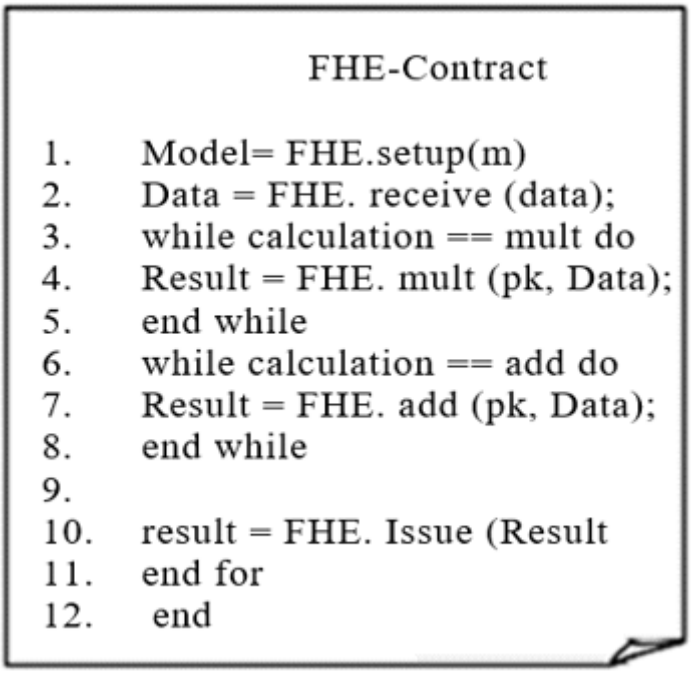

Figure 4

FHE-Contract algorithm

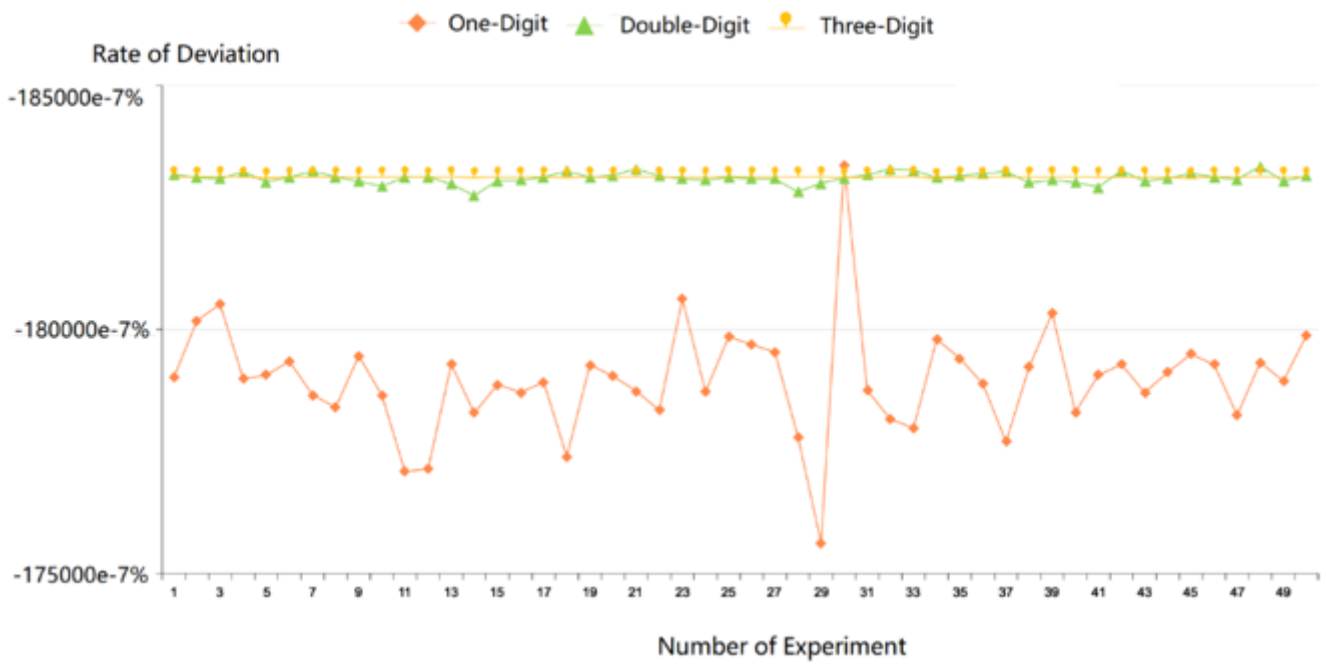

Figure 5

Variable error rate of different digits