Hindawi
Scientific Programming
Volume 2022, Article ID 4169340, 12 pages
https://doi.org/10.1155/2022/4169340

*Research Article*

# Information Sharing and Privacy Protection of Electronic Nursing Record Management System

**Qiong Li,[1] Hui Yu,[2] and Wei Li[3]**

[1]*Nursing Department, Jiangxi Health Vocational College, Nanchang 330052, China*
[2]*Quality Management Office, Jiangxi Health Vocational College, Nanchang 330052, China*
[3]*School of Mathematics and Statistics, Jiangxi Normal University, Nanchang 330022, China*

Correspondence should be addressed to Wei Li; liwei@jxnu.edu.cn

Received 23 October 2021; Revised 7 December 2021; Accepted 13 December 2021; Published 5 January 2022

Academic Editor: Ahmed Farouk

The traditional centralized storage of traditional electronic medical records (EMRs) faces problems like data leakage, data loss, and EMR misplacement. The current protection measures for patients' privacy in EMRs cannot withstand the fast-developing password cracking technologies and frequency cyberattacks. This paper intends to innovate the information sharing and privacy protection of electronic nursing records (ENRs) management system. Specifically, the signature interception technology was introduced to EMRs, the different phases of certificateless signature interception scheme were depicted, and the validation procedures of the scheme were designed. Then, the six phases of ENR information sharing protocol based on alliance blockchain were described in detail. Finally, an end-to-end memory neural network was constructed for ENR classification. The proposed management scheme was proved effective through experiments.

## 1. Introduction

With the development of medical technology, major hospitals have begun to record patients' personal health information in electronic medical records (EMRs) and connect the EMRs to the Internet. The EMRs store a lot of private information about patients' personal health, such as diagnosis and medication, and face a high risk of information leakage. Traditionally, the EMRs are stored in a centralized manner. The centralized storage makes it hard to share patients' personal health information and increases the proneness to cyberattacks. The resulting problems include data leakage, data loss, and EMR misplacement [1–3]. A series of security threats arise for EMR information. Therefore, the security of EMR usage is an urgent problem to be solved in the sharing and storage of medical information. In recent years, blockchain and cloud storage gradually enter the medical field. Many EMR storage systems no longer give patients the full control of health information [4, 5]. However, there are still some malicious behaviors in cloud servers, and the security management of EMRs in cloud storage poses an urgent problem to be solved.

Traditional EMR sharing platforms lack effective privacy protection schemes [6–8]. Xanthidis and Xanthidou [9] designed an error-correcting code hash function and constructed an anonymization algorithm for privacy protection, which effectively controls the access rights of other users, while ensuring the safe sharing of data between patients and doctors. Ma et al. [10] proposed an authentication mechanism and authorized access mechanism for the users who make access requests and effectively solved the patients' control of EMR data and the authorized access to EMR data.

EMRs need to be shared and transmitted in different formats from traditional structured data, because they contain lots of contents about the health and privacy of patients [11–13]. Responding to the classification and protection requirements of privacy-sensitive information in EMRs, Blondon and Ehrler [14] proposed a recognition and classification algorithm for medical terms that represent patient health-sensitive information in EMR texts and performed selective encryption and confidential search of the recognized words. Kim et al. [15] constructed an EMR management system based on the browser/server (B/S) architecture. The system realizes various functions: batch entry of massive medical records, multicondition query of complex EMRs, standard full-text query, and classified statistical analysis on EMRs of different years and types, providing support to the information sharing of EMRs.

The design of the consensus mechanism is the key to ensure the security of medical data in the EMR management system [16–18]. Kawser and Nyeem [19] proposed a dynamic mode Byzantine fault-tolerant (DMBFT) consensus mechanism, which applies aggregate signatures to the consensus process and optimizes the single mode of the consensus mechanism to a dynamic mode. In this way, the efficiency of signature verification is effectively improved.

The previous studies have presented solutions to the access control, storage system design, and information sharing from different angles [20–26]. However, their protection measures for patient privacy cannot cope with the fast-developing password cracking technologies and frequent cyberattacks. To solve the problems, this paper takes electronic nursing records (ENRs), which involves many people, for example, and tries to innovate the information sharing and privacy protection of ENR management system. The main contents of this research are as follows:

(1) The signature interception technology was introduced to EMRs, the different phases of certificateless signature interception scheme were depicted, and the validation procedures of the scheme were designed.

(2) The six phases of ENR information sharing protocol based on alliance blockchain were described in detail.

(3) An end-to-end memory neural network was constructed for ENR classification, which satisfies the classified protection of private information in the records. The proposed management scheme was proved effective through experiments.

## 2. Certificateless Signature Interception Scheme for ENRs

As an important part of medical big data, EMRs involve a lot of private information of patients, which should be protected according to laws. Compared with EMRs, ENRs involve a lot of people, including the responsible doctors, as well as the responsible nurses in different shifts. To conceal the sensitive parts of EMRs and protect the privacy of patients (e.g., basic information, type of disease, and state of disease), this paper applies the signature interception scheme to the information confirmation in the ENR scenario in Figure 1, laying the basis for blockchain-based ENR information sharing and security management.

*2.1. Phase Description.* Based on the certificateless public key cryptosystem, this paper designs an efficient certificateless signature interception scheme, which consists of eight phases:

Phase 1: management system initialization. Let $ST_i$ be the serial number $ST_i$ of identity authentication for patient $V_i$. The management system can be initialized in the following steps:

Step 1: the key generation center randomly selects an l-bit prime number $w$, creating a set $\{G\,w, R/G\,w, H_1, O\}$, where $G\,w$ is a finite field; $R/G\,w$ is an elliptic curve on $G\,w$; $H_1$ is the additive group; $w$ is the order; $O$ is the generator.
Step 2: randomly select $e\in\mathbb{R}^{C*}\ w$ as the primary key, and compute the public key of the system by formula $O_{SPK} = e\cdot O$.
Step 3: select five independent collision-proof hash functions $F_0$, $F_1$, $F_2$, $F_3$ and $F_4$:

$$\begin{aligned} &F0\colon \{0,1\}* \times H1 \times H1 \rightarrow C*w;\\ &F1\colon \{0,1\}* \rightarrow \{0,l\}l;\\ &F2\colon \{0,1\}* \rightarrow \{0,l\},\\ &F3\colon \{0,1\}* \times \{0,1\}* \times H1 \times H1 \rightarrow C*w;\\ &F4\colon \{0,1\}* \times \{0,1\}* \times H1 \times H1 \rightarrow C*w. \end{aligned} \tag{1}$$

Step 4: the key generation center publicizes system parameter $SP = \{G\,w, R/G\,w, H_1, O, O_{SPK}, F_0, F_1, F_2, F_3, F_4\}$, and stores it secretly to prevent anyone from illegally acquiring the master key $e$.

Phase 2: setting secret value. Select a random number $a_i\in\mathbb{R}^{C*}\ w$ as the secret value of $V_i$. Make $O_i = a_iO$ the public key of $V_i$, and transmit it to the key generation center.

Phase 3: partial generation of keys. This phase mainly includes the following two steps:

Step 1: the key generation center randomly selects $s_i\in\mathbb{R}^{C*}w$, and computes part of the public key $S_i = s_iO$
Step 2: the key generation center computes $f_0 = F_0\ (ST_i, S_i, O_i)$, and $c_i = s_i + s\cdot h_{0i}$, and secretly transmits part of the private key $C_i = (c_i, S_i)$ to patient $V_i$

Phase 4: setting private key. Upon receiving the ${}_iC_i$ from the key generation center, patient $V_i$ firstly verifies the equation $c_i\cdot O = S_i + F_0(ST_i, S_i, O_i)O_{SPK}$. If the equation holds, $V_i$ configures the entire private key $PR_i = (C_i, a_i)$. If the equation does not hold, terminate the algorithm.

Phase 5: setting public key. Patient $V_i$ configures his/her entire public key $GR_i = (S_i, O_i)$.

Phase 6: signature generation. To sign his/her name on ENR information $N = \{n_l, n_2,...,n_m\}$, patient $V_i$ needs to go through the following four steps:

Step 1: first, calculate the hash value $f_{i1} = F_1(n_i||CIA)$ of each subsegment $n_i$ ($i\in[l, nm]$) in N of the content interception and access (CIA) structure. Then, cascade $f_{i1}$ subsegments by the serial number $i$ from 1 to $m$, producing the hashed value $N' = F_2\cdot(F_1\ (n_1||CIA)\cdot F_1\ (n_2||CIA),...,F_1\ (n_m||CIA))$.
Step 2: randomly select $b_i\in\mathbb{R}^{C*}w$, and compute $B_i = b_iO$.

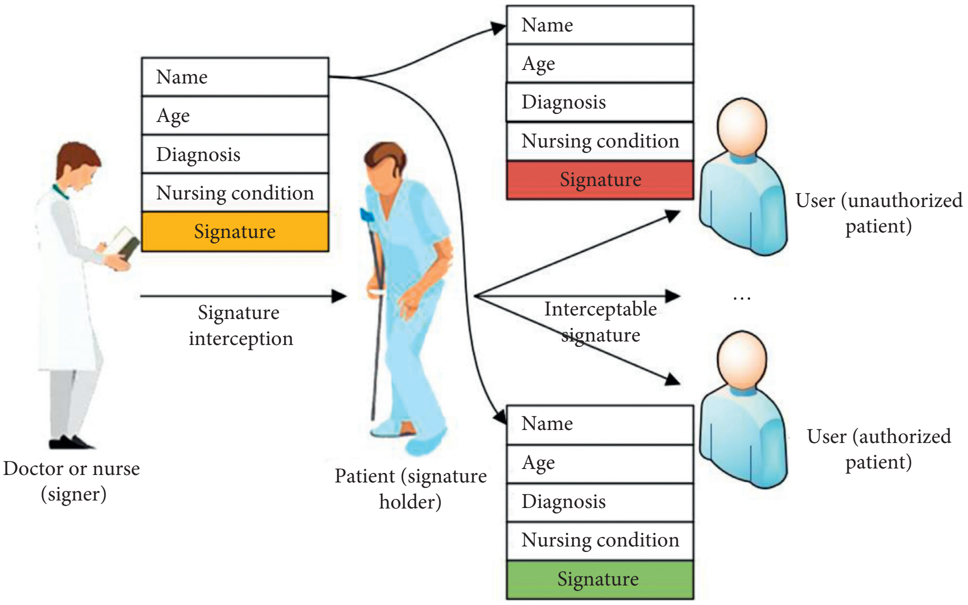

Figure 1: Application of signature interception in ENR scenario.

Step 3: compute $g_i = F_3$ $(N', ST_i, B_i, S_i)$, and $\tau_i = F_4$ $(N', ST_i, B_i, O_i)$.
Step 4: compute $\varepsilon_i = b_i - (\tau_i \cdot a_i + g_i \cdot c_i)\ mod\ w$. If $\varepsilon_i = 0$, return to Step 1; otherwise, generate the global signature $\varepsilon_G = (CIA, \varepsilon_i, B_i)$.

Phase 7: signature interception. The interceptor should intercept the global signature $\varepsilon_G$ after the signature passes the validity test. Through signature generation, compute the total hashed value $N'$, hash value $g_i = F_3$ $(N', ST_i, B_i, S_i)$, and $\tau_i = F_4(N', ST_i, B_i, O_i)$. Next, verify if $\varepsilon_i O = B_i\text{-}\tau_i\cdot O_i\text{-}g_i(S_i + F_0(ST_i, S_i, O_i)O_{SPK})$ holds. If not, terminate the operation; if yes, move on to the following operations:

Step 1: intercept subset $SUB_{CIA}(N^*)$ according to the CIA structure.
Step 2: generate the intercepted information $N^* = \{n_1^*, n_2^*, \ldots, n_m^*\}$ based on $N = \{n_1, n_2, \ldots, n_m\}$ and $SUB_{CIA}(N^*)$. For each intercepted subsegment $i \in SUB_{CIA}(N^*)$, make $n_i^* = n_i$; for each un-intercepted subsegment, replace it with $n_i^* = F_1(n_i||CIA)$.
Step 3: segment signature $\varepsilon_I = (CIA, SUB_{CIA}(N^*), \varepsilon_i, B_i)$ for $N^*$.

Phase 8: signature verification. The verifier should verify the intercepted signature $\varepsilon_I$ in the following three steps:

Step 1: judge if CIA belongs to $SUB_{CIA}(N^*)$. If not, terminate the algorithm; if yes, move on to the next operation.
Step 2: restore the total hash value $N'$ from the segmented subset $SUB_{CIA}(N^*)$ and segmented information $N^*$. If $i$ belongs to $SUB_{CIA}(N^*)$, then restore $n_i^*$ with hash value $F_1(n_i||CIA)$, where $n_i = n_i^*$; otherwise, keep the original location $n_i^*$. After that compute $N' = F_2\cdot(F_1(n_1||CIA)\cdot F_1(n_2||CIA),\ldots,F_1(n_m||CIA))$.
Step 3: calculate $g_i = F_3(N', ST_i, B_i, S_i)$ and $\tau_i = F_4(N', ST_i, B_i, O_i)$ by interceptable signature generation algorithm, and check if $\varepsilon_i O = B_i\text{-}\tau_i O_i - g_i\ (S_i + F_0(ST_i, S_i, O_i)O_{SPK})$ is valid. If yes, $\varepsilon_I$ is valid; otherwise, $\varepsilon_I$ is invalid.

*2.2. Scheme Verification.* This paper verifies the correctness of the proposed certificateless signature interception scheme. The first is to ensure the consistency between the hashed value $N'$ produced in signature generation and the value $N'$ restored in signature verification. Each subsegment of signature generation information $N$ can be replaced by

$$n_i^* = \begin{cases} n_i, & i \in \mathrm{SUB}_{\mathrm{CIA}}(N^*), \\ F_1(n_i \| \mathrm{CIA}), & i \notin \mathrm{SUB}_{\mathrm{CIA}}(N^*). \end{cases} \quad (2)$$

Each subsegment of signature verification information $N^*$ can be restored by

$$n_i^* = \begin{cases} F_1(n_i \| \mathrm{CIA}), & i \in \mathrm{SUB}_{\mathrm{CIA}}(N^*), \\ n_i^*, & i \notin \mathrm{SUB}_{\mathrm{CIA}}(N^*). \end{cases} \quad (3)$$

Formulas (2) and (3) show that the subsegment values of both $N$ and $N^*$ are $F_1(n_i||CIA)$. Therefore, signature verification and signature generation should have the same total hashed value N'.

The next is to verify the correctness of the equation. Since $g_i = F_3(N', ST_i, B_i, S_i)$, $\tau_i = F_4(N', ST_i, B_i, O_i)$, $B_i = b_i O$, $O_i = a_i O$, $S_i = s_i O$, and $O_{SPK} = eO$, the equation can be verified through the following derivation:

$$\begin{aligned}\varepsilon_i O &= [b_i - (\tau_i \cdot a_i + g_i \cdot c_i)]O \\ &= b_i \cdot O - (\tau_i \cdot a_i + g_i \cdot c_i)O \\ &= B_i - \tau_i \cdot a_i \cdot O - g_i(s_i + eF_0(\mathrm{ST}_i, S_i, O_i))O \\ &= B_i - \tau_i \cdot O_i - g_i(s_i \cdot O + F_0(\mathrm{ST}_i, S_i, O_i)e \cdot O) \\ &= B_i - \tau_i \cdot O_i - g_i(S_i + F_0(\mathrm{ST}_i, S_i, O_i)O_{\mathrm{SPK}}).\end{aligned} \tag{4}$$

The proposed certificateless signature interception scheme was proved correct through the above two steps.

## 3. Blockchain-Based Information Sharing and Privacy Protection

Figure 2 shows the structure of the ENR management system, which includes MMSAC, different types of users, cloud storage, consensus node, and blockchain ledger. Traditionally, the data sharing of ENR management system depends too much on the centralized mechanism. To solve the problem, this paper proposes an ENR information sharing protocol based on alliance blockchain. The protocol contains a total of six phases.

Phase 1: system initialization. Similar to the preceding section, the system administrator needs to initialize the system in the following steps:

Step 1: let $w$ be a large prime number. The system administrator chooses an elliptic curve on a finite field. The order formed by the points on the curve is denoted as $w$, and the additive group with the generator O is denoted as $H_1$.
Step 2: the system administrator selects $e \in \mathbb{R}^{C*}w$ as the master key MK, and computes $O_{SPK} = e \cdot O$ as the public key of the system.
Step 3: the system administrator chooses hash functions $F_0$, $F_1$, $F_2$, $F_3$, and $F_4$:

$$\begin{aligned}&F0\colon \{0, 1\}* \times H1 \times H1 \longrightarrow C * w; \\ &F1\colon \{0, 1\}* \longrightarrow \{0, l\}l; \\ &F2\colon \{0, 1\}* \longrightarrow \{0, l\}l; \\ &F3\colon \{0, 1\}* \times \{0, 1\}* \times H1 \times H1 \longrightarrow C * w; \\ &F4\colon \{0, 1\}* \times \{0, 1\}* \times H1 \times H1 \longrightarrow C * w.\end{aligned} \tag{5}$$

Step 4: the system administrator publicizes system parameter $SP = \{G\,w, R/G\,w, H_1, O, O_{SPK}, F_0, F_1, F_2, F_3, F_4\}$, and stores the master key $e$ secretly.

Phase 2: system registration. The system is registered in three steps:

Step 1: the ENR creator registers at the system administrator:

(a) The ENR creator (doctor or nurse) selects a random number $a_c \in \mathbb{R}^{C*}w$ as its secret value, computes $O_c = a_c \cdot O$, and transmits its identity $ST_c$ and part of the public key $O_c$ to the system administrator, as a preparatory work of registration.
(b) Upon receiving the $ST_c$ and $O_c$ from the ENR creator, the system administrator randomly selects $e_c \in \mathbb{R}^{C*}w$, computes $S_c = s_c \cdot O f_c = F_0(ST_i, S_i, O_i)$, and $c_i = s_i + e \cdot f_c$, and securely transmits part of the private key $CR_c = (c_c, S_c)$ to the ENR creator.
(c) The ENR creator verifies if $c_c O = S_c + F_0(ST_c, S_c, O_c)O_{SPK}$ is valid. If yes, configure the private key $PU_c = (CR_c, a_c)$ and the public key $GU_c = (S_c, O_c)$.

Step 2: the patient registers at the system administrator. The patient selects a random number $a\ v \in \mathbb{R}^{C*}w$, configures the private key $PU\ v = a\ v$, and computes the public key $GU\ v = a\ v\ O$. Then, he/she transmits his/her identity $ST\ v$ and public key $GU\ v$ to MMSAC via safe channels.
Step 3: the patient registers at MMSAC. MMSAC authenticates the identity and role of the patient and issues a real-name registration certificate to the patient $RNRC\ v = (ST\ v, GU\ v, SI_{PU})$, where $SI_{PU}$ is the signature set by MMSAC for the public key $ST\ v$ of the patient, using its own private key. Figure 3 shows the registration flow of the ENR management system.

Phase 3: ENR creation. This paper signs ENRs following the certificateless signature interception scheme. The ENR creator needs to execute the following operations:

Step 1: compute the hash values $F_1(n_i||CIA)$ of the ten subsegments $n_i(i \in [1, 11])$ of the patient (e.g., name, gender, age, contact number, identity card number, condition description, medical history, diagnosis, treatment and medication, imaging data, and nursing conditions). Then, cascade the $n_i$ subsegments by the serial number $i$ from 1 to $m$, producing the hashed value

$$N' = F2 \cdot (F1(n1\|\mathrm{CIA}) \cdot F1(n2\|\mathrm{CIA})\&F1(nm\|\mathrm{CIA})). \tag{6}$$

Step 2: randomly select $b_c \in \mathbb{R}^{C*w}$, and compute $B_c = b_c \cdot O$.
Step 3: compute $g_i = F_3(N', ST_i, B_i, S_i)$, and $\tau_i = F_4(N', ST_i, B_i, O_i)$.

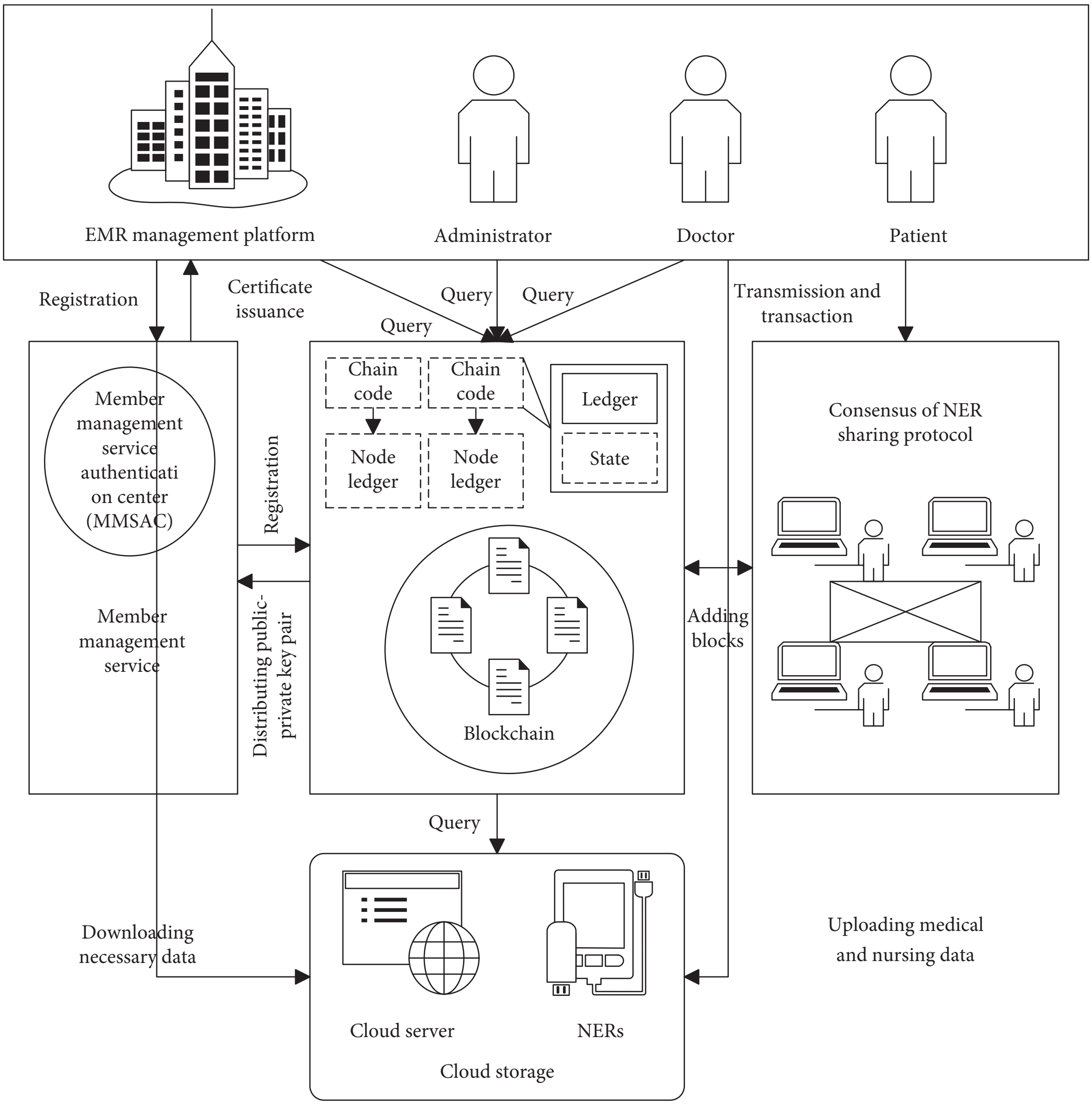
EMR management platform
Administrator
Doctor
Patient
Registration
Certificate issuance
Query
Query
Query
Transmission and transaction
Member management service authenticati on center (MMSAC)
Member management service
Registration
Distributing public-private key pair
Chain code
Chain code
Node ledger
Node ledger
Ledger
State
Blockchain
Adding blocks
Consensus of NER sharing protocol
Query
Downloading necessary data
Cloud server
NERs
Cloud storage
Uploading medical and nursing data

Figure 2: Structure of ENR management system.

Step 4: compute $\varepsilon_c = b_c - (\tau_c \cdot a_c + g_c \cdot c_c) \bmod w$. If $\varepsilon_c = 0$, return to Step 1; otherwise, generate the global signature $\varepsilon_G = (CIA, \varepsilon_c, B_c)$.

The ENR creator selects a random number $l \in \mathbb{R}^{C*w}$ as his/her symmetric key $SL_c = l$, and uses $SL_c = l$ to encrypt the original EMR N, identity information $ST_c$, hash value $f_N = F_1(n_i \| CIA)$, the global signature $\varepsilon_G$ of N, CIA, and timestamp $\tau$. Then, the patient's public key $GU_o$ is used to encrypt $SL_c$. Finally, the patient will receive ciphertexts:

$$\begin{aligned} \mathrm{CR} \longrightarrow V\colon\ \mathrm{info} = \Big\{ & R_{L_c}\big(N \| \mathrm{ST}_c \| f_N \| \varepsilon_G \| \mathrm{CIA} \| \tau\big), \\ & R_{\mathrm{GU}_o}\left(L_c\right)\Big\}. \end{aligned} \tag{7}$$

Phase 4: ENR storage. After receiving the *info* from the ENR creator, the patient decrypts the ciphertext $R_{GU}{}^{o}(L_c)$ with the private key $PU_o$ to obtain $SL_c$. Then, the patient solves EMR information N based on $SL_c$. Finally, the patient verifies the ENR signature. There are two specific steps in this phase:

Step 1: compute $f_{N*} = F_1(n_i \| CIA)$, and verify if $f_{N*}$ is consistent with $f_N$. If yes, ENR $N$ is highly secure and not tampered.

Step 2: compute $N'$, $g_c$ and $\tau_c$ through the signature generation operations in ENR creation phase, and verify if $\varepsilon_c O = B_c - \tau_c O_c - g_c(S_c + F_0(ST_c, S_c, O_c) O_{SPK})$ holds. If yes, global signature $\varepsilon_G$ is the valid signature of the recognized doctor or nurse.

If the signature fails one of the two steps, the patient will communicate with the doctor and nurse participating in nursing care. If the signature passes both steps, the patient will hide his/her sensitive

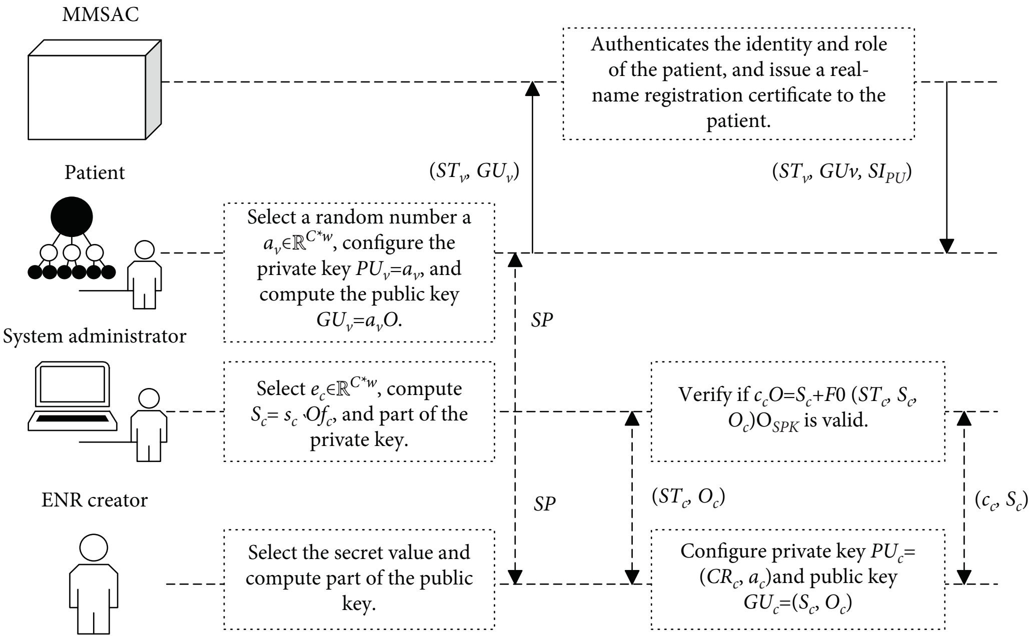
MMSAC
Authenticates the identity and role of the patient, and issue a real-name registration certificate to the patient.
Patient
$(ST_v, GU_v)$
$(ST_v, GUv, SI_{PU})$
Select a random number a $a_v \in \mathbb{R}^{C^* w}$, configure the private key $PU_v = a_v$, and compute the public key $GU_v = a_v O$.
SP
System administrator
Select $e_c \in \mathbb{R}^{C^* w}$, compute $S_c = s_c \cdot Of_c$, and part of the private key.
Verify if $c_c O = S_c + F0\ (ST_c, S_c, O_c) O_{SPK}$ is valid.
ENR creator
SP
$(ST_c, O_c)$
$(c_c, S_c)$
Select the secret value and compute part of the public key.
Configure private key $PU_c = (CR_c, a_c)$and public key $GU_c = (S_c, O_c)$

Figure 3: Registration flow of the ENR management system.

information in his/her ENR, according to his/her use needs, and the CIA structure provided by the doctor and nurse.

The huge amount of intercepted data, intercepted signatures, and hash values of ENRs are encrypted by formula (8) and then stored in the cloud:

$$\mathrm{CD} = \left(N^* \| \mathrm{ST}_c \| \mathrm{ST}_o \| f_N \| \varepsilon_G \| \mathrm{SUB}_{\mathrm{CIA}}(N^*) \| \mathrm{CIA} \| \tau\right), \tag{8}$$

where

$$f_N^* = F_1(N^* | \mathrm{ST}_o). \tag{9}$$

Figure 4 explains the creation and storage flow of ENR.

Phase 5: ENR issuance. Let CT and $\tau$ be the position and timestamp of the encrypted ENR data of the patient being stored in the cloud, respectively. The cyphertexts of CT and $\tau$ and other transaction data TD (e.g., hash values and signatures) are attached to the deployed chain code, which contains the access control list (ACL) and algebraic logic function (ALF), and the chain code is then broadcasted across the network. Let $TP_{oi}$ be the patient's alias for transaction, and let HD be the anonymous transaction certificate. The issuance process can be described by

$$V \longrightarrow T\colon \begin{cases} \mathrm{TD}_i = \langle R_{GU_{TP_{o_i}}}(\mathrm{YD}) \| F(\mathrm{YD}) \| \mathrm{SL}_i \| f_N^* \| \mathrm{HP}_{TP_{o_i}} \| \tau \rangle, \\ CC_{o_i} = \langle \mathrm{ACL}, \mathrm{ALF} \rangle, \end{cases} \tag{10}$$

where

$$\begin{aligned} \mathrm{YD} &= (\mathrm{CT} \| \tau), \\ \mathrm{SL}_i &= \mathrm{SL}_{\mathrm{PU}_{TP_{o_i}}}\left(R_{\mathrm{GU}_{TP_{o_i}}}(\mathrm{YD})\right). \end{aligned} \tag{11}$$

In the blockchain, each transaction initiated by a node carries a signature, which the node signs to verify the validity of the transaction. With the growing transaction volume, the consensus efficiency will be dragged down, if each transaction is verified one by one. To speed up transaction authentication, this paper applies the consensus algorithm in Figure 5 to consensus-making and adopts a more suitable aggregate signature scheme.

Phase 6: ENR sharing. In a channel, if another user $V$ wants to access the ENR of patient O, the access control and effective sharing of the relevant data can be realized by calling the transaction chain code deployed by consensus node for patient O. This phase requires three operations:

Step 1: the other user sends a nursing data access request AC, including the object ST, purpose VP, and visit time VT, to the management system:

$$V \rightarrow \text{All: } \mathrm{AC} = \langle \mathrm{ST}_o \| \mathrm{VP} \| \mathrm{ST}_v \| \mathrm{GU}_v \| \mathrm{HP}_v \| \tau \rangle. \tag{12}$$

Step 2: after consensus node receives the access request, the chain code $CC_o$ verifies whether the identity $ST\ g$ of the requestor exists in the ACL preset by

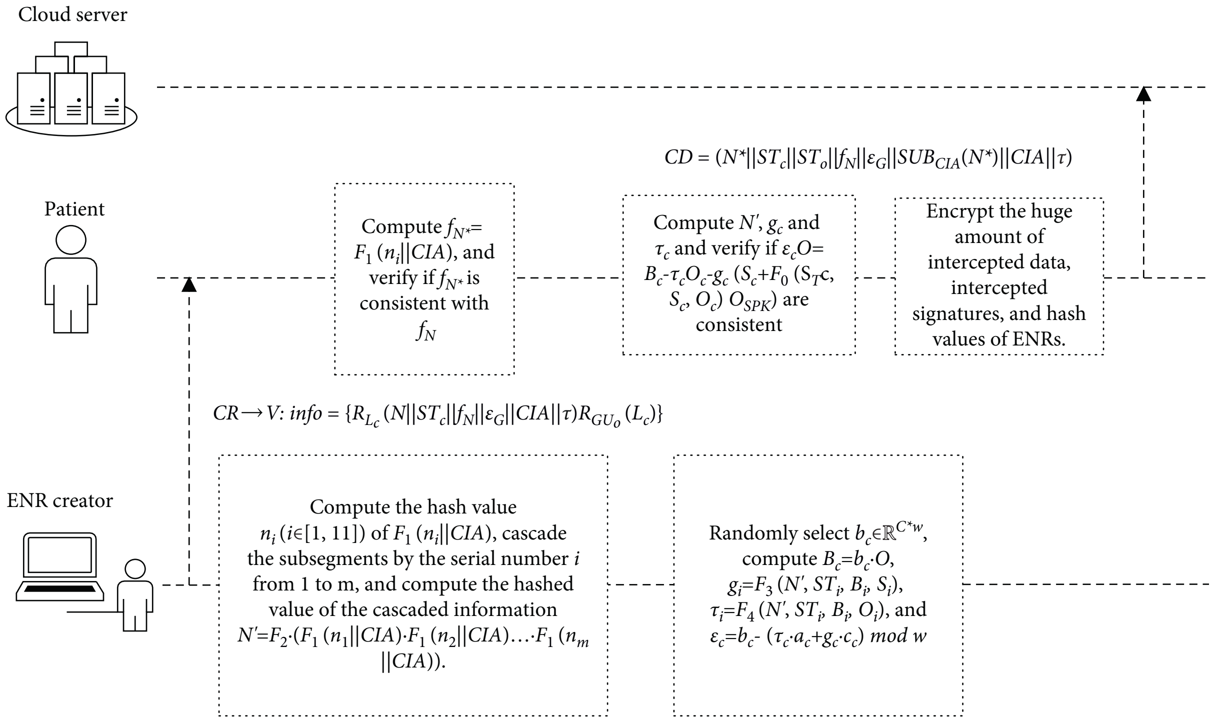
Cloud server
Patient
ENR creator
$CD = (N^*||ST_c||ST_o||f_N||\varepsilon_G||SUB_{CIA}(N^*)||CIA||\tau)$
Compute $f_{N^*}$= $F_1$ ($n_i$||$CIA$), and verify if $f_{N^*}$ is consistent with $f_N$
Compute $N'$, $g_c$ and $\tau_c$ and verify if $\varepsilon_c O$= $B_c$-$\tau_c O_c$-$g_c$ ($S_c$+$F_0$ ($S_T$c, $S_c$, $O_c$) $O_{SPK}$) are consistent
Encrypt the huge amount of intercepted data, intercepted signatures, and hash values of ENRs.
$CR \longrightarrow V$: $info = \{R_{L_c}(N||ST_c||f_N||\varepsilon_G||CIA||\tau)R_{GU_o}(L_c)\}$
Compute the hash value $n_i$ ($i$∈[1, 11]) of $F_1$ ($n_i$||$CIA$), cascade the subsegments by the serial number $i$ from 1 to m, and compute the hashed value of the cascaded information $N'$=$F_2$·($F_1$ ($n_1$||$CIA$)·$F_1$ ($n_2$||$CIA$)…·$F_1$ ($n_m$ ||$CIA$)).
Randomly select $b_c \in \mathbb{R}^{C^*w}$, compute $B_c$=$b_c$·$O$, $g_i$=$F_3$ ($N'$, $ST_i$, $B_i$, $S_i$), $\tau_i$=$F_4$ ($N'$, $ST_i$, $B_i$, $O_i$), and $\varepsilon_c$=$b_c$- ($\tau_c$·$a_c$+$g_c$·$c_c$) $mod\ w$

Figure 4: Flow of ENR creation and storage.

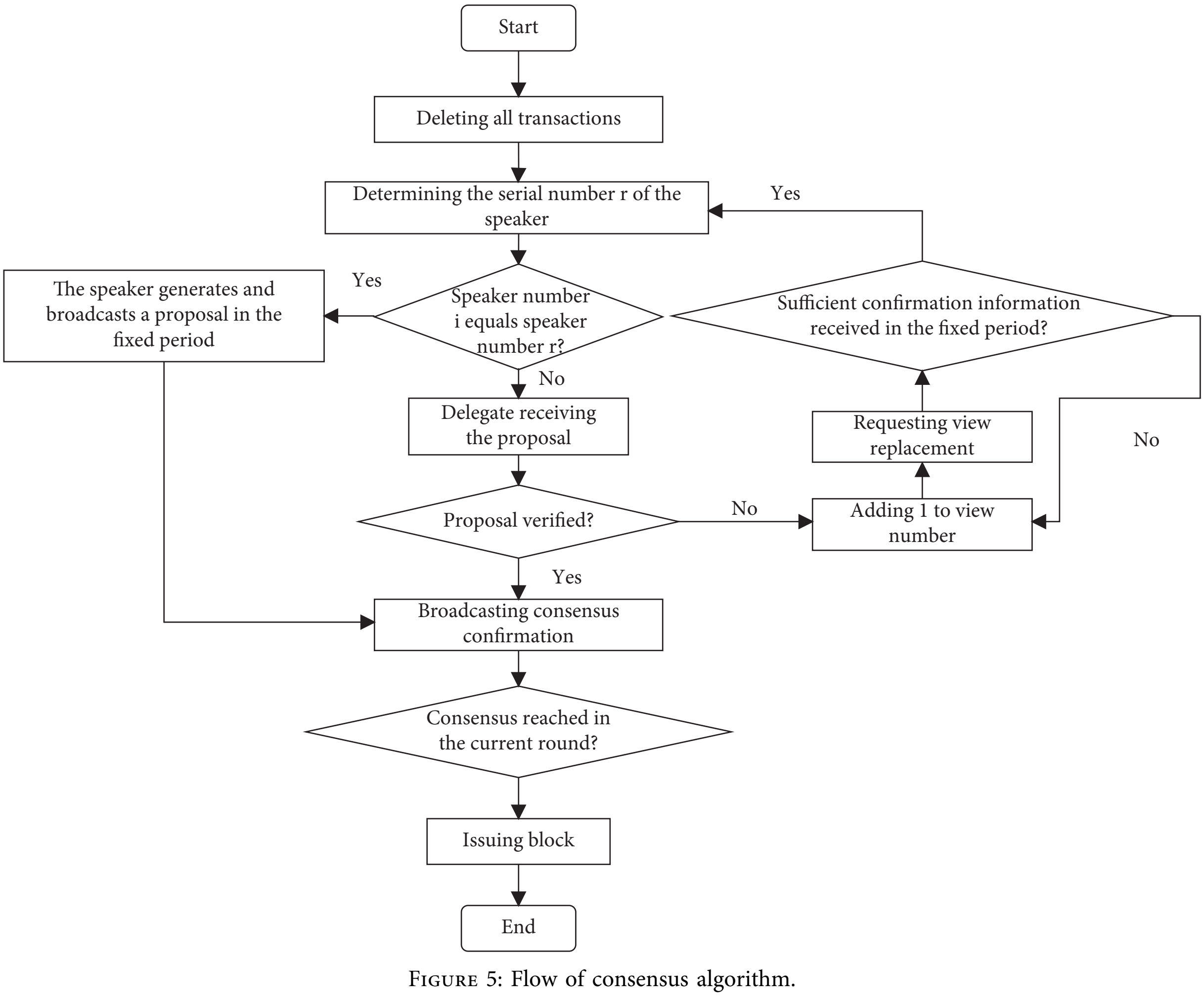
Start
Deleting all transactions
Determining the serial number r of the speaker
Yes
Speaker number i equals speaker number r?
Yes
The speaker generates and broadcasts a proposal in the fixed period
No
Delegate receiving the proposal
Sufficient confirmation information received in the fixed period?
Requesting view replacement
No
Proposal verified?
No
Adding 1 to view number
Yes
Broadcasting consensus confirmation
Consensus reached in the current round?
Issuing block
End

Figure 5: Flow of consensus algorithm.

patient $ST_o$. If not, the requestor is not authenticated by the patient. Then, $CC_o$ refuse to execute any operation and send a rejection notice to the requestor. If yes, $CC_o$ will start to execute the corresponding ALF. First, compute the storage location index CT of the shareable metadata of patient O according to his/her alias private key $PU_{TP}{}^{o}$. Then, encrypt the CT based on the public key $GU\ v$ of the requestor V. Finally, return the ciphertext (13) to the requestor $V$:

$$N = R_{\mathrm{GU}_v}\left(\mathrm{CT}\left\|f_N\right\|\tau\right). \tag{13}$$

Step 3: upon receiving the ciphertext, the requestor V decrypts the information with his/her private key, producing the storage location index CT of the ENR in the cloud, and further acquires the relevant data.

Through ENT sharing, the requestor $V$ can obtain the data object CD by inputting the storage location index CT. To judge if the EMR of patient O is complete and effective, it is necessary to verify the consistency between $f_{N*}$ and $f_N$ in CD and then examine if $f_{N*}$ equals the hash value of the intercepted EMR $N'$. Figure 6 explains the flow of ENR sharing.

## 4. ENR Classification Based on End-to-End Memory Neural Network

This paper mainly deals with the information sharing and privacy protection of ENRs. Some ENRs involve multiple reviewers and signers. If these ENRs are classified reasonably, the ENR management system will be more efficient. To this end, this paper introduces an end-to-end memory neural network and selects the MemN2N architecture for the learning model. The network can accept semistructured and nonstructured data, including medical terms and medical texts and classify ENR information through correlation analysis.

The end-to-end memory neural network receives the basic information entry $A = \{a_1, a_2, \ldots, a_m\}$ of the ENR to be classified. Passing through word vector matrices $Q$ and W, A can be transformed into an input memory unit (13) and an output memory unit (14):

$$\begin{aligned} \beta_i &= Q\phi\left(a_i\right), \\ \alpha_i &= W\phi\left(a_i\right). \end{aligned} \tag{14}$$

Let $X$ and $Y$ be the number of medical terms and the dimension of the corresponding word vectors in the entire ENR dataset, respectively. Then, $Q$ and W are $X * Y$-dimensional matrices obeying Gaussian distribution. During neural network training, the vector of each class approximates the effective representation of the medical terms in that class, along with the gradual update of gradient descent algorithm. In this process, the basic information of each ENR class being inputted can be expressed as a matrix of memory units.

For embedded representation of the ENR, a word vector matrix $P\in\mathbb{R}^{X*Y}$ was defined, which also obeys Gaussian distribution. Every medical term in the ENR was mapped into a word vector. Then, the word vectors were added up directly into a sentence vector:

$$\gamma = P\phi(t). \tag{15}$$

Based on the input memory unit $\{\beta_i\}$ of each ENR class and the embedded representation $\gamma$ of the ENR, the correlation between each ENR class and ENR can be computed by the Softmax function:

$$\omega_i = \operatorname{soft}\max\left(\gamma^T\beta_i\right). \tag{16}$$

The Softmax function can be defined as

$$\operatorname{soft}\max\left(\beta_i\right) = \frac{e^{\beta_i}}{\sum_{j\in[1,m]} e^{\beta_j}}. \tag{17}$$

The output memory unit $\{\alpha_i\}$ corresponding to each ENR class was adopted to compute the weighted embedded representation of each ENR based on $\omega_i$:

$$\xi = \sum_i \omega_i\gamma_i. \tag{18}$$

Let $E$ be the dimension of the word vector for each medical term, i.e., the dimension of the final vector for each ENR class; let $Z$ be the number of labels in the ENR sample set. To obtain the class label of the current samples, it is necessary to map the class of each sample into a $1 * Z$-dimensional vector, using the parameter matrix $K\in\mathbb{R}^{E*Z}$. The final class of ENR outputted by the network can be expressed as

$$\widehat{b} = \operatorname{soft}\max\left(K\left(\xi + \gamma\right)\right). \tag{19}$$

Let $b$ be the ground-truth label of the current ENR sample; let $b^*$ be the corresponding label outputted by the neural network. For ENR classification problem, this paper adopts binary cross entropy as the loss function of the network:

$$\mathrm{LOSS} = -\sum_{i=1}^{M} b^{(i)}\log\left(b^{*(i)}\right) + \left(1 - b^{(i)}\right)\log\left(1 - b^{*(i)}\right). \tag{20}$$

The neural network was trained by minimizing the loss. The gradient descent algorithm was adopted to update the weights and thresholds of the neural network.

## 5. Experiments and Results Analysis

After simulating different signature interception schemes, this paper records the runtime of each phase of these schemes in Figure 7. The bar graphs in Figure 7 visually compare the time consumptions of our scheme and the other three existing schemes in the phases of signature generation, signature interception, and signature verification. Our scheme had a small advantage over scheme [21] in signature generation and verification phases but achieved a marked superiority in signature interception phase and total time. Hence, the proposed certificateless signature interception scheme generally outperforms the contrastive schemes.

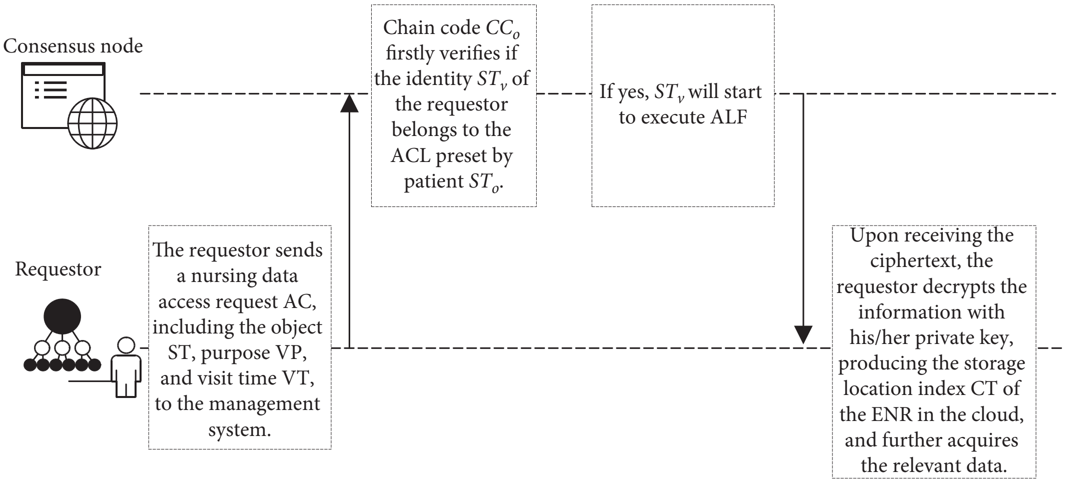
Consensus node
Chain code $CC_o$ firstly verifies if the identity $ST_v$ of the requestor belongs to the ACL preset by patient $ST_o$.
If yes, $ST_v$ will start to execute ALF
Requestor
The requestor sends a nursing data access request AC, including the object ST, purpose VP, and visit time VT, to the management system.
Upon receiving the ciphertext, the requestor decrypts the information with his/her private key, producing the storage location index CT of the ENR in the cloud, and further acquires the relevant data.

Figure 6: Flow of ENR sharing.

The throughput of a management system is generally measured by the transactions handled in each second. Figure 8 compares the time consumptions of one-by-one verification and aggregate verification. Aggregate verification consumed less than 10 s to handle 2,000 access requests. The throughput was 250–350 transactions per second. The multicenter structure of the selected alliance chain can realize the fast connection, rapid sync, and effective sharing between distributed ENR nodes, because the proposed alliance blockchain-based ENR information sharing protocol adopts the Fabric chain, which determines the node number and equipment configuration in advance. Besides, the selected consensus algorithm boasts a streamlined consensus process and a short response time. Capable of handling 5,000–10,000 transactions, the algorithm facilitates the dynamic expansion of ENR management system.

The performance of the proposed EMR information sharing scheme was compared with that of three existing information sharing schemes through comparative analysis. Scheme [21] adopts the delegated proof of stake (DPoS) consensus mechanism that alleviates the pressure on the main chain. This scheme is inferior in terms of system stability, the reliance on trustworthy third-parties, and patient control of ENR. Scheme [22] employs model chain to protect the privacy and ensure the safe storage of patient ENR information. But this scheme needs to bear some pressure of the main chain. Scheme [23] is defected in the safe storage of information. Meanwhile, our scheme effectively reduces the utilization rate of computer resources and guarantees system stability. The ENR accesses are restricted by the alliance blockchain and improved hash algorithm, laying the basis for privacy protection. Before storing the ENR, the anonymization algorithm for privacy protection is introduced to process the sensitive information in the ENR, which the patient wants to hide, thereby realizing safe storage. Table 1 compares the performance of different ENR information sharing schemes.

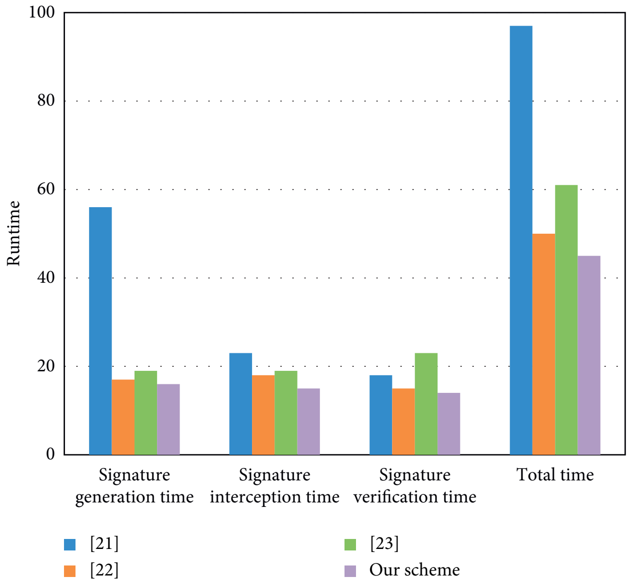

Figure 7: Runtime of each phase of different signature interception schemes.

In our ENR information sharing scheme, the confirmation time of data block transaction was set to 10 min. On the consensus-making of blocks, this paper adopts the certificateless signature interception scheme. Therefore, the consensus algorithm needs no peer-to-peer communication between nodes. As a result, fewer consensus nodes are necessary. Since the consensus is reached between the patient and the doctor/nurse, the proposed EMR information sharing scheme saved more than 5 times the time in confirming data blocks, and transmitted data with 79.45% higher efficiency than the traditional blockchain (Figure 9). With the number of blocks to be confirmed, the confirmation times of our method and traditional blockchain were both on the rise. However, our method consumed less computing power and improved system throughput, due to the control of the number of nodes.

Furthermore, the original and improved consensus algorithms were compared through experiments. The

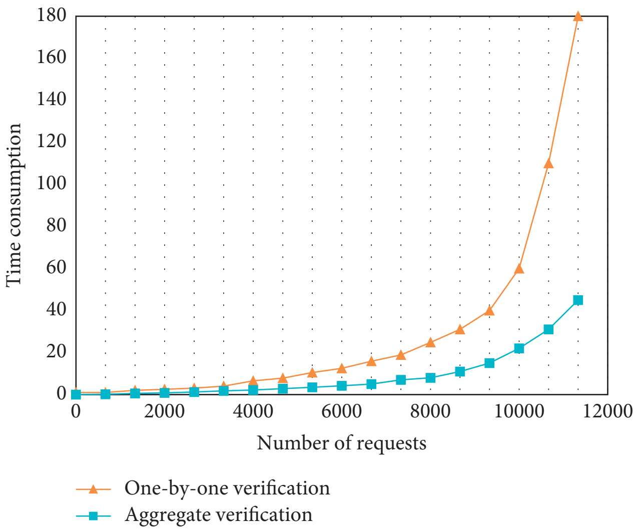

Figure 8: Time consumptions of one-by-one verification and aggregate verification.

Table 1: Performance of different ENR information sharing schemes.

| | [21] | [22] | [23] | Our scheme |
|---|---|---|---|---|
| Capable of alleviating the pressure on the main chain? | Yes | No | No | Yes |
| Number of nodes needed by the alliance blockchain | Many | Many | Many | Few |
| Relying on trustworthy third-parties? | Yes | Yes | Yes | No |
| Capable of protecting privacy? | Yes | Yes | Yes | Yes |
| Capable of safe storage? | Yes | No | Yes | Yes |
| Degree of EMR control | Incomplete control | Incomplete control | Complete control | Complete control |

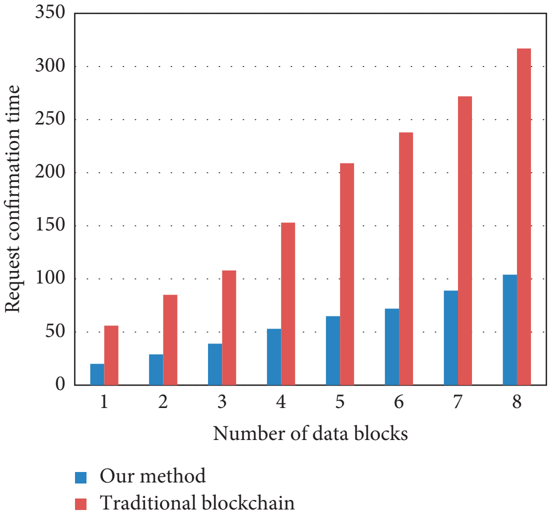

Figure 9: Comparison of request confirmation time of ENR information sharing scheme.

improved algorithm is more suitable to ENR management system. Figure 10 shows the CPU occupancies of the adopted consensus mechanism. From the CPU occupancy curves, it can be observed that, with the elapse of time, the CPU occupancy of the improved consensus algorithm was much smaller than that of the original algorithm. Hence, our consensus algorithm can respond to access requests more rapidly.

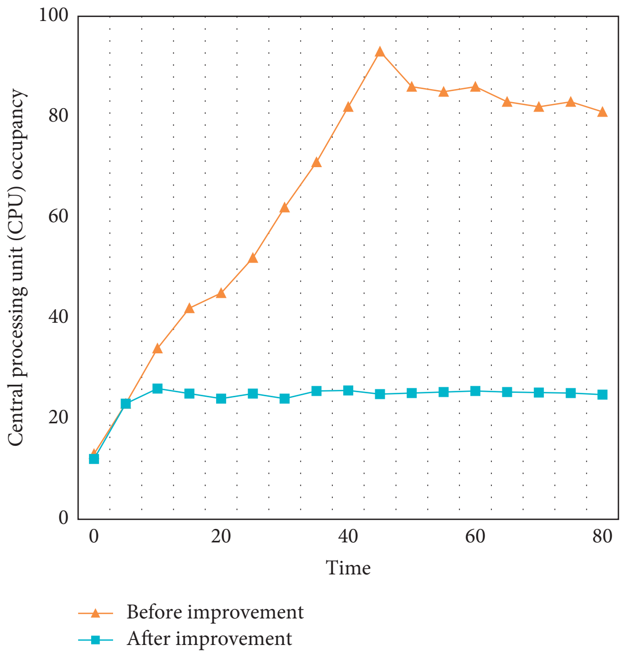

Figure 10: CPU occupancies of original and improved consensus algorithms.

## 6. Conclusions

This paper innovatively studies the information sharing and privacy protection of ENR management system. Specifically, the certificateless signature interception scheme was depicted phase by phase, and the validation procedures of the scheme were designed. Next, the six phases of ENR information sharing protocol based on alliance blockchain were described in detail. Afterwards, end-to-end memory neural network was constructed for ENR classification. The proposed management scheme was proved superior through experimental results on the runtime of each phase. Besides, the time consumption of one-by-one verification was compared with that of aggregate verification, suggesting that our consensus algorithm has a streamlined consensus process and supports the fast connection, rapid synchronization, and effectives haring between ENR nodes. In addition, our EMR information sharing scheme was compared with three existing information sharing schemes. The comparative analysis confirms the superiority of our scheme in functional completeness, computing power, and CPU occupancy.

## Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

## Conflicts of Interest

The authors declare that they have no conflicts of interest.

## References

[1] E. M. Tillman, S. L. Suppes, K. Feldman, and J. L. Goldman, "Enhancing pediatric adverse drug reaction documentation in the electronic medical record," *The Journal of Clinical Pharmacology*, vol. 61, no. 2, pp. 181–186, 2021.

[2] S. Chabbi, R. Boudour, and F. Semchedine, "A secure cloud password and secure authentication protocol for electronic NFC payment between ATM and smartphone," *Ingénierie des Systèmes d'Information*, vol. 25, no. 2, pp. 139–152, 2020.

[3] K. Li, G. Zhang, N. Li, and H. Yang, "A novel public information system for mobile geriatric medical services," *Revue d'Intelligence Artificielle*, vol. 33, no. 3, pp. 197–202, 2019.

[4] S. Hashemi and F. Burstein, "A framework for managing cognitive load in electronic medical record systems training," in *Proceedings of the Twenty fifth Americas Conference on Information Systems*, Cancún, Mexico, August 2019.

[5] M. Z. Ahmed and C. Mahesh, "A weight based labeled classifier using machine learning technique for classification of medical data," *Revue d'Intelligence Artificielle*, vol. 35, no. 1, pp. 39–46, 2021.

[6] M. Kushima, T. Yamazaki, and K. Araki, "Text data mining of the nursing care life log from electronic medical record," *Lecture Notes in Engineering and Computer Science*, vol. 2239, pp. 257–261, 2019.

[7] Y. Zhao, M. Cui, L. Zheng et al., "Research on electronic medical record access control based on blockchain," *International Journal of Distributed Sensor Networks*, vol. 15, no. 11, 2019.

[8] N. Masana and G. M. Muriithi, "Adoption of an integrated cloud-based electronic medical record system at public healthcare facilities in Free-State, South Africa," in *Proceedings of the 2019 Conference on Information Communications Technology and Society*, Durban, South Africa, March 2019.

[9] D. Xanthidis and O. K. Xanthidou, "A proposed framework for developing an electronic medical record system," *Journal of Global Information Management*, vol. 29, no. 4, pp. 78–92, 2021.

[10] Q. S. Ma, X. X. Cen, J. Y. Yuan, and X. M. Hou, "Word embedding bootstrapped deep active learning method to information extraction on Chinese electronic medical record," *Journal of Shanghai Jiaotong University*, vol. 26, no. 4, pp. 494–502, 2021.

[11] A. Sarkar and M. Sarkar, "Tree parity machine guided patients' privileged based secure sharing of electronic medical record: cybersecurity for telehealth during COVID-19," *Multimedia Tools and Applications*, vol. 80, no. 14, Article ID 21899, 2021.

[12] R. V. Deolekar and S. B. Wankhade, "A study of electronic health record to unfold its significance for medical reforms," *Advances in Intelligent Systems and Computing*, vol. 1200, pp. 113–123, 2021.

[13] G. Bingham, E. Tong, S. Poole, P. Ross, and M. Dooley, "A longitudinal time and motion study quantifying how implementation of an electronic medical record influences hospital nurses' care delivery," *International Journal of Medical Informatics*, vol. 153, Article ID 104537, 2021.

[14] K. Blondon and F. Ehrler, "Integrating patient-generated health data in an electronic medical record: stakeholders' perspectives," *Studies in Health Technology and Informatics*, vol. 275, pp. 12–16, 2020.

[15] D. H. Kim, J. E. Lee, Y. G. Kim et al., "High-throughput algorithm for discovering new drug indications by utilizing

large-scale electronic medical record data," *Clinical Pharmacology & Therapeutics*, vol. 108, no. 6, pp. 1299–1307, 2020.

[16] M. Naeem and I. Alqasimi, "Unfolding and addressing the issues of electronic medical record implementation," *Information Resources Management Journal*, vol. 33, no. 3, pp. 59–80, 2020.

[17] H. Ma, R. Zhang, G. Yang, Z. Song, K. He, and Y. Xiao, "Efficient fine-grained data sharing mechanism for electronic medical record systems with mobile devices," *IEEE Transactions on Dependable and Secure Computing*, vol. 17, no. 5, pp. 1026–1038, 2020.

[18] M. G. Kathi and J. H. Shaik, "An approach of detecting the age of a human by extracting the face parts and applying the hierarchical methods," *Traitement du Signal*, vol. 38, no. 3, pp. 681–688, 2021.

[19] M. A. Kawser and H. Nyeem, "High fidelity embedding of electronic patient record in medical images," in *Proceedings of the 2020 IEEE Region Tenth Symposium*, pp. 1844–1847, Dhaka, Bangladesh, June 2020.

[20] J. Austin, M. Barras, and C. Sullivan, "Interventions designed to improve the safety and quality of therapeutic anticoagulation in an inpatient electronic medical record," *International Journal of Medical Informatics*, vol. 135, Article ID 104066, 2020.

[21] T. Galluzzi, M. Ridao, and S. Esteban, "Strategy for the analysis and visualization of electronic medical record data for public hospitals in the city of Buenos Aires," *Studies in Health Technology and Informatics*, vol. 270, pp. 1397-1398, 2020.

[22] M. Volpi, S. Esteban, and S. Terrasa, "Safety and drugs: how do we record medication consumption and prescription in electronic medical records? A look on aspirin," *Digital Personalized Health and Medicine*, vol. 270, pp. 1383-1384, 2020.

[23] R. Madhusudhan and C. S. Nayak, "An improved user authentication scheme for electronic medical record systems," *Multimedia Tools and Applications*, vol. 79, no. 29-30, Article ID 22007, 2020.

[24] N. Flores, M. Enteria, M. Pefianco, and M. N. Young, "Electronic medical record database with accessible online summary and statistics," in *Proceedings of the 2020 The Sixth International Conference on Industrial and Business Engineerin*, pp. 86–90, Macau Macao, China, September 2020.

[25] S. Li, "A decision model for bike sharing based on big data analysis," *Journal Européen des Systèmes Automatisés*, vol. 53, no. 2, pp. 283–288, 2020.

[26] P. Guttikonda and N. Mundukur, "Secret sharing with reduced share size and data integrity," *Ingénierie des Systèmes d'Information*, vol. 25, no. 2, pp. 227–237, 2020.