Array 14 (2022) 100150

Contents lists available at ScienceDirect

Array

journal homepage: www.sciencedirect.com/journal/array

Blockchain based context-aware CP-ABE schema for Internet of Medical Things security

Boubakeur Annane [a], Adel Alti [a,b,*], Abderrahim Lakehal [a]

[a] Department of Computer Science, Faculty of Sciences, Ferhat Abbas Sétif-1 University, LRSD Laboratory, P.O. 19000, Sétif, Algeria
[b] Department of Management Information Systems & Production Management, College of Business & Economics, Qassim University, P.O. 6633, Buraidah, 51452, Saudi Arabia

ARTICLE INFO

Keywords:
COVID-19
Healthcare
Authentication
Privacy
Blockchain
IoMT

ABSTRACT

Nowadays, the number of corona patients is increasing significantly. The relationship between the Internet of Medical Things (IoMT) and the Internet is struggling to keep up with this number of patients. The transmission of Patient Health Records (PHR) to the care of a patient through Internet plays an important role in the remote monitoring and fast detection of new contaminated patient with coronavirus. Moreover, it has generated significant security and privacy concerns for the global health care system due to tampering of control messages. This paper focuses on the application of blockchain and smart contract mechanisms to solve the shortcomings of the current health application and propose a new security schema based on context-aware CP-ABE. The proposed schema includes context-aware policies to achieve a robust authentication of identity and confidentiality of patient's healthcare data. Therefore, the proposed schema shows promising results in enhancing security and minimizing encryption time in Fog cloud environments based on proxy-fog and reinforcement of security policies.

1. Introduction

Nowadays, COVID-19 has spread rapidly from its original apparition in Wuhan, China. With the virus's rapid spread, there is an urgent need for both frontline healthcare personnel and ordinary individuals to take precautions and restrict the disease. In parallel with the rapid development of science and technology, the Internet covers all parts of the world and provides humans with various and efficient health services. Therefore, remote diagnosis and early detection of coronavirus have become one of the main issues of healthcare domain in today's society.

Taking COVID-19 in China as an example, the number of infected people has achieved 2.5 million in September 2019. As the number of infected humans with the virus is continuously increasing, the relationship between Internet of Medical Things (IoMT) and Internet is necessary to keep up with new infected patients. The transmission of Patient Health Records (PHR) to the care of a patient through Internet plays an important role in the remote monitoring and detection of new contaminated patient with coronavirus. It generated significant security and privacy concerns for the global health care system due to tampering of control messages.

In e-health systems, there are lot of health data in which physics need to diagnose different critical patient's situation in order to complete the healthcare process. The transfer of patients to a new hospital or clinic, their healthcare data should be also made available for use, which is becoming more and more necessary until it leads to untenable situations that may converge towards a complete blockage of the healthcare process. The Cloud plays a key role in the storage of unlimited medical information of patients and convenient transmission of sensitive data across different stockholders. Whereas, the data is gathered by the medical things (IoMT) and transmitted to Cloud for analyzing by various healthcare experts such as physicians, radiologists, and specialists. While the medical data are stored on the cloud, the latter can be exchanged across different cloud resources decision-making. However, an e-health system-based Cloud may raise several security challenges such as confidentially, privacy of patient data. Also, there are many problems facing Cloud-based systems like overhead communicate security problems in reason of network access misuse using hackers access nodes. Meantime, blockchain can be represented as a portion of the implementation layer of a distributed e-health system. By using blockchain, the integrity of the data in distributed e-health systems can be accomplished and maintained [1].

The blockchain is one of the most hyped technologies that appear in

* Corresponding author. Department of Computer Science, Faculty of Sciences, Ferhat Abbas Sétif-1 University, LRSD Laboratory, P.O. 19000, Sétif, Algeria.
E-mail addresses: baker11@live.fr (B. Annane), a.alti@qu.edu.sa (A. Alti), lakehal.abderrahim@gmail.com (A. Lakehal).

https://doi.org/10.1016/j.array.2022.100150
Received 24 November 2021; Received in revised form 19 February 2022; Accepted 1 April 2022
Available online 7 April 2022

the last few years and it makes a real revolution in the financial sector. In addition, it started to include different fields like healthcare, supply chain, and many fields. Blockchain technology enables to provide cryptographically validated transactions and data, which are not under the control of any third-party organization [2]. In general, blockchain technology has a key advantage of decentralization, persistency, anonymity, and audibility. With these features, it can save costs greatly and develop efficiency [3]. In this work, we will apply blockchain technology and cryptography techniques to ensure security and privacy of healthcare data without needing a third party to control it. The application of blockchain enables the hospitals or clinics to access a specific patient's healthcare data that is needed. This solves the problem of collecting health data from different locations. In addition, it solves the problem of delay in obtaining the required healthcare data so that it can be accessed directly by exchanging the public key. Another reason is to protect healthcare data from loss or fraud because the blockchain and cryptography techniques provide a high level of privacy. This leads to enable the physics to access healthcare data of their patients securely. In addition, cryptography guarantees a high degree of privacy to protect healthcare data from loss or modification by illegitimate entities.

In this paper, we propose a new approach tackling certain security concerns in the Cloud such as patient data authenticity and confidentiality with less processing execution time. The motivation behind proposing new security solution is to control the security aspects of decentralized health data access and keeping patient's health data safe against the most standard attacks in eHealth applications. The contribution of this work is to find an efficient model for eHealth applications. The model is based on decentralized Mobile-Fog-Cloud architecture, IoMT, cryptography, and Blockchain for health data. The main contributions of this work are:

- Firstly, applying a public key (one-to-many) encryption technique for securing cloud storage and data sharing among a group of physicians. The authentication is performed by a remote Proxy/Fog, which is a part of the Cloud through blockchain and context-aware attributes based CP-ABE encryption. It receives the user's authentication request, then starts the authentication process and monitors the control access rules.
- Secondly, combining cryptography techniques and Blockchain technology for reinforcing the management of decentralized access control and a high level of anonymity offered by blockchain and context-aware security policies.
- Thirdly, providing the security analysis of proposed scheme with AVISPA[1] simulator.

The paper is organized as follows. Detailed related work is represented in Section 2. Section 3 gives an overview of the ontology model. The proposed schema in Section 4. Implementation details and experimental results are given in Section 5. The conclusion and some perspectives are illustrated in Section 6.

2. Related works

Over the past several decades, there have been many research works on blockchain technology on Cloud mobile services. They have been proposed to preserve the confidentiality and privacy of distributed application tasks on mobile devices, Fog, or Cloud to ensure the application security requirements. However, Blockchain is a distributed and secure decentralized transaction that has emerged as a platform on mobile devices, Fog, and Cloud applications. As well as application in the Cloud uses Blockchain technology to protect users' information. The existing literature has proposed the conceptual underpinnings of Fog and mobile Cloud computing [4].

Zou et al. discussed the benefits and challenges of securing the mobile devices, Fog, and Cloud layers in a hierarchical model [5] without examining in detail their impact on distributed IoMT applications and their security. To the best of our knowledge, none of the existing approaches can provide a decentralized approach to secure and manage a service-based application through user devices to minimize attackers' efficiency. Thus, confidentiality, integrity, and access control of stored data are among the major challenges raised by an external storage.

For that reason, a new authentication technique based-secure communication in the mobile Cloud has been proposed by Jegadeesan et al. [6] to protect the control access of mobile users to the Cloud services. The technique is based on mutual verification between users and Cloud providers where both sides need to provide their legitimacy to each other. Due to the limited storage capacity of mobile devices, mobile users are not able to store the huge details of Cloud services anonymously. Therefore, the technique exchanges only session keys once the successful authentication of mobile users to Cloud services occurs which decreases the computational cost. The technique uses a third party known as Trusted Third Party (TTP) to send private keys and public keys for both users and service providers to ensure registration and the authentication phases. The legitimacy of both components is checked via the hashing and cryptographic methods. This approach does not incorporate environmental attributes.

Ensuring health data confidentiality and privacy is considered as a major objective to protect the processing data within services on edge servers. Hou et al. [7] proposed a data security-enhanced Fine-Grained Access Control mechanism (FGAC) to ensure data security during data access to mobile edge computing. The scheme assigns roles based on the credibility of user groups and further verifies users based on attributes matching to achieve fine-grained protection of data by reducing the risk of internal attacks. However, there is still a limitation for access attributes explosion constraint to provide precise and consistent access control. Aftab et al. proposed [8] a hybrid Role and Attribute-Based Access Control (RBAC) by implementing least privileges. The access decision in RABAC is based on the notion of roles and attributes. Although, RBAC makes the policy administration easy and well audit with some limitations. However, it also has one main weakness (*e.g. explosion of roles and attributes*), it is inefficient for fine-grained policy specifications, which leads to a large number of attributes required to accomplish fine-grained authorization. Moreover, RABAC does not support for situations where the contextual attributes are considered while making access decisions. For example, an access control policy may depend on the user's time of day or current location when the access is requested. Singh et al. [10] presented a comprehensive literature review of the security problems that affect the implementation of Blockchain in sustainable smart cities. Incorporating the Blockchain and artificial intelligence in the smart society concept opens new security suggestions such as the protection of privacy. Moreover, encryption methods are not sufficient to ensure the protection of security and privacy of the nodes, like hash functions necessitate an improvement by using intelligent search techniques and algorithms. However, it remains a limitation for role explosion problem to provide fine-grained access control.

Several recent works have integrated the Blockchain [9–17] to secure the healthcare application but to our best knowledge, none of them are focusing on protecting the distributed services by adopting Blockchain with hybrid cryptography methods where the services are considered as main components in Cloud computing and any successful attacks occur to them may lead to retrieve users' sensitive data. Reffad et al. [15] have proposed a new proxy to optimize the composition of Cloud services provided by different Cloud providers. However, the main limitation of the proposed proxy is not detecting the malicious communication that occurs between the different services deployed in different services providers. The proposed work for detecting malicious services communication in the Fog based on integrated Blockchain is an

[1] AVISPA: A formal security verification tool for the automatic authentication of cryptographic protocols and applications.

improvement of this work in which detects attacks between health services while deployed on the Cloud.

Many other works [21–23] have applied blockchain technology and Neural Networks to ensure secure access control in digital healthcare system. For instance, Ali et al. [21] ensures a secure search and keywords-based access to the database using neural network with homomorphic encryption and blockchain technology. The work provides more security and less computational cost, which was characterized by a homomorphic encryption method and neural network. Another approach has applied deep learning and blockchain to process IoT data in health field [22] giving a prediction rate of 99%. Furthermore, Ben Daoud [23] has applied a secure and intelligent method for IoT-Fog Environments that persist network attacks.

In this work, we propose a new manner to achieve robust authentication and optimal confidentiality by utilizing proxy/fog computing with the assistance of IoMT, secure policies, and blockchain. This could help in securing the transfer of health data and offer efficient and secure authentication for users.

3. Preliminaries

This section presents the basic foundations of the proposed method. The need for the security PHR is presented also. The details of Access Policy and Attribute-Based Encryption (ABE) are demonstrated and significant policies are described.

3.1. *Security of personal health record (PHR)*

The Personal Healthcare Record (PHR) is an electronic, lifelong resource of health information that is needed by individuals to make health decisions. An individual owns and manages the information of the PHR, which comes from healthcare providers. The PHR must be maintained securely, while the individuals determining policies for access control. The Cloud enabled health data to be deployed easily, inadvertent or malicious disclosure of data that contains Personally Identical Information (PII) to unauthorized individuals or organizations may have catastrophic consequences. Thus, healthcare providers must comply with security policies when they release sensitive medical data. The security policies must be carefully updated and enforced while patient health status changes. Ensure data security is considering the first step towards compliance.

3.2. *Attribute-Based Encryption (ABE)*

Attribute-Based Encryption (ABE) is a recent approach that uses Public-Key (PK) cryptography [**3; 15**]. It can be flexible for systems with large-scale applications that use one-to-many encryption messages based on attributes such as roles and context. ABE is becoming functional encryption and Identity-Based Encryption (IBE) in cryptography. The access control must respect a set of policies that are defined over a set of attribute values (Ciphertext-Policy ABE: CP-ABE). The ABE security model is based on the following phases:

- Phase 1: The challenger executes the configuration algorithm and gives the PK to the opponent. The adversary creates repeated Private Keys (PV) corresponding to the sets of attributes $a_1 \ldots a_n$.
- Phase 2: phase 1 is repeated with the restriction that none of the attributes sets $a_{n+1} \ldots a_n$ satisfy the access structure corresponding to the challenge.

3.3. *Context-awareness and attribute-based access control*

A system is context-aware if it uses context to provide relevant information and/or services to the user, where relevancy depends on the user's task [19]. We notice that context-awareness can be based on two important mechanisms: the ability to monitor contextual information and the ability to exploit and react to environmental changes. To improve the efficiency of the control process, attribute-based access control is being used, with the goal of applying and integrating contextual data to detect authorized users of cloud resources. More specifically, To address the role explosion problem and provide exact results, the proposed scheme leverages features of the contexts at the session for role activation, where users may be assigned to one or more roles and only one role may be active.

3.4. *Blockchain*

Blockchain has been known as a distributed ledger type (data structure) that has information about transactions or events. Moreover, blockchain can create a decentralized environment, which does not allow the transactions and data to be under the control of any third-party organization. This technology enables sharing and replicating the information between the participants in the network. In addition, the completed transaction is usually recorded using an immutable ledger.

3.5. *Cryptography*

With the increased use of public communication networks, security and privacy have become major concern in healthcare. Cryptography is the practice and study of secure communications techniques. Encrypting health information is the essential strategy in cryptography when it comes to patient history details. In recent years, a large number of encryption algorithms have been proposed, but the majority of these algorithms have high computational overhead and are no longer sufficient to recent attacks. Thus, we need to propose robust low-cost encryption-decryption schemes for IoMT. The next section will focus on our proposal in context-aware attributes based access control, IoMT and blockchain technology in health system.

3.6. *Hash functions*

A cryptographic hash functions is one-way procedure that designed to protect the integrity of data and generate unique outputs from any fixed-length input. The proposed blockchain based context-aware policies is developed using hash functions.

4. Secure IoMT based on context-aware crypto schema and blockchain

4.1. *System architecture*

In this research work, we use a blockchain technology and a context-aware attribute based encryption to design a secure eHealth system. The system uses blockchain technology to store healthcare data from medical sensors to physics. It includes physics, patients, a cloud service provider for data storage, the hospital fog server, which serves as the registration authority for a hospital. The proposed architecture of the system consists of 8 components, which are shown in Fig. 1 and described below.

- **Patient**: includes different types of biomedical information and medical sensors that are used to monitor the vital signs of a patient. He defines the access policies and encrypts his/her data under the policies before uploading them on the Cloud.
- **Medical Sensors**: are responsible for the data generation and sending it to Proxy/Fog in real-time in a secure manner using Cx-ABC encryption after the authentication process and exchange of secret keys. Some examples of sensors include blood oxygen saturation sensor, blood-pressure sensor, and body temperature sensor.
- **Fog Server (Registration Authority):** Each hospital has its registration authority. These are used to register both users and doctors. If the verification is successful, fog server will generate a random

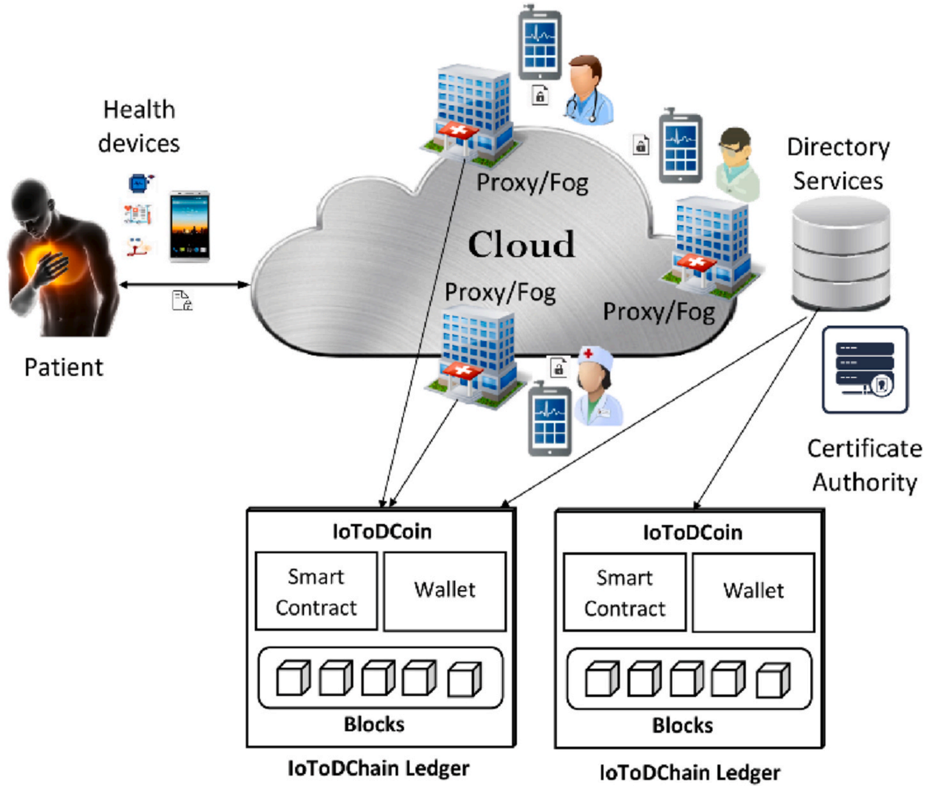

Fig. 1. System general architecture.

number and determine the session key that will be used for future authentication.

- **Proxy/Fog**: is the healthcare provider such as hospitals, laboratories, and clinics, which are linked with physicians or nurses. They can take care of a relatively large number of patients.
- **Cloud**: is defined as a network of different healthcare services that are connected by sending and receiving packets. It stores medical patient's data and executes intensive tasks.
- **Blockchain:** plays the role of decentralized trust part between provider/consumer of sensitive health data or both. It is used to ensure access control management while ensuring data integrity and traceability of transactions conducted across an unsecured network.
- **Attribute Manager (AM):** generating the group key for the users in each group. In addition, AM is responsible for re-encrypting ciphertext under different context changes.
- **Certificate Authority (CA):** allows managing all attributes and generates them, according to the identity of the users, the set of key pairs and grants them access privileges to end-users by providing them with their secret keys according to their attributes.
- **Directory Users:** this allows users (doctors, nurses, caregivers) to consume the data. They request access to data according to their attributes from cloud servers. Only users with required attributes and satisfying access policies can decrypt the data. Doctors can also add diagnostics and suggestions to share with peers.

Firstly, all patients, medical sensors, and physics need to register with the blockchain to obtain public and private keys for data encryption/decryption. Secondly, when the patient's sensors want to send the monitored data through the proxy/Fog. The transmitted data record will be encrypted with the private key and sent to the proxy/Fog, added permissions, and downloads their metadata. The proxy/Fog will verify the signature of the patient's sensors and generate blockchain data, and then the proxy/Fog will notify the physics, inform the availability date and time. Finally, when the physics wants to access health data,.The proxy/Fog will send the signed and encrypted message containing the transaction number (see Fig. 2).

4.2. Proposed schema

Let $\mathbb{G}_0$ and $\mathbb{G}_1$ be two bilinear groups of prime order p, g is a generator point of $\mathbb{G}_0$ and e is a bilinear map defined by: $\mathbb{G}_0 \times \mathbb{G}_0 \rightarrow \mathbb{G}_1.r$. The details of all the notations are mentioned in Table 1. The Cx-CP-ABE schema extends CP-ABE schemas by adding Fog/Proxy component to the existing components and contextual access attributes. The proposed schema is divided into five phases (see Fig. 3). The first phase is the attribution of certificates to physics and patients. The second phase is the generation of master keys and public keys to physics and patients. The patient authentication and data encryption are realized in the third phase. While, the last phase is the authorization phase, where the user authorizes physics to access their data.

4.2.1. Smart contract initialization

Blockchain technology was applied in the proposed architecture. We have developed key information that is stored in the blockchain in the proposed smart contract. The smart contract includes fields of ID (the account identity), transaction detail, certificate, and timestamp. This information is highly encrypted and can only be accessed with the authorization of the data owner, thereby ensuring data security and personal privacy using the following two main transactions:

- *GenerateAuthorization*$(ID, S,\ \mathrm{Gr},\ \ \mathrm{Cloud})$ is executed by the Proxy/Fog to generate authorization for a group of physics *Gr* to access data with identifier *ID* and the corresponding encrypted data set *S*, which is stored in the Cloud. The latter is chosen as $\sum_{1}^{m} s_i id_i$ where id_i is the identifier of the i^{th} metadata in which the service's context of the patient is matched. We noticed the continuous updates of ID according to the evolution of patient states.

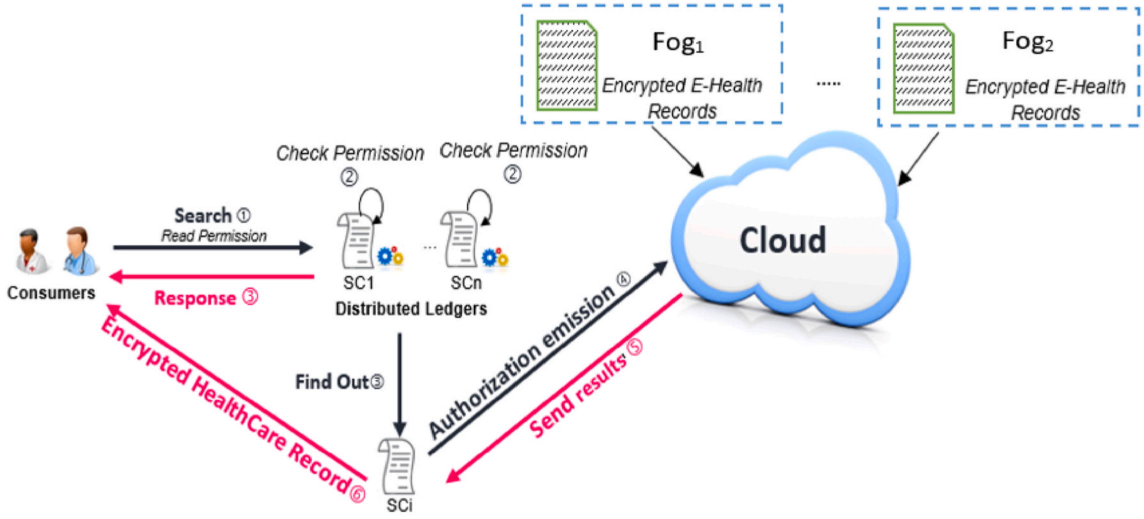

Fig. 2. Physicians health sensitive data access.

Table 1
Used notations.

Notation	Description
PK_d	User/IoMT device public key
SK_d	User/IoMT device secret key
PK_p	Physics public key
SK_p	Physics secret key
Id_u	Identity of user/device
Id_p	Identity of physics
PK_f	Proxy/Fog public key
SK_f	Proxy/Fog private key
MK	Master key
M	A sensed data (message)
CT	Encrypted data (text encrypted by Cx-CP-ABE).
C_i	components of encrypted data.
D_i	components of secret key.
G_0	A first bilinear group
G_1	Asecond bilinear group
g	Generator point (512-bit prime)
p	A large prime number (144-bit)
e	Bilinear mapping: $G_0 \times G_0 \rightarrow G_1.r$
α and β	Random numbers

- *RequestAuthorization* (*permission*, *Gr*, *@req*) is used to load authorization within the Blockchain from a provider account to the consumer's account. The requests use their @req address and send a request to the storage Cloud provider. The cloud sends this request to the Fog/Proxy. The consumer obtains authorization to access the provider's data.

4.2.2. *Certification and registration phase*

All IoMT, patients, and physics need to register with a certificate authority (CA) to obtain digital certificates via a secure channel. The participant's role can represent the medical IoMT, patients, and physics (*nurse, doctor, and specialist*). Each certificate contains public and private keys for message signing. Fig. 4 shows the flowchart of the certification and registration phase.

Step 1: The sender S (IoMT device or physics) generates an identity ID_s, and sends it with a set of context attributes CxA_s to the Attributes Authority (AA).
Step 2: The Attributes Authority (AA) generates a master key (MK) and public key (PK_s) based on the identity of sender ID_s and CxA_s and then transmit them to the Fog/Proxy. The n MK is only known to the context-aware attribute-based access control system, for that reason, it is used to generate each participant's secret keys.

Step 3: The public key PK_s is distributed to each participant for encrypting their data. The secret key may be used later for decrypting ciphertext that have an access policy satisfied by the contextual attributes CxA.

```
Algorithm 1. Registration function of Smart contract of the proposed schema
function insert_new_device (string id, string info, string cert)
{
  index ++;
  tab [index].id = id;
  tab [index]. info = info;
  tab [index]. cert = cert;
}
return tab_keypairs;
```

4.2.3. *IoMT device's authentication and encryption phase*

In the proposed scheme, the system must first verify the identities of the patient's sensors through the certificate authority at the beginning of the monitoring process. The patient's sensors can further use the public key to encrypt monitored data before transmission. It uses the Fog/Proxy public key PK_{Fog} and generate its secret key PV_D. Fig. 5 shows the authentication process and Algorithm 2 shows the encryption process.

The patient setup the context-based access policy (T) and his IoMT device encrypts the monitored health data (M) by the algorithm $Encrypt(M, T, PK_{Fog})$ via the Fog/proxy public key PK_{Fog} and sending the ciphertext (CT) to the Fog/proxy. The ciphertext (CT) is stored on the blockchain for data sharing. The Fog/Proxy broadcasts the transaction *GenerateAuthorization* to authorize a group of physics to access the patient's data in the cloud. Then it will iterate until all context attributes of the tree leaves have been treated.

```
Algorithm 2. $Encrypt(M, T, PK_{Fog}, \mathrm{P}_1)$
IF Check_Access_Policy ($\mathrm{P}_1$, T) Then
Begin
$s \leftarrow \mathbb{Z}_p$
$C_1 \leftarrow g^s$
$C_2 \leftarrow M \oplus (e(H_1(id), g)^{\alpha}, e(H_2(id), g)^{\beta})^{s}$
$C_i \leftarrow (H_2(i). \prod_{i=1}^{n} x_i)^s$
$CT \leftarrow [C_1; C_2; C_i]$
End;
Return $CT$
```

4.2.4. *Physics authentication and authorization for data access phase*

When a physics receives permission to access ciphertext (CT) from

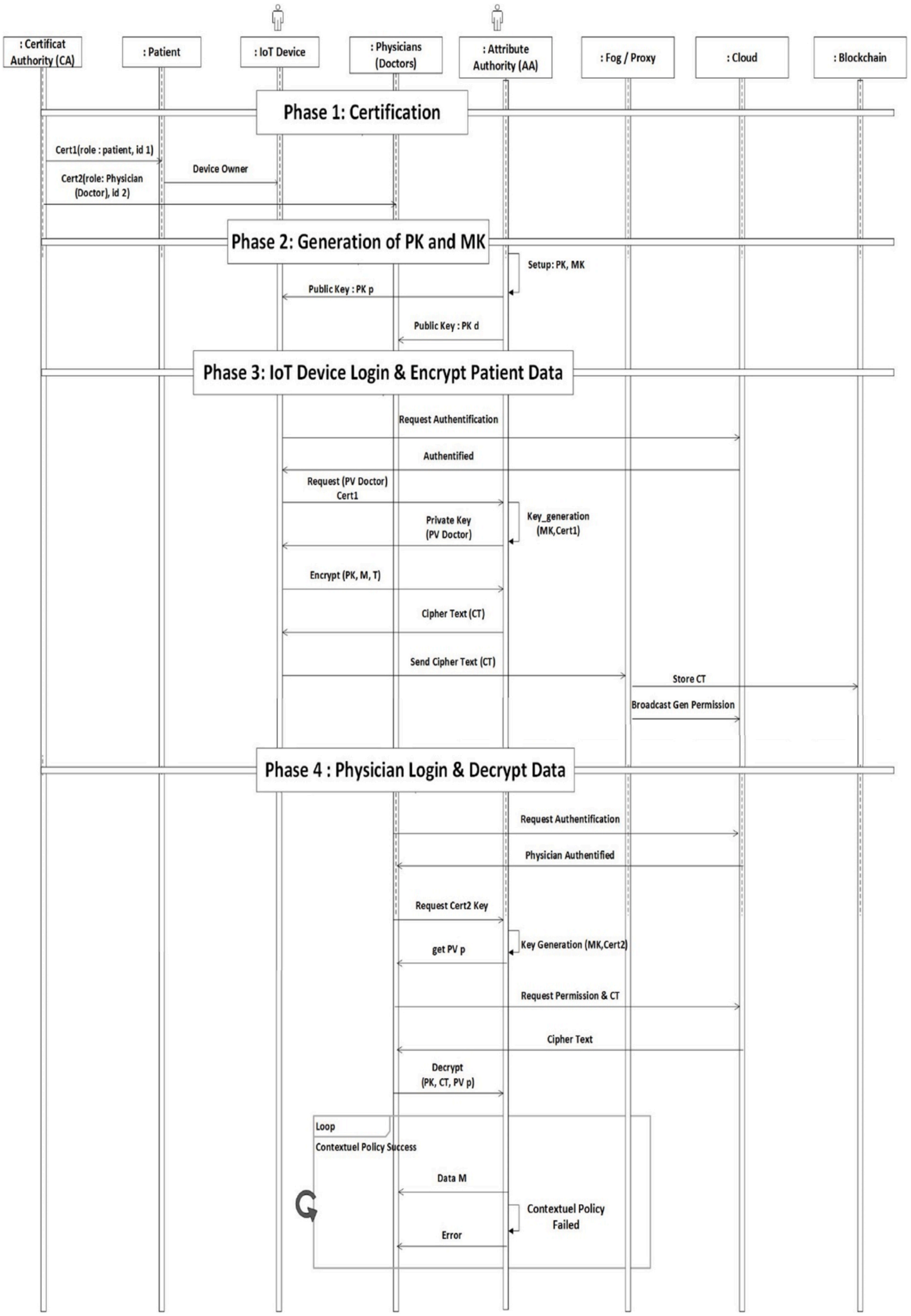

Fig. 3. The UML sequence diagram of our architecture.

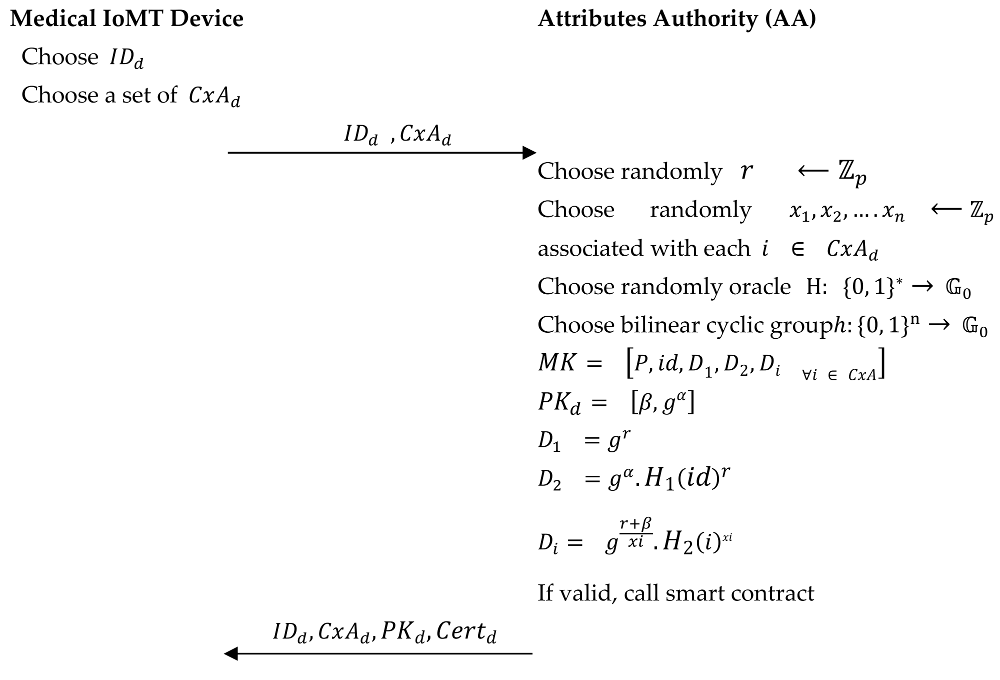
Medical IoMT Device
Attributes Authority (AA)
Choose ID_d
Choose a set of CxA_d
ID_d , CxA_d
Choose randomly $r \longleftarrow \mathbb{Z}_p$
Choose randomly $x_1, x_2, \ldots . x_n \longleftarrow \mathbb{Z}_p$
associated with each $i \in CxA_d$
Choose randomly oracle H: $\{0,1\}^* \rightarrow \mathbb{G}_0$
Choose bilinear cyclic group$h$: $\{0,1\}^n \rightarrow \mathbb{G}_0$
$MK = [P, id, D_1, D_2, D_i \ _{\forall i \in CxA}]$
$PK_d = [\beta, g^\alpha]$
$D_1 = g^r$
$D_2 = g^\alpha . H_1(id)^r$
$D_i = g^{\frac{r+\beta}{xi}} . H_2(i)^{xi}$
If valid, call smart contract
$ID_d, CxA_d, PK_d, Cert_d$

Fig. 4. The certification and registration process.

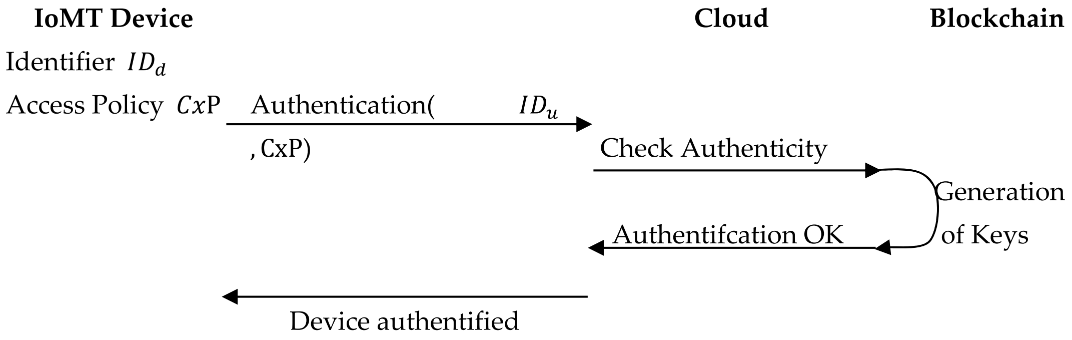

Fig. 5. The authentication process.

the blockchain. First of all, he authenticates to the Cloud with his certificate which defines his context attributes. Therefore, the Cloud with Directory Users (*DU*) has descriptions of all users' attributes involved in the health application. Then, the Cloud sends the ciphertext of the patient stored in the blockchain. A physics receives the ciphertext and decrypted it using the *Decrypt* algorithm with his private key Cx-CP-ABE PV_p. If physics's secret key has satisfied the ciphertext policy (T), the health data (M) is returned; otherwise, the decryption failed with error. The Cloud notifies the Fog/Proxy about the access status of physics.

Algorithm 3. *Encrypt*(M, T, PV_p, P)

```
IF Check_Access_Policy ($PV_p$, P) Then
Begin
$s \leftarrow \mathbb{Z}_p$
$C_i \leftarrow (H_2(i). \prod_{i=1}^{n} x_i)^s$

$M \leftarrow \frac{C_1 . e(D_1, C_i)}{e(D, C_2)}$
return $M$
End
Else return false;
```

5. Case study and security analysis

This section provides the performance analysis of the proposed scheme. It introduces the simulator tool that we used in order to get the security results in terms of stability, encryption time, and execution time.

5.1. Case study: access control for Patient's health information

In this section, context-aware CP-ABE scheme is illustrated through several scenarios of a hospital database placed on fog computing to protect PHR against unauthorized access. In the hospital, there are several numbers of practitioners with its departments such as the patient, the physics, the nurse, and many others. If we want to achieve context-aware access control, we need to include the user's context attributes (*e.g., role, activity, specialty, etc.*) and the environment's context attributes (*e.g., department, resources, etc.*) in the control access policy to overcome the role explosion problem. Patients are interested in securing access control that is represented by contextual constraints while publishing health records.

First Scenario. The patient is equipped with wearable devices (*glucose meter, temperature sensor, and smartwatch*). He wants to protect his/her published health data using a context-aware access control policy. The system allows this patient to contact its nearest fog node, register himself or herself on certificate authority on joining the hospital and specify the access control policy to their health status, its location, and different context attributes. This policy can be defined as follows:

(role = *'physics'*) **AND** (location = *'hospital'*) **AND** (Health_Speciality = *'cardiology'*) **AND** (Action = *'r/w'*)

This policy is reinforced by context-aware attributes to match the environment context (*e.g., cardiology department*) and the resource-department (*e.g., resources of cardiology department*) as follows:

(role = *'physics'*) **AND** (location = *'hospital'*) **AND** (Health_Speciality = *'cardiology'*) **AND** (Action = '*r/w*') **AND** (department = 'cardiology') **AND** (resource-department = 'cardiology')

When the patient sends his health data encrypted with the respective public key to Fog/proxy node, he will receive it and in turn, send it to Cloud server to access the data. The physics can read/write the medical records of those patients who belong only to his department.

Second Scenario. When a patient wants to delegate his right access to another physics specialty from another hospital, a notification is sent to the proxy/Fog component and the access policy is dynamically updated. Of course, his access policy will be updated to include environmental attributes (*e.g.*, orthopedic department, resource-department = 'orthopedic'). The updated policy is defined as follows:

(role = *'physics'*) **AND** (location = *'hospital'*) **AND** (Health_Speciality = 'orthopedic) **AND** (Action = '*r/w*') **AND** (department = 'orthopedic') **AND** (resource-department = 'orthopedic')

Using context-aware CP-ABE, the new encrypted PHR can be decrypted only by the physics of the orthopedic department that he can find useful in his working domain. All this while he can always check the state of his health (*e.g.*, if it is orthopedic problem, then deploy vitamin D service).

5.2. Secuirty analysis

AVISPA is a formal security verification technique for the automatic authentication of cryptographic protocols and applications [18]. AVISPA simulator will be used to analyze security for the patient and proxy/fog registration and phases of the proposed schema. Through AVISPA, the symmetrical schema demonstrates that it is secure. The security model is specified and proved [20] as follows:

We suppose an attacker $\mathscr{A}$ with a significant advantage $\text{Adv}_{\mathscr{A}} = \mathscr{E}$ tries to enter the system using false credentials and broke semantic security of the session key in authentication schema. An attacker $\mathscr{A}$ selects randomly a set of attributes to generate the access control policy $\mathscr{P}^{*}$ and then send it to the adversary $\mathscr{B}$. The adversary $\mathscr{B}$ runs *Setup* algorithm to generate the public key and then send it to. $\mathscr{A}$.

Phase 1. In this phase, the attacker $\mathscr{A}$ answers private key queries. He can adaptively submit set S_i to $\mathscr{B}$ where S_i does not satisfy $\mathscr{P}^{*}$ and $\mathscr{B}$ responds with the secret key $\mathscr{SK}^{*}$ corresponding to the submitted set S_i. The attacker $\mathscr{A}$ sends two messages m_0 and m_1 of same size to the simulator. The simulator chooses a β value. It creates $C_2 = M_1 .(e(H_1(id), g)^{\alpha}, e(H_2(id), g)^{\beta})^{s}$ and $C_1 = g^{s}$. It will also choose random $x_1, x_2, \dots . x_n \in \mathbb{Z}_p$ and generate the ciphertext components C_i
Phase 2. The adversary $\mathscr{A}$ will eventually output $\beta^{'}$ of β. The simulator then outputs zero if $\beta = \beta^{'}$; otherwise, it outputs one if $\beta \neq \beta_0$. Finally, the Advantage of $\mathscr{B}$ is as follows:

$$\text{Adv}_{\mathscr{B}} = \frac{1}{2}[Pr\{\beta^{'} = \beta \ / \beta = 1\}] + \frac{1}{2}[Pr\{\beta^{'} = \beta \ / \beta = 0\}] - \frac{1}{2} = \frac{\mathscr{E}}{2} = \frac{1}{2} + \text{Adv}_{\mathscr{A}}$$

Consequently, as $\text{Adv}_{\mathscr{A}} = \mathscr{E}$ is assumed not to be negligible, $\text{Adv}_{\mathscr{B}} = \frac{\mathscr{E}}{2}$ is also with not negligible advantage.

5.3. Performance evluation

As previously mentioned, we propose the application of context-aware CP-ABE in the access control for patient's health Information. Then, we aim to evaluate our proposal by the application of a set of classifiers on a real dataset based on two different metrics: stability and total execution time. All experiments have been performed on a PC with Intel Core i5 2.67 GHz, with 4 GB of RAM, 250 GB hard disk and window 7 (64 bits) using Eclipse java platform and BSWABE [17] java library.

To evaluate the context-aware CP-ABE, we use a data set that contains a total of 13 access policies and 32 attributes (*e.g. glucose level, heart beating, blood pressure, hypertension, user's state, user's age, weakness, articular pain, headache, physician's grade, physician's grade, department name, department resources, etc.*). The attributes set is classified into different groups based on the type of disease (*diabetic, heart, nerves, hyperthyroidism, blood pressure*) and permits the context-aware access control process to be simulated. The number of access control policies and health attributes is varied in each execution. Thus, we can simulate the scalability and execution time experiments for a different number of attributes.

5.3.1. Scalability evaluation

The stability metric indicates the impact of the number of attributes in the access policy on the encryption time. Fig. 6 illustrates the encryption time of the proposed context-aware CP-ABE algorithm versus the number of attributes ranging from 2 to 10. The results of the experiments reveal that the encryption time of context-aware CP-ABE algorithm remains stable versus number of attributes in IoMT-cloud scenarios. This is due to the use of limited and relevant sensitive information policy (*i.e. user's role, user's location and time, relevant health information such as glucose level and weight*) needed for control access.

5.3.2. Execution time evalaution

For performance comparison, we mainly rely on the total execution time, which represents the required time to encrypt/decrypt the messages according to the number of attributes in the access policy. Fig. 7 shows execution time comparison between the proposed context-aware CP-ABE algorithm (Cx-CP-ABE) and the original CP-ABE.

The obtained result shows that the proposed method requires a small execution time for both encryption and decryption operations compared to original CP-ABE. This is due to both encryption and decryption algorithms are based on relevant sensitive attributes that are used to reduce significantly the access policy checking time.

5.3.3. Computionnal time comparaison

To compare the execution time, four approaches are evaluated which some existing works HealthFog [4], Role-based ABAC model [8] and blockchain-based electronic healthcare record system for healthcare application [14] and the proposed approach. The results of the evaluation results are presented in Fig. 8. The comparison shows that proposed schema has low execution time than other two schemas [8,14]. This is due to context sensitive data access and federated blockchain based on local fog servers and distant server's machine.

5.3.4. Public-private key space analysis

The proposed scheme uses context-aware CP-ABE algorithm, which involves two real random numbers as its initial conditions, and a 140-bit initial seed for the smart contract initialization. The generation of keys is called 3 times for one iteration of the encryption algorithm, which needs 3 sets of keys {D_1, D_2, D_i}. Considering the precision of D_1, D_2, D_i is 10−10 that generates a space of 1536. Hence, the key-space becomes 140 + 1536 = 2389. Which is greater than the current standard of 256 bit and large enough to defy any brute force or advanced attacks.

The proposed Cx-CP-ABE algorithm on the attributes set of health domain achieves promising performance results when compared to the original CP-ABE as shown in Figs. 6–8. However, the Cx-CP-ABE

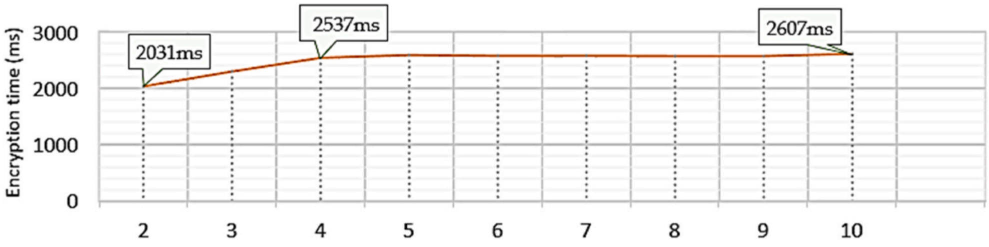

Fig. 6. Encryption time versus numbers of sensitive attributes.

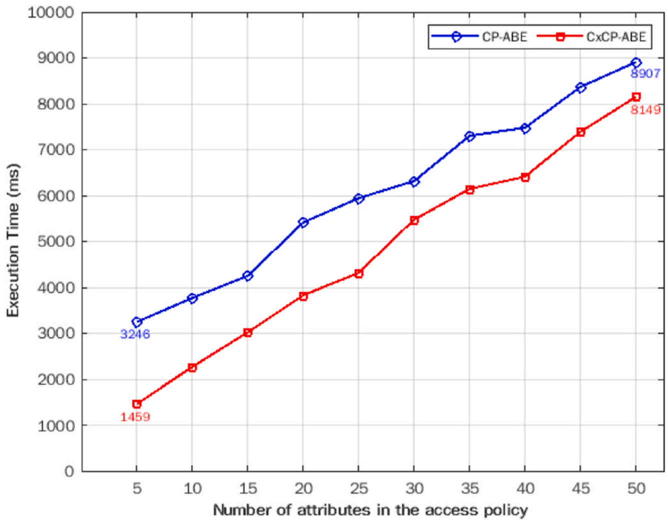

Fig. 7. Execution time comparison between the original CP-ABE and CxCP-ABE.

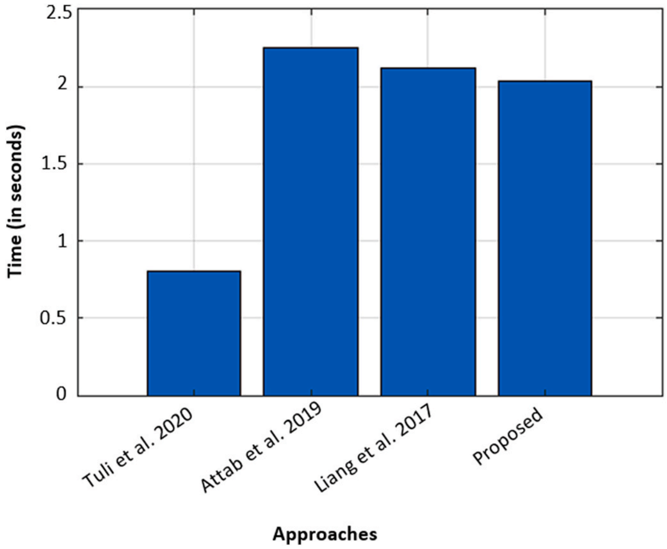

Fig. 8. Computational time comparison between the proposed schema and other existing works [4,8,14].

algorithm is much better than the original CP-ABE in checking and reducing access policy attributes in terms of sensitivity, stability, and total execution time.

5.4. *Advantages and limits of our schema*

5.4.1. *Advantages*

- Because of 154 bits prime number, it returns a diversity of keys in the generation phase.
- The schema achieved optimal performance and it is secure since the combination of Blockchain and Cx-CP-ABE close the unauthorized access.
- The schema is more efficient than the original ABE in terms of execution time.
- AVISPA tool demonstrates that the schema is protected from unsolicited and intrigue attacks.

5.4.2. *Limitations*

- As the number of users grows as well as the communications traffic between, this might affect the algorithm's execution time.
- Hard to predict all possible behavior of attackers which implies the use of machine learning.

6. Conclusion

In this paper, we presented the IoMT-Fog-Cloud architecture of health systems to secure e-health applications by exchanging data confidentially and protecting patient privacy. We presented also a new extension of CP-ABE algorithm known as Context-aware Ciphertext-Policy ABE (Cx-CP-ABE) which integrates the Blockchain and context-awareness to enhance security at the level of data access control management. Besides, our proposal ensures integrity and keeps track of data sharing. After several conducted experiments, we demonstrated the Cx-CP-ABE technique to ensure the patient's data confidentiality. With sufficient integration skills and blockchain expertise, we can even record the health data into real-life usage scenarios. We will also seek to strengthen our model by using machine learning to secure the cloud-computing environment including various connected objects in upcoming future works.

Credit author statement

Boubakeur Annane: Conceptualization, Methodology, Software, Writing – original draft preparation, Data curation, Validation. **Adel Alti**: Project administration, Supervision, Reviewing, Validation **Abderrahim Lakehal**: Reviewing and Editing, Validation.

Declaration of competing interest

No Conflicts of Interest.

References

[1] Kumar P, Kumar R, Gupta GP, Tripathi R. A Distributed framework for detecting DDoS attacks in smart contract-based Blockchain-IoT Systems by leveraging Fog computing. Transact Emerg Telecommun Technol 2021;32(6):e4112.

[2] Sivan R, Zukarnain ZA. Security and privacy in cloud-based E-health system. Symmetry 2021;13(5):742.

[3] Hu VC, Ferraiolo D, Kuhn R, Friedman AR, Lang AJ, Cogdell MM, Scarfone K. Guide to attribute based access control (ABAC) definition and considerations (draft)vol. 800. NIST special publication; 2013. p. 1–54. 162.

[4] Tuli S, Basumatary N, Gill SS, Kahani M, Arya RC, Wander GS, Buyya R. HealthFog: "an ensemble deep learning-based smart healthcare system for automatic diagnosis of heart diseases in integrated IoT and fog computing environments", vol. 104. Future Generation Computer Systems; 2020. p. 187–200. https://doi.org/10.1016/j.future.2019.10.043.2019.

[5] Zou D, Chen S, Han S. Design of a practical WSN based fingerprint localization system. Mobile Network Appl 2020;25:806–18. https://doi.org/10.1007/s11036-019-01298-4.

[6] Jegadeesan S, Azees M, Malarvizhi P, Manogaran G, Chilamkurti N, Varatharajan R, Hsu C. An efficient anonymous mutual authentication technique for providing secure communication in mobile cloud computing for smart city applications. Sustain Cities Soc 2019;49(March):101–522. https://doi.org/10.1016/j.scs.2019.101522.

[7] Hou Y, Garg S, Hui L, Jayakody DNK, Jin R, Hossain MS. A data security enhanced access control mechanism in mobile edge computing. IEEE Access 2020;8:136119–30. https://doi.org/10.1109/ACCESS.2020.3011477.

[8] Aftab MU, Qin Z, Quadri SF, Javed A, Nie X. Role-based ABAC model for implementing least privileges. In: Proceedings of the 2019 8th international conference on software and computer applications; 2019. p. 467–71. https://doi.org/10.1145/3316615.33166674.

[9] Khare N, Preethi D, Chiranji L, Sweta B, Geeta S, Saurabh S, Byungun Y. SMO-DNN: spider monkey optimization and deep neural network hybrid classifier model for intrusion detection. Electronics 2020;9(4):692. https://doi.org/10.3390/electronics9040692.

[10] Singh S, Pradip K, Sharma BY, Mohammad S, Gi Hwan C, In-Ho R. Convergence of Blockchain and artificial intelligence in IoT network for the sustainable smart city. Sustain Cities Soc 2020;63:102364. https://doi.org/10.1016/j.scs.2020.102364. 2020.

[11] Nagasubramanian G, Kumar R, Rizwan S, Amir P. Securing e-health records using keyless signature infrastructure blockchain technology in the cloud. Neural Comput Appl 2018;1. https://doi.org/10.1007/s00521-018-3915-1. 10.1016/B978-0-12-819593-2.00004-2.

[12] Xu X, Chen Y, Yuan Y. Blockchain-based cloudlet management for multimedia workflow in mobile cloud computing. Multimed Tool Appl 2020;79:9819–44. https://doi.org/10.1007/s11042-019-07900-x.

[13] Tuli S, Mahmud R, Tuli S, Buyya R. The journal of systems and software FogBus : a blockchain-based lightweight framework for edge and fog computing. J Syst Software 2019;154:22–36. https://doi.org/10.1016/j.jss.2019.04.050.

[14] Tanwar S, Parekh K, Evans R. Blockchain-based electronic healthcare record system for healthcare 4 . 0 applications. J Inf Secur Appl 2020;50:102407. https://doi.org/10.1016/j.jisa.2019.102407.

[15] Reffad H, Alti A. New approach for optimal semantic-based context-aware cloud service composition for ERP. https://doi.org/10.1007/s00354-018-0036-4; 2018. 36, 4.

[16] Liang X, Zhao J, Shetty S, Liu J, Li D. Integrating blockchain for data sharing and collaboration in mobile healthcare applications. In: IEEE 28th annual international symposium on personal, indoor, and mobile radio communications (PIMRC); 2018. https://doi.org/10.1109/CCGRID.2017.111.

[17] BSWABE java library, co.junwei.bswabe.Bswabe java code examples | Tabnine.

[18] Mir O, van der Weide T, Lee CC. A secure user anonymity and authentication scheme using AVISPA for telecare medical information systems. J Med Syst 2015;39(9):1–16. https://doi.org/10.1007/s10916-015-0265-8.

[19] Abowd GD, Dey AK, Brown PJ, Davies N, Smith M, Steggles P. Towards a better understanding of context and context-awareness. In: International symposium on handheld and ubiquitous computing; 1999. p. 304–7. https://doi.org/10.1007/3-540-48157-5_29.

[20] Waters Brent. Ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization. In: International workshop on public key cryptography. Berlin, Heidelberg: Springer; 2011.

[21] Ali A, Almaiah MA, Hajjej F, Pasha MF, Fang OH, Khan R, Zakarya M. An industrial IoT-based blockchain-enabled secure searchable encryption approach for healthcare systems using neural network. Sensors 2022;22(2):572.

[22] Hannah S, Deepa AJ, Chooralil VS, BrillySangeetha S, Yuvaraj N, Arshath Raja R, Alene A. Blockchain-based deep learning to process IoT data acquisition in cognitive data. Biomed Res Int J 2022. .

[23] Ben Daoud W, Mahfoudhi S. SIMAD: secure intelligent method for IoT-fog environments attacks detection. Comput Mater Continua (CMC) 2022;70(2):2727–42.