[Array 14 (2022) 100150](https://doi.org/10.1016/j.array.2022.100150)

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | Contents lists available at ScienceDirect |  |
| Array |
| journal homepage: [www.sciencedirect.com/journal/array](https://www.sciencedirect.com/journal/array) |

Blockchain based context-aware CP-ABE schema for Internet of Medical Things security   
Boubakeur Annanea, Adel Altia,b,\*, Abderrahim Lakehala   
a *Department of Computer Science, Faculty of Sciences, Ferhat Abbas S*´*etif-1 University, LRSD Laboratory, P.O. 19000, S*´*etif, Algeria*   
b *Department of Management Information Systems & Production Management, College of Business & Economics, Qassim University, P.O. 6633, Buraidah, 51452, Saudi Arabia*

|  |  |
| --- | --- |
| A R T I C L E I N F O | A B S T R A C T |
| *Keywords:*  COVID-19  Healthcare  Authentication  Privacy  Blockchain  IoMT | 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 sig-nificant 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 devel-opment 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 rela-tionship 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 pro-cess. 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 se-curity 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 block-chain, 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 S´etif-1 University, LRSD Laboratory, P.O. 19000, S´etif, Algeria. *E-mail addresses:* [baker11@live.fr](mailto:baker11@live.fr) (B. Annane), [a.alti@qu.edu.sa](mailto:a.alti@qu.edu.sa) (A. Alti), [lakehal.abderrahim@gmail.com](mailto:lakehal.abderrahim@gmail.com) (A. Lakehal).

<https://doi.org/10.1016/j.array.2022.100150>   
[Received 24 November 2021; Received in rev](https://doi.org/10.1016/j.array.2022.100150)ised form 19 February 2022; Accepted 1 April 2022   
Available online 7 April 2022   
2590-0056/© 2022 The Authors. Published by Elsevier Inc. This is an open access article under the CC BY license (<http://creativecommons.org/licenses/by/4.0/>).

*B. Annane et al.*  *Array 14 (2022) 100150*

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, ano-nymity, and audibility. With these features, it can save costs greatly and develop efficiency [3]. In this work, we will apply blockchain technol-ogy and cryptography techniques to ensure security and privacy of healthcare data without needing a third party to control it. The appli-cation 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 confidenti-ality with less processing execution time. The motivation behind pro-posing 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 contri-bution 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 contri-butions 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 phy-sicians. 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 authenti-cation request, then starts the authentication process and monitors the control access rules.

technology for reinforcing the management of decentralized access • Secondly, combining cryptography techniques and Blockchain control and a high level of anonymity offered by blockchain and context-aware security policies.

• Thirdly, providing the security analysis of proposed scheme with AVISPA1 simulator.

The paper is organized as follows. Detailed related work is repre-sented in Section 2. Section 3 gives an overview of the ontology model. The proposed schema in Section 4. Implementation details and experi-mental results are given in Section 5. The conclusion and some per-spectives 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 appli-cation 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

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

2

*B. Annane et al.*  *Array 14 (2022) 100150*

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 ho-momorphic 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 authenti-cation 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.

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 in-formation between the participants in the network. In addition, the completed transaction is usually recorded using an immutable ledger.

**3. Preliminaries**  *3.5. Cryptography*

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 ac-cess 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 pa-tient 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 func-tional 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 secu-rity 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 a1 … an.

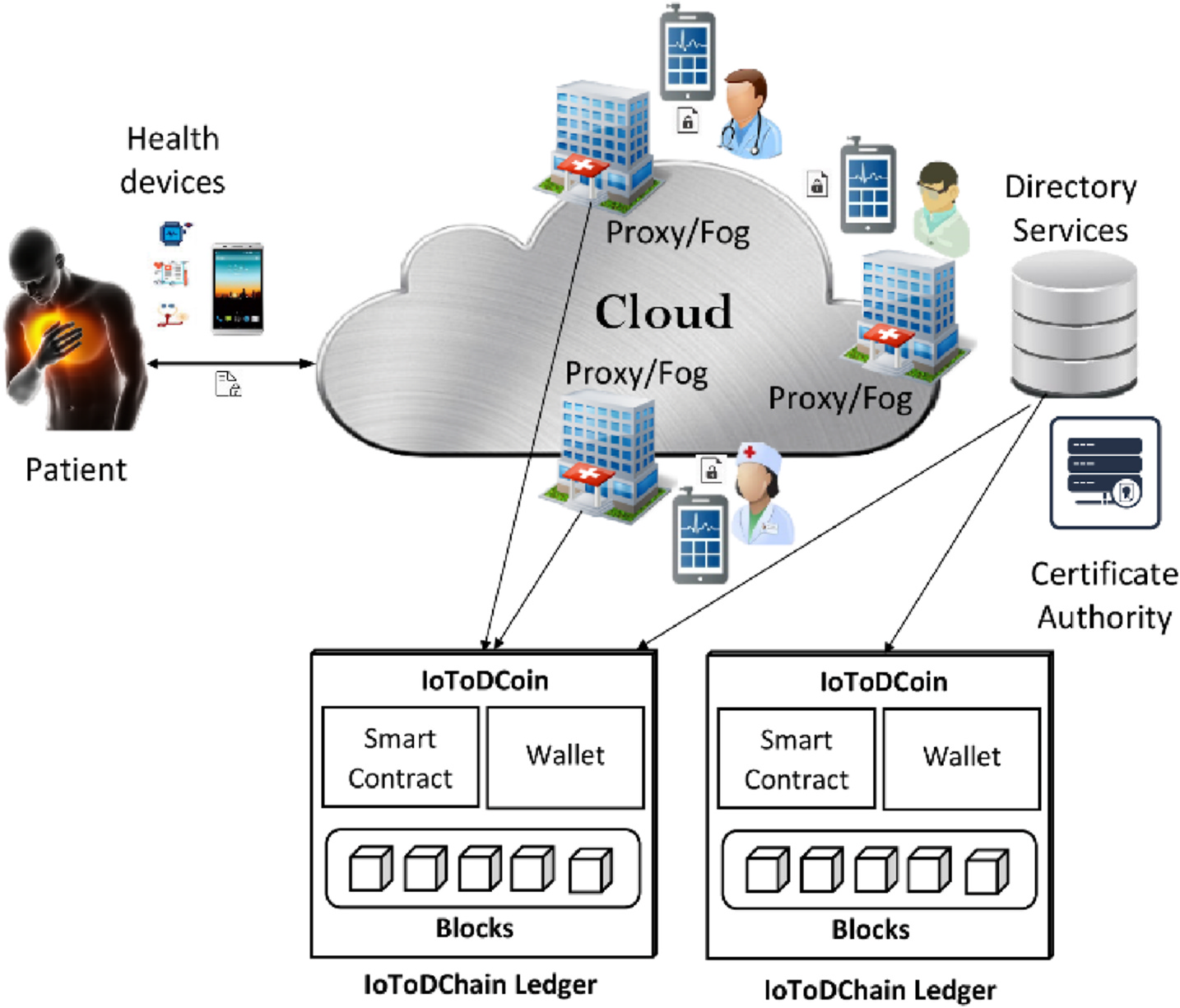
• Phase 2: phase 1 is repeated with the restriction that none of the attributes sets an+1 … an satisfy the access structure corresponding to the challenge.

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

A system is context-aware if it uses context to provide relevant in-formation 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

3

*B. Annane et al.*  *Array 14 (2022) 100150*



**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 pro-vider/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.

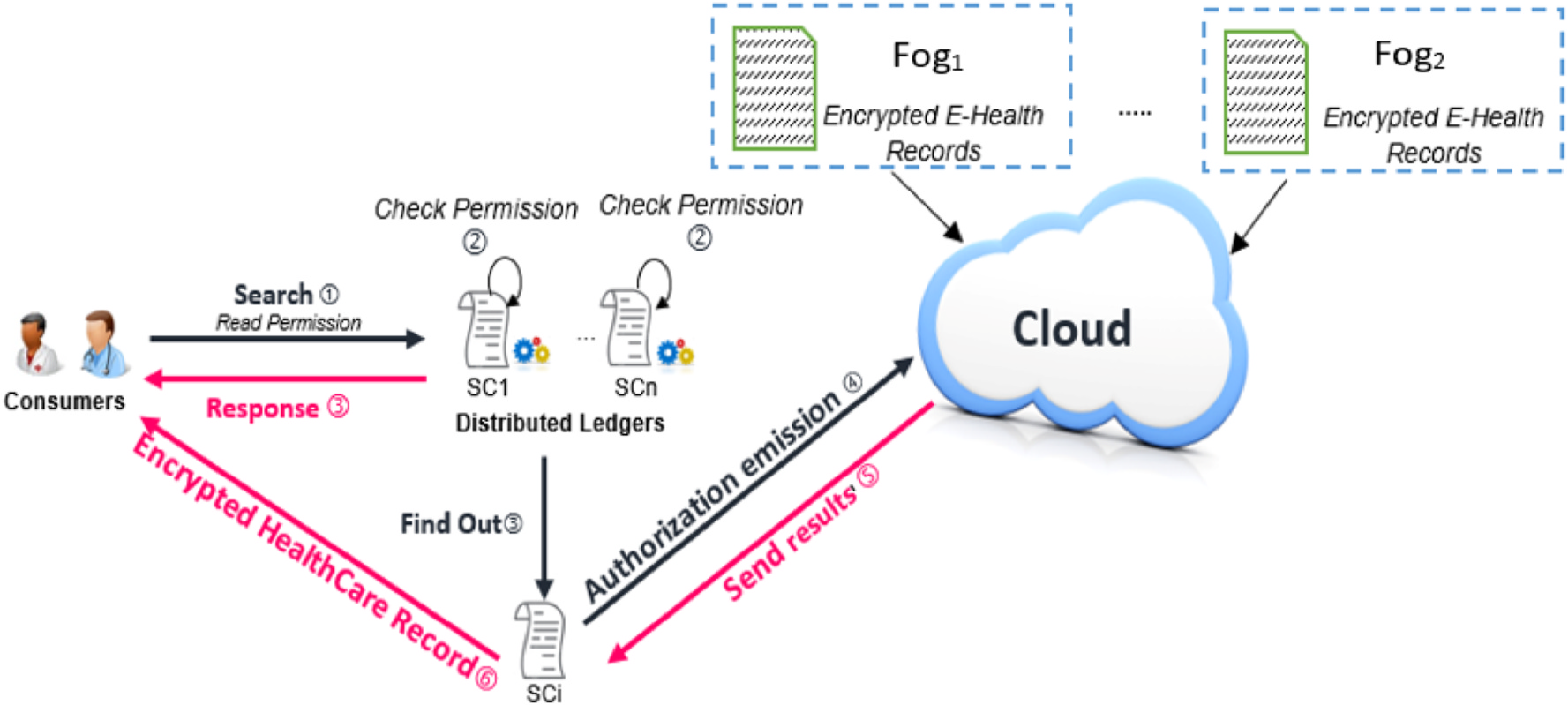
generates them, according to the identity of the users, the set of key • **Certificate Authority (CA):** allows managing all attributes and pairs and grants them access privileges to end-users by providing them with their secret keys according to their attributes.

• **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 encryp-tion/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

4

*B. Annane et al.*  *Array 14 (2022) 100150*



**Fig. 2.** Physicians health sensitive data access.

**Table 1**   
Used notations.

|  |  |
| --- | --- |
| Notation | Description |
| *PKd*  *SKd*  *PKp*  *SKp*  *Idu*  *Idp*  *PKf*  *SKf*  *MK*  *M*  *CT*  *Ci*  *Di*  *G*0  *G*1  *g*  *p*  *e*  *α* and *β* | User/IoMT device public key  User/IoMT device secret key  Physics public key  Physics secret key  Identity of user/device  Identity of physics  Proxy/Fog public key  Proxy/Fog private key  Master key  A sensed data (message)  Encrypted data (text encrypted by Cx-CP-ABE). components of encrypted data.  components of secret key.  A first bilinear group  Asecond bilinear group  Generator point (512-bit prime) A large prime number (144-bit) Bilinear mapping: *G*0 × *G*0 → *G*1*.r* Random numbers |
| • *RequestAuthorization* (*permission, Gr,* @*req*) is used to load authori-zation within the Blockchain from a provider account to the con-sumer’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. | |

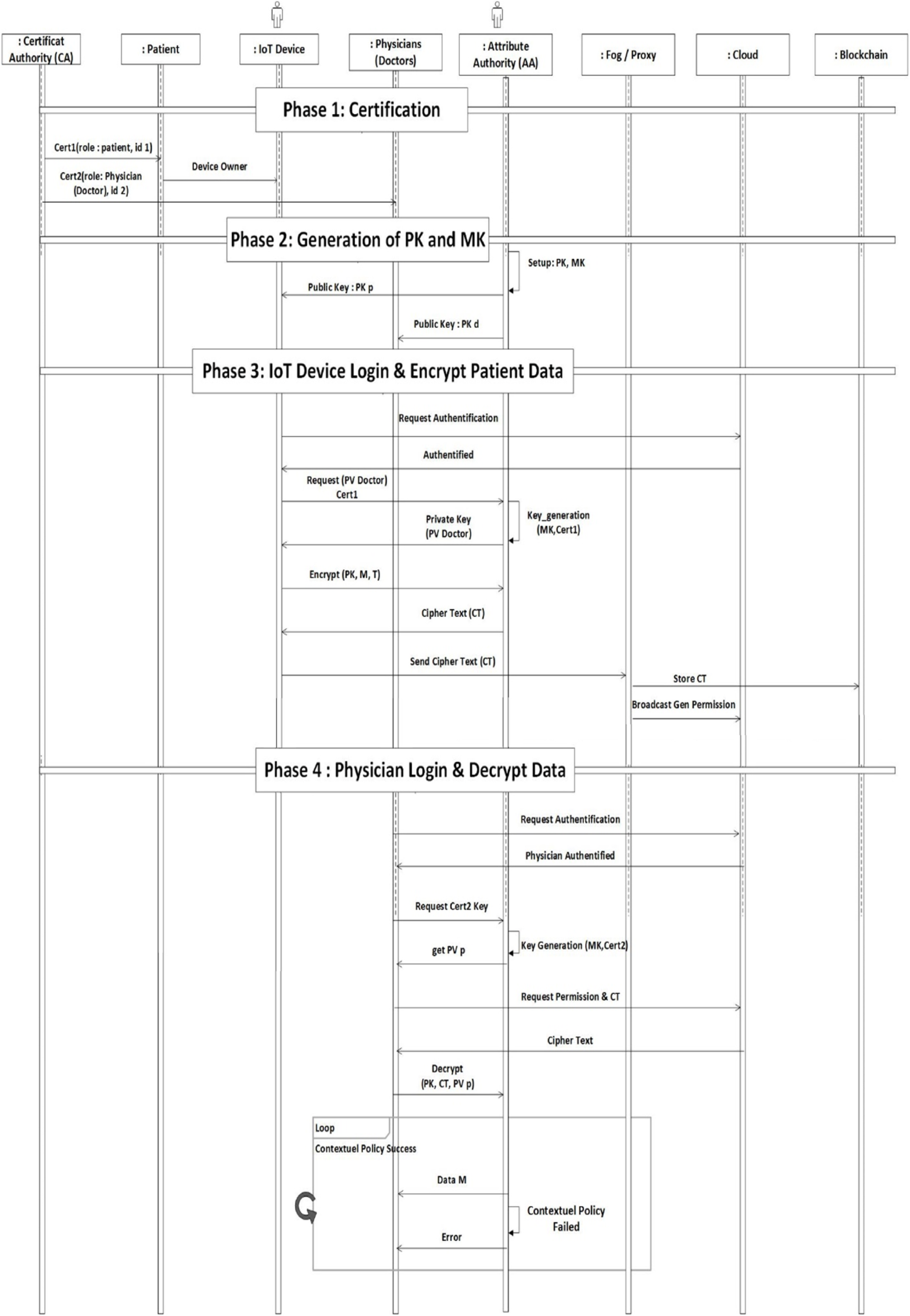
*4.2.2. Certification and registration phase*   
 All IoMT, patients, and physics need to register with a certificate authority (CA) to obtain digital certificates via a secure channel. The participant’s role can represent the medical IoMT, patients, and physics (*nurse, doctor, and specialist*). Each 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 *IDs*, and sends it with a set of context attributes *CxAs* to the Attri-butes Authority (AA).

**Step 2:** The Attributes Authority (AA) generates a master key (*MK*) and public key (*PKs*) based on the identity of sender *IDs* and *CxAs* 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.

5

*B. Annane et al.*  *Array 14 (2022) 100150*



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

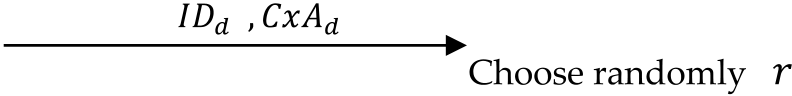
6

*B. Annane et al.*  *Array 14 (2022) 100150*

















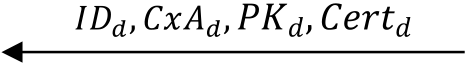












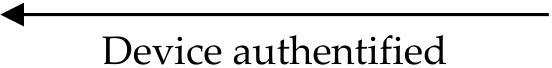
**Fig. 4.** The certification and registration process.







|  |  |
| --- | --- |
|  |  |



**Fig. 5.** The authentication process.

the blockchain. First of all, he authenticates to the Cloud with his cer-tificate 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 pa-tient stored in the blockchain. A physics receives the ciphertext and decrypted it using the *Decrypt* algorithm with his private key Cx-CP-ABE *PVp*. 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,PVp,*P) |  |
| 1:  2:  3:  4:  5:  6:  7:  8:  9: | IF Check\_Access\_Policy (*PVp*, P) Then Begin  *s*←Z*p*  *Ci* ←(*H*2(*i*)*.*∏*n i*=1*xi*)*s*  *M* ←*C*1*.*e(D1*,* C*i*)  return *M* e(D*, C*2 )  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

7

*B. Annane et al.*  *Array 14 (2022) 100150*

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 envi-ronmental 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’)

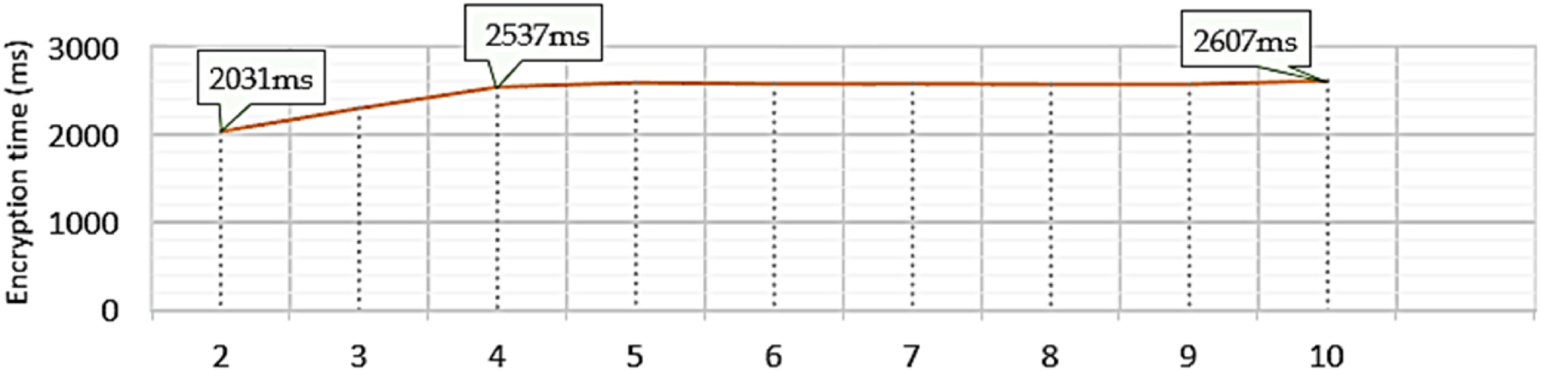
Using context-aware CP-ABE, the new encrypted PHR can be decrypted only by the physics of the orthopedic department that he can find useful in his working domain. All this while he can always check the state of his health (*e.g.*, if it is orthopedic problem, then deploy vitamin D service).

*5.2. Secuirty analysis*

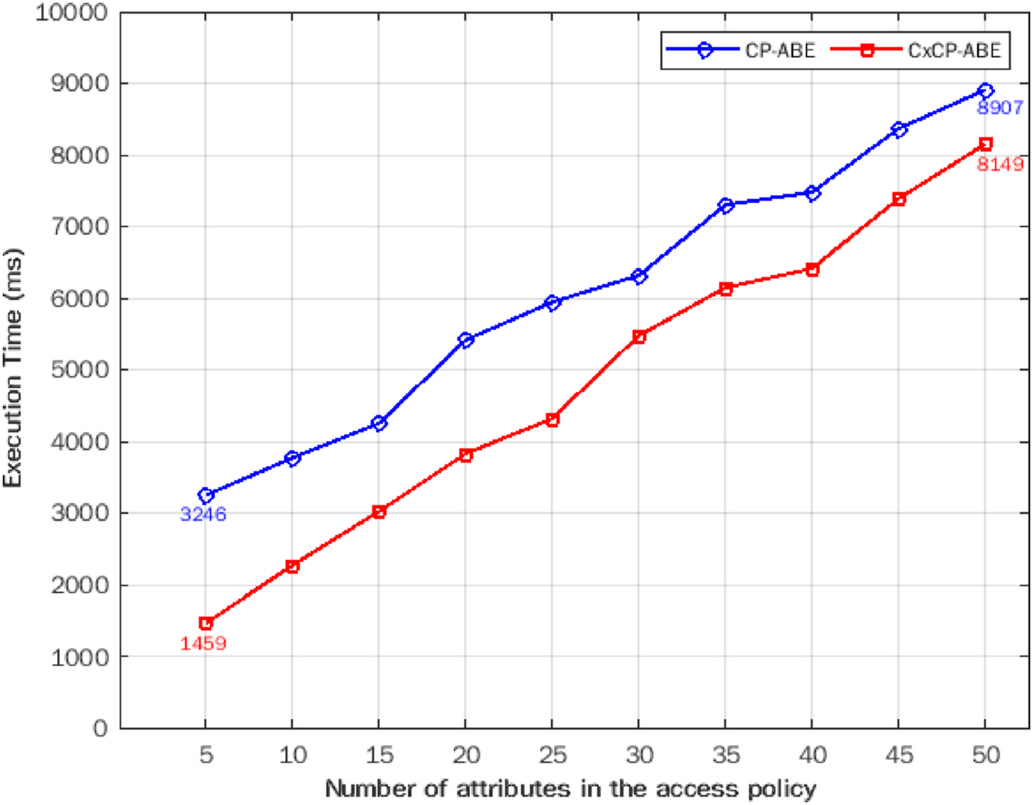
|  |  |
| --- | --- |
| AVISPA is a formal security verification technique for the automatic authentication of cryptographic protocols and applications [18]. AVI-SPA simulator will be used to analyze security for the patient and proxy/fog registration and phases of the proposed schema. Through AVISPA, the symmetrical schema demonstrates that it is secure. The security model is specified and proved [20] as follows:  tries to enter the system using false credentials and broke semantic se-We suppose an attacker **A** with a significant advantage Adv**A** = **E**  curity of the session key in authentication schema. An attacker **A** selects randomly a set of attributes to generate the access control policy **P**\* and then send it to the adversary **B** . The adversary **B** runs *Setup* algorithm to generate the public key and then send it to. **A** *.*  **Phase 1.** In this phase, the attacker **A** answers private key queries. He can adaptively submit set *Si* to **B** where *Si* does not satisfy **P**\* and **B** responds with the secret key **S K**\* corresponding to the sub-mitted set *Si*. The attacker **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*)*α, e*(*H*2(*id*)*, g*)*β*)*s* and *C*1 = *gs*. It will also choose  **Phase 2.** The adversary **A** will eventually output *β* random *x*1*, x*2*,* …*.xn* ∈ Z*p* and generate the ciphertext components *Ci* ′ of *β*. The simu-  lator then outputs zero if *β* = *β* Finally, the Advantage of **B** is as follows: ′ ; otherwise, it outputs one if *β* ∕= *β*0. | |
| Adv**B** =1 2[*Pr*{*β*′ = *β / β* = 1}] + 1 2[*Pr*{*β*′ = *β / β* = 0}] − 1 2= **E** | =1 2+ Adv**A** |
| **E** 2 is also with not negligible advantage. Consequently, as Adv**A** = **E** is assumed not to be negligible, Adv**B** = | |

8

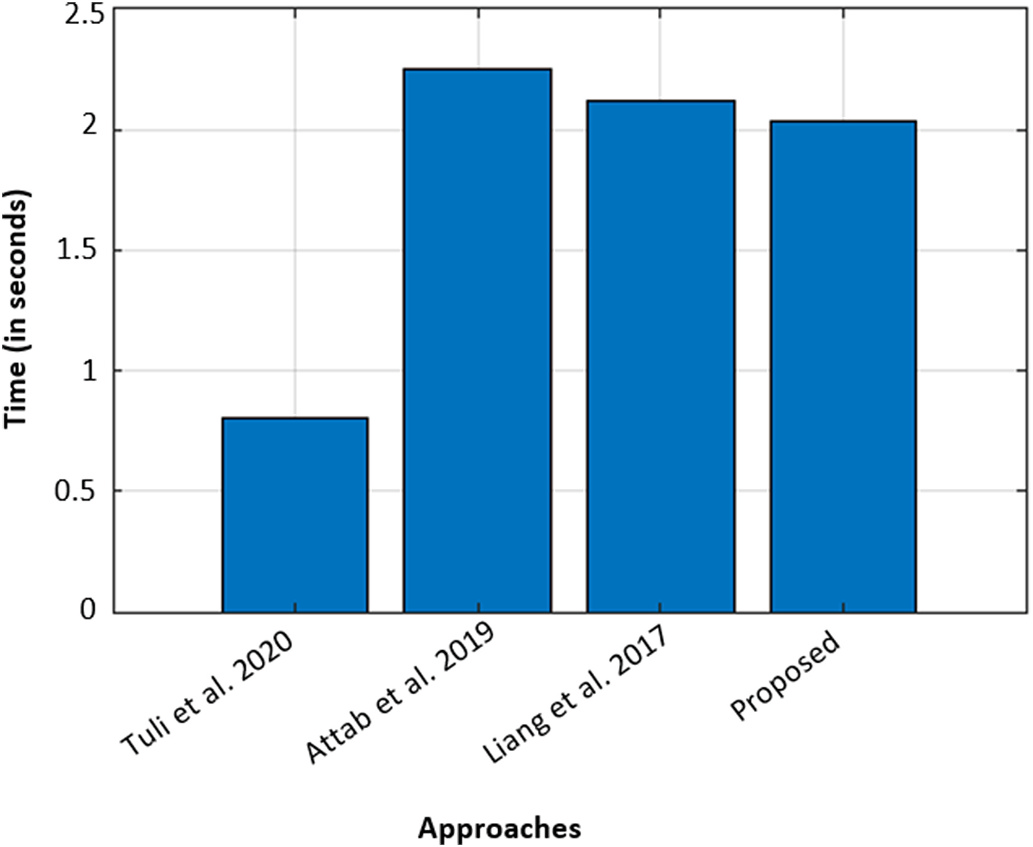
*B. Annane et al.*  *Array 14 (2022) 100150*



**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.

9

*B. Annane et al.*  *Array 14 (2022) 100150*

[2] [Sivan R, Zukarnain ZA. Security and privacy in cloud-based E-health system.](http://refhub.elsevier.com/S2590-0056(22)00019-4/sref2) [Symmetry 2021;13(5):742.](http://refhub.elsevier.com/S2590-0056(22)00019-4/sref2)

[3] [Hu VC, Ferraiolo D, Kuhn](http://refhub.elsevier.com/S2590-0056(22)00019-4/sref2) [R, Friedman AR, Lang AJ, Cogdell MM, Scarfone K.](http://refhub.elsevier.com/S2590-0056(22)00019-4/sref3)

[Guide to attribute based access control (ABAC) definition and considerations](http://refhub.elsevier.com/S2590-0056(22)00019-4/sref3) [(draft)vol. 800. NIST special publication; 2013. p. 1–54. 162.](http://refhub.elsevier.com/S2590-0056(22)00019-4/sref3)

[4] [Tuli S, Basumatary N, Gill SS, Kahani M, Arya RC, Wander GS,](http://refhub.elsevier.com/S2590-0056(22)00019-4/sref3) 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/](https://doi.org/10.1016/j.future.2019.10.043.2019) [j.future.2019.10.043.2019](https://doi.org/10.1016/j.future.2019.10.043.2019).

[5] [Zou D, Chen S, Han S. De](https://doi.org/10.1016/j.future.2019.10.043.2019)sign of a practical WSN based fingerprint localization system. Mobile Network Appl 2020;25:806–18. [https://doi.org/10.1007/s11036-](https://doi.org/10.1007/s11036-019-01298-4) [019-01298-4](https://doi.org/10.1007/s11036-019-01298-4).

[6] [Jegadeesan S](https://doi.org/10.1007/s11036-019-01298-4), 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/](https://doi.org/10.1016/j.scs.2019.101522) [10.1016/j.scs.2019.101522](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](http://refhub.elsevier.com/S2590-0056(22)00019-4/sref7) [access control mechanism in mobile edge computing. IEEE Access 2020;8:](http://refhub.elsevier.com/S2590-0056(22)00019-4/sref7) [136119–30. https://doi.org/10.1109/ACCESS.2020.3011477.](http://refhub.elsevier.com/S2590-0056(22)00019-4/sref7)

[8] [Aftab MU, Qin Z, Quadri SF, Javed A, Nie X. Role-based AB](http://refhub.elsevier.com/S2590-0056(22)00019-4/sref7)AC model for implementing least privileges. In: Proceedings of the 2019 8th international conference on software and computer applications; 2019. p. 467–71. [https://doi.](https://doi.org/10.1145/3316615.33166674) [org/10.1145/3316615.33166674](https://doi.org/10.1145/3316615.33166674).

[9] [Khare N, Preethi D, Chiranji L, Sw](https://doi.org/10.1145/3316615.33166674)eta 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/](https://doi.org/10.3390/electronics9040692)   
[electronics9040692](https://doi.org/10.3390/electronics9040692).

[10] [Singh S, Pradip K, S](https://doi.org/10.3390/electronics9040692)harma 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/ B978-0-12-819593-2.0[0004-2.](https://doi.org/10.1007/s00521-018-3915-1)

10