Towards privacy and ownership preserving of outsourced health data in IoT-cloud context

Youcef Ould-Yahia, Samia Bouzefrane, Hanifa Boucheneb

Towards privacy and ownership preserving of outsourced health data in IoT-cloud context

1st Youcef Ould-Yahia
CEDRIC Lab.
CNAM
Paris, France
youcef.ouldyahia.auditeur@lecnam.net

2nd Samia Bouzefrane
CEDRIC Lab.
CNAM
Paris, France
samia.bouzefrane@lecnam.net

3rd Hanifa Boucheneb
VeriForm Lab.
Ecole Polytechnique de Montréal
Montréal, Canada
hanifa.boucheneb@polymtl.ca

***Abstract*—In this paper, we propose a novel data-owner centric privacy model for in-home-monitoring applications, that implements a promising attribute-based encryption (ABE) to reinforce the data-owner access control and the security of anonymous data access. This proposed protocol avoids threats from curious cloud service providers. Unlike other schemes that implement ABE by outsourcing the heavy computational tasks such as encryption and decryption processes, we propose a framework in which we externalize the complete ABE-encryption algorithms to avoid complex outsourcing process and use well know efficient symmetric encryption in constrained devices. We have performed an experimental analysis to show how much gain allows such offloading.**

***Index Terms*—e-Health, IoT, Cloud, Privacy, ABE.**

I. Introduction

Privacy has become one of the main concerns in healthcare applications from the perspective of data ownership. This concern is exacerbated by the rapid developpement of Internet of Things (IoT), where connected devices collect a substantial amount of personal data, such as locations and physiological parameters, and transmits them to the cloud in order to store, process and share them, thanks to information and communication technologies. When health science is combined with IT, the result is the e-Health paradigm. Unlike telemedicine, e-Health is not exclusively reserved for healthcare professionals. E-Health model is rather centered and pivoted on the consumers of health systems [1]. But one critical issue of the e-Health paradigm is that it deals with personal sensitive data that can harm the data privacy. Furthermore, some threats may arise from service providers since many companies have significant commercial interests in collecting private health data [2]. There are also other risks to provide her/his personal data to the service providers that are not completely free from security breaches [3]. Additionally, even the so called trusted third party may deliberately or by inadvertence perform illegal activities on personal healthcare data. In this paper, we consider that privacy protection includes data-ownership control of encryption and access [4], and avoids leakage of information that can be deduced from available metadata (informations on data: date, time, kind of measurement, etc.) [5]. To meet these requirements, we propose a new security model implementing a recent and promising cryptographic scheme called attribute-based encryption (ABE). Our solution is a realistic proposal for in-home monitoring applications that involve largely IoT devices. The main objective of this paper is the data and privacy protection while giving to the data owner a better control on his/her data encryption and sharing.

The remainder of this paper is organized as follows: in Section 2, a brief description is given regarding the context and the environment of in-home monitoring, the challenges and threats on privacy, the regulation and the associated legal constraints. Section 3 is devoted to the literature review on data privacy for e-Health in IoT-cloud environment. It also presents the principle of attribute-based encryption mechanism. In Section 4, our proposed model is described followed by a security analysis, while a formal validation and an experimental analysis to validate the concept are presented in Section 5. Finally, we conclude the paper with some perspectives.

II. In-home monitoring: case description and threat model

One interesting scenario in e-Health is in-home monitoring as it brings an IoT-cloud architecture and strong privacy constraints.

a) In-home monitoring case description: In-home monitoring technology includes many sensors and smart devices that collect data related to health parameters like blood pressure, heartbeat, etc. to be transmitted for processing, storage and sharing within the cloud. In this context, many commercial solutions are being developed to assist the patient to deliberately share his own health data with health specialists [4]. However, as we can see below, the cloud cannot be considered as completely trustful.

b) Threat model: To define an adversary model, the in-home monitoring in the real world should be considered. The purpose of our proposed solution is to retain and to preserve the privacy of the patient. Therefore, threats derived from the communication channel must be considered. There is an adequate overview provided by the Dolev-Yao model [6], which assumes the network as an intruder. Thus, an attacker can listen, delete, replay and modify a message. However, the attacker will not be able to decrypt a message, if he does not possess the decryption key. Then, since cloud infrastructures are under control of a third party that may be curious [3], we adopt the same model as in [7], that considers

the cloud as a honest but a curious actor. This means that the cloud rolls out the protocol correctly but could try to deduce information about the patient. Furthermore, this model supports the realistic threat involved in the cloud context where a cloud infrastructure can be targeted by malicious entities or can have inadvertent leak personal information.

III. Review of the literature on data protection and privacy

a) Privacy in IoT-cloud: Integrating IoT with cloud computing provides a promising solution for managing healthcare sensor data efficiently [8]. However IoT-cloud is a heterogeneous environment. In addition, offering an end-to-end solution in that environment to protect data and privacy is difficult. Hence, the cloud is a resourceful entity that provides unlimited virtual resources while its security and trustworthy are managed by a third party [3]. Whereas, IoT may have a high level of trust with a physical control on the devices while facing resource restrictions. Relevant literature reviews bring out that the solutions offered are confronted with this issue. For example, authors of [3] and [7] provide an interesting solution to achieve a fine-grained access control on cloud environment, but did not deal with restrictive IoT environment. However in [9] and [10], the authors propose to secure data and protect privacy in IoT environment without evidence of privacy in the cloud side. The approach proposed in [11], [12] and [13] is based on Attribute-Based Encryption (ABE), by outsourcing heavy computational operations. This scheme provides a patient-centric encryption and access control. However, the proposed solution needs a significant increase in messages exchanges, furthermore [11] and [12] did not propose to outsource the encryption process,which is needed in some IoT-health applications.

b) Attribute-Based Encryption (ABE): Recently, the promising ABE scheme is proposed to enhance privacy for e-Health applications like in-home monitoring [14]. ABE is a public key one-to-many encryption scheme. In addition to securing data transmission and storage, ABE provides a fine-grained access control, a scalable key management and a flexible data distribution [15] and [7]. It allows encrypting the data without any prior knowledge of the identities of the recipients. Two principal variants are proposed : Ciphertext Policy Attribute Based Encryption (CP-ABE) [16] and Key Policy Attribute Based Encryption (KP-ABE) [17]. We focus on CP-ABE (Fig.1) which allows the data owner to encrypt and define access policy for his data. The algorithms associated to CP-ABE are reported in table I. ABE is a pairing based encryption scheme, using a bilinear map denoted $e : \mathbb{G}_0 \times \mathbb{G}_0 \rightarrow \mathbb{G}_T$, where $\mathbb{G}_0$ and $\mathbb{G}_T$ are a bilinear group of prime order p. The usual implementation of ABE builds a group from an elliptic curve E defined over a finite field F_q, to obtain a multiplicative cyclic group of prime order p, where the field size q and the prime order p determine the security strength [15]. For a security level corresponding to AES 128 bits, as shown in table II, we choose an elliptic curve defined over a finite field with a prime order of 256 and a field size of 1536 [18].

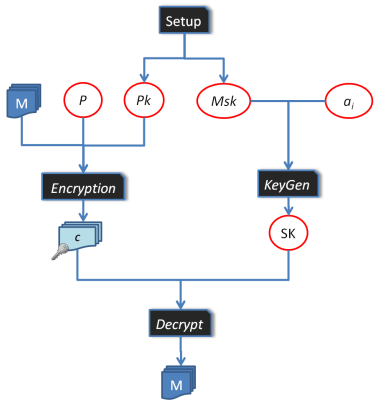


Fig. 1. CP-ABE working flow

TABLE I
CP-ABE algorithms input/output

Setup	*Input*: security parameter. *Output*: a public key for encryption Pk and a master secret key Msk to generate decryption key.
Encrypt	*Input* : message m, public key Pk and policy P. *Output*: ciphertext "c".
KeyGen	*Input*: Master Secret Key Msk and a set of attributes a_i. *Output*: a decryption secret key Sk.
Decrypt	*Input*: a cipher text c, a decryption secret key Sk. *Output*: If attributes a_i satisfy the policy P then m else $\perp$.

The characteristics of ABE scheme seem to be interesting to be implemented for the user privacy concerns [19] but ABE is a computationally expensive encryption method, especially on resource-constrained devices [20]. We propose, in the next section, a design that gives an end-to-end strong privacy protection with a data-owner centric access control in IoT-cloud environment for e-Health applications.

IV. Description of the proposed solution

The privacy protection is a process that brings several mechanisms at various levels of the data life cycle. To guarantee this protection, it is necessary to use cryptographic primitives for the data encryption and to ensure their confidentiality and integrity. Simultaneously, it becomes mandatory to set up access control mechanisms under data-owner control to enhance privacy. For this purpose, the proposed solution is built on Attribute-Based Encryption and cloudlet architecture (see Fig.3). The proposed solution should be able to provide an access control centred on the data-owner, while preserving privacy in in-home monitoring. The premise of the proposed model provides a total access control for the data owner. Each requester for data must authenticate himself to the data owner while hiding his identity for the cloud. Another advantage of the proposed solution is to reduce the cloud provider intervention. Before detailing our proposed solution, a brief description of the system will be presented. The components of our system are given as roles and the interactions between the roles are presented in Fig.2.

TABLE II
SECURITY LEVEL COMPARISON

Security Strength(bits)	Symmetric algorithms	RSA-Key length	ABE p (prime order), q (field size)
80	2TDEA	1024	p=160, q=512
112	3TDEA	2048	p=224, q=1024
128	AES-128	3072	p=256, q=1536

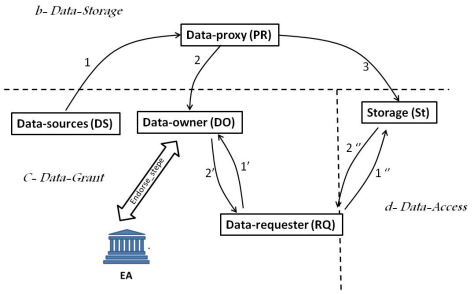


Fig. 2. Personal IoT data sharing (For convenience, we omit the first process, which is the initialization)

A. The identified roles in our system

In our system, we identify the following roles: 1) *Data-owner (DO)* is in charge of generating data with his owned devices and storing them in the cloud. The data-owner is the only one who has the right to grant access to his data. 2) *Data-proxy (PR)* in our proposed architecture, the cloudlet acts as a proxy. The cloudlet can be viewed as a base station, a smart box or a WIFI Hotspot/router that hosts a hypervisor. Using a cloudlet instead of a cloud to outsource the computation of the devices fosters the usage of a good bandwidth quality to ensure data security. 3) *Data-requester (RQ)* can be a physician or any other medical practitioner that requests access to the personal data that are well identified by the data owner. To prove the identity of the data requester, we use a PKI infrastructure with an Endorsement Authority. 4) *Endorsement Authority (EA)*: is the trusted authority that verifies the identity and attributes of the requester. The requester provides an evidence of his identity endorsed by this authority. For example, the French digital health agency (ASIP Santé) maintains a directory of the health professionals. 5) *Storage (ST)*: is instantiated by a cloud storage. This actor can only check, if an anonymous requester can provide evidence, which is allowed by DO to access data. 6) *Data-sources (DS)*: are the devices that generate data (sensors or any health devices used to make measurements).

B. Assumptions

In the proposed solution, we make the following assumptions: 1) The Data-owner knows the identity of the Data-requester, which means that the Data-owner (DO) knows the Data-requester (RQ) public key PK_{RQ}. This assumption involves that DO can authenticate signed messages of that Data-requester. 2) The identity of RQ is authenticated with a current available PKI infrastructure. In this case, DO trusts an

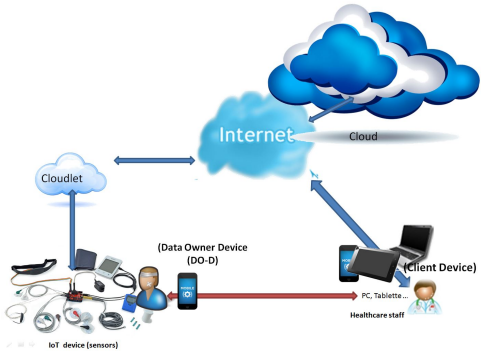


Fig. 3. The proposed architecture model

Endorsement authority EA, which issues a digital certificate or maintains a list of valid public keys. The same mechanism is available to authenticate storage (ST). 3) Sensors and cloudlet are under physical control of the Data-owner. The delegation of calculations to the cloudlet will not compromise the solution, the related cloudlet security and trust are out of scope of this work. 4) The perfect cryptography and the messages are exchanged over a network that is controlled by Dolev-Yao intruder [6].

C. Proposed protocol

We use in the proposed solution a CP-ABE including four algorithms (*Setup, KeyGen, Encrypt, Decrypt*) as defined before and a cryptographic hash function H. To enhance the protection of privacy, the identity of the data requester should be hidden. In order to achieve this, every requester generates a public/secret key pair that will be used to perform the access grant request. After endorsement of the requester identity by EA, the data owner issues an anonymous credential for the requester to let him accessing to the ciphertext in the cloud. An overview of the interaction between actors after initialization steps is given in Fig.2 and detailed message exchanges are shown in Fig.4. Table III presents the notation used in the protocol.

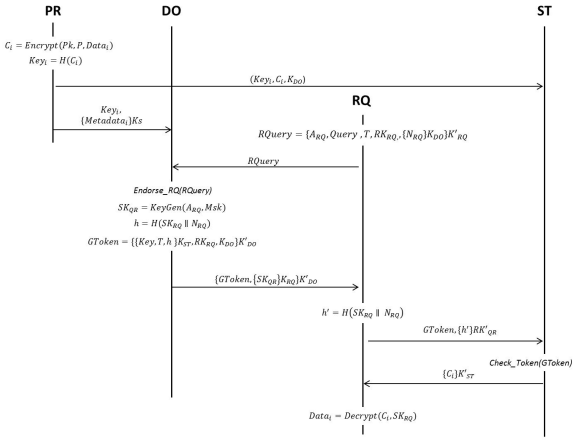


Fig. 4. Message exchanges of the proposed scheme

TABLE III
NOTATIONS USED

Notation	Description
X	Identity of X playing a role in the system
Ks	Symmetric session key
Msk	Master Secret Key, used in ABE primitive
Pk	Public key used to encrypt data in ABE primitive
SK_X	ABE decryption key generated to X
Key	Index used in Cloud storage
K_x	Public key of X
K'_x	Secret key of X
MK_x	Encrypt message M with X's public key Kx
MK_x	Signed message M with X's private key Kx

The outline of the proposed solution consists of four major processes:

*1) **Initialization process**:* In this step, we execute the *setup* algorithm. The result is a master secret key Msk and a public key Pk. The public key Pk as well as the data access policy P are sent to the cloudlet for encryption.

We provision all the connected devices with cryptographic material to secure communication between these devices and the cloudlet. This operation is called bootstrapping in IoT [21]. We adopt an offline key distribution solution that can be easily deployed in the proposed use case. In this kind of solution, a symmetric session key Sk is generated after few data exchanges between the data sources and the data proxy [21]. Authors of [10] have described such a solution.

*2) **Cloud storage process**:* In these steps, all the data generated by Data-source are transmitted to Data-proxy (cloudlet) with metadata through a secure channel. Data-proxy executes *Encrypt(Pk,P,Data)* and generates a cypher text C. C is stored in the cloud in the form of a key-value, where $key = H(C)$ and $value = C$. Data-proxy sends then the key and metatdata to Data-owner. Data-owner maintains a table of $(Metadata, Key, P)$, where Key is used to query C in storage ST and P is an access policy.

Message 1: after the establishment of a key session Ks, Data-source can send the collected data to Data-proxy. These data are linked with a metadata *(date, time, type of data, etc.)*. $DS \rightarrow PR$: $\{Data_i, Metadata_i\}K_s$

Message 2: in parallel with *Message 2*, PR executes $Encryption(Pk, P, Data)$ algorithm and computes the hash value of the ciphertext to generate Key. $C_i = Encrypt(Pk, P, Data_i)$ and $Key_i = H(C_i)$, the message 2 is $PR \rightarrow St : (Key_i, C_i, K_{DO})$

Message 3: PR informs Data-owner that new data have been generated by sending to him Metadata encrypted with session key Ks and Key to localize those data in the cloud: $PR \rightarrow DO$:$\{Key_i, Metadata_i\}Ks$

*3) **Access grant process**:* In this process, DO provides a privilege to RQ to access the ciphertext in the cloud (ST) and issues to RQ an appropriate ABE decryption key (SK_{RQ}).

We define some data structures to perform this process :

Request query (RQuery): is a data structure that RQ can send to DO to formulate the following request:

$$RQuery = \{A_{RQ}, Query, T, RK_{RQ}, \{N\}K_{DO}\}K'_RQ$$

Where $A_{RQ} = \{a_0, a_1, ..a_n\} \in \mathcal{A}$ is a set of RQ attributes, *Query* is a description of the data requested, T is a grant time validation, RK_{RQ} is a public key generated to be used in this request and $\{N_{RQ}\}K_{DO}$ is a nonce generated by RQ and cyphered with the public key of DO.

GToken: This data structure is issued by the data owner DO and sent to the RQ to provide the evidence for the data-storage (ST) that this requester has a decryption key and has been granted by the data owner to access to the cyphertext C identified by Key. This authorization is valid for T time.

$$GToken = \{\{Key, T, h\}K_{ST}, RK_{RQ}, K_{DO}\}K'_{DO}$$

With $h = H(SK_{RQ} \| N_{RQ})$. We also define two primitives that will be used:

Endorse_RQ(RQuery): This primitive allows DO to parse $RQuery$, checks and authenticates the identity of RQ and his attributes thanks to the Endorsement Authority.

Token_Gen(RQuery): Once all the controls are done, DO executes this primitive to generate a structure. This structure is the evidence of the DO agreement to access to the $data$.

Message 1': RQ sends his query: $RQ \rightarrow DO$: $RQuery$. After receiving *Message 1'*, DO, executes $Endorse\_RQ(RQuery)$ to verify and to authenticate the identity of RQ and his attributes.

Message 2': Once all the controls are done, DO executes $KeyGen(A_{RQ}, Msk)$ algorithm to generate a specific decryption key SK_{RQ} and *Token_Gen(RQuery, SK_{RQ})* primitive to generate an appropriate $GToken$ and to send it to RQ:$DO \rightarrow RQ$: $\{GToken, \{Sk_{QR}\}K_{RQ}\}K'_{DO}$.

*4) **Data access process**:* When the data owner (DO) agrees to grant access to the requester (RQ) by sending $GToken$ and SK_{QR}, the RQ can ask the cloud (ST) to transfer the ciphered data C in order to decrypt them locally with the received SK_{RQ}. ST checks whether $GToken$ is a valid one by performing a $Check\_Token(GToken)$ primitive.

Check_Token(GToken): ST parses $GToken = \{\{Key, T, h\}K_{ST}, RK_{RQ}, K_{DO}\}K'_{DO}$ and does the verifications, as presented in table IV.

Message 1": Once $GToken$ and SK_{RQ} are received, RQ computes $h' = H(SK_{RQ} \| N_{RQ})$ and signs it with RK'_{RQ} and sends it to ST. $RQ \rightarrow ST$: $GToken, \{h'\}RK'_{RQ}$

Message 2": When ST receives *Message 1"*, it performs $Check\_Token(GToken)$. If all the tests are valid, ST has the evidence that the $GToken$ refers to the data owned by the issuer of $GToken$ and the requester is the one for whom $GToken$ has been issued. At this point, ST can send the ciphertext requested. $ST \rightarrow RQ$: $\{C_i\}K'_{ST}$. After *Message 2"*, RQ can execute *Decrypt* algorithm to retrieve the clear desired $data$. The overall workflow of the protocol is given in Fig.4.

V. MODEL VALIDATION

In this section, we describe a formal verification of the proposed protocol and we perform an experimental analysis to validate our technical choices.

TABLE IV
GTOKEN VERIFICATIONS

Received elements	Verifications	Cryptographic elements
GToken	GToken issuers (Signature validity)	K'_{DO}
GToken	GToken time validity	T
GToken	GToken issuers ownership of requested C_i	K'_{DO}
GToken + $\{h'\}RK'_{RQ}$	Requester valid ownership of GToken	$h + h' + RK_{RQ}$

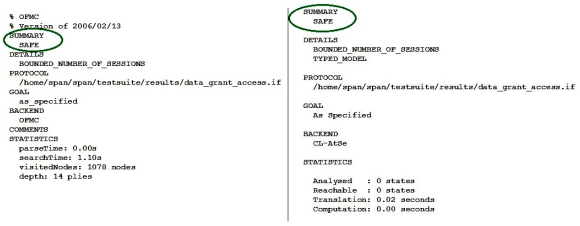


Fig. 5. Protocol verification with OFMC and ATSE backbends results.

A. Formal validation

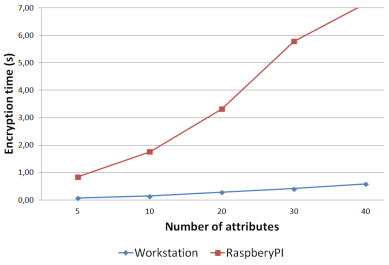
To validate the safety of the proposed system, we made a formal description with a specification of the expected security properties with the High Level Protocol Specification Language (HLPSL) by using the automatic verification tool Avispa [22]. The High Level Protocol Specification Language (HLPSL) is based on roles description. For each role, we define a set of variables to describe the state and transition rules that describe the behavior of the agent who plays this role. There are specific roles: *session* role, which is a combination of different roles and *environment* role to define the intruder initial knowledge, the expected security specification in goals section and a session composition execution, that are useful to simulate different attack scenarios. Avispa is a preferment tool to verify security properties. It is composed from automatic analysis techniques called backbends: On-the-fly model-checker (OFMC), CL-based Attack searcher (CL-AtSe), SAT-based model-checker (SATMC), and Tree automata-based protocol analyzer (TA4SP). Avispa input is an HLPSL specification that is converted in a lower level language called Intermediate Format (IF) that can be interpreted by different backbends. The system is modeled using HLPSL specification. The behavior of each entity involved in the protocol *(DO, PR, DS...)* is described as roles. With regard to the e-Health security goals, we define in our model the secrecy of data and metadata and authentication of RQ by DO as security properties. The authentication is implicitly expressed in the protocol (PKI infrastructure) but we explicitly specify an authentication exchanges derived from TLS certificate between the DO and DR with HLPSL. The cloud $Gtoken$ control is specified using a matching variable to define which messages are acceptable. Secrecy of Data-Request identity is modeled with predicate $secret(RQ', sec\_2, DO, RQ)$, which means that this identity should be known only by the Data-Owner and the Data-Requester. In the same way, we model secrecy of Data and Metadata. Authentication of Data-Requester by Data-Owner is specified by the predicates $request(DO, RQ, do\_rq2, Ndo.Nrq)$ and $witness(RQ, DO, do\_rq2, Ndo'.Nrq')$, where $Ndo'.Nrq'$ is the message data on which RQ and DO authenticate. Besides the scenarios explored automatically by the tool, we feigned other possible attacks, where the intruder may play several roles. The results obtained by AVISPA show that the protocol is secure and satisfies the expected security properties, as presented in Fig.5, under assumptions made in IV-B.

B. Experimental analysis

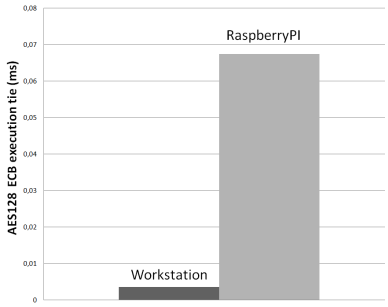
To validate our proposal, we perform experiments with C code on Raspberry Pi platforms acting as constrained devices and on a workstation as a cloudlet node. The experimental simulation of the CP-ABE scheme is done using the pairing based cryptography library (PBC-Library) [23]. We also perform some tests with AES 129 ECB provided by [24] with Raspberry Pi platforms to compare its execution time with the original CP-ABE scheme [25] and with another recent CP-ABE proposition [13]. The workstation runs 64-bits Ubuntu 16.04 LTS, with Intel(R) Core (TM) i5-4590s 3.00GHz CPU and 8GB RAM. The Raspberry Pi 3 Model B runs a Raspbian operating system, with 1.2GHz 64-bit quad-core ARMv8 and 1GB RAM. To achieve a 128-bit security level, we lightly modify the original PBC-Library Type-A pairing parameters to use a 256-bit elliptic curve group based on the supersingular curve $y2 = x3 + x$ over 1536-bit finite field. The number of attributes is $N = \{5, 10, 20, 30, 40\}$. We consider this range to be representative of the real-world applications. To avoid errors, the experimental results are the means of 10 trials. For the in-home monitoring use case, we analyse the encryption time because it is the most significant operation performed by the data-owner constrained devices. We simulate the encryption algorithm of CP-ABE scheme [25] both on constrained and unconstrained devices. We take the significant computational operations by considering the number of exponentiation in $\mathbb{G}_0$ and $\mathbb{G}_T$ and pairing operation. Fig.6 (a) shows the execution time of CP-ABE encryption algorithm on Raspberry Pi platform and workstation. As we can expect, the execution time on Raspberry Pi is in average 12.5 time slower than in a workstation where the time does not exceed one second for up to fourteen attributes. Furthermore, even if the speed of AES algorithm in Raspberry Pi is 18.9 times slower than in the workstation, as we can see in Fig.6 (b), the results presented in table V show that AES is significantly more efficient than ABE in constrained devices. The results motivate our system architecture to outsource ABE encryption to the cloudlet.

VI. CONCLUSION

In this paper, we presented a data-owner centric approach that provides a limited grant for the cloud provider and that takes into consideration the Internet of things constraints. Our solution enhances privacy protection by masking the data client identity for the cloud service provider. In addition, we



(a) CP-ABE encryption time



(b) AES 128 execution time

Fig. 6. Experimental results

TABLE V
COMPARISON BETWEEN CP-ABE ENCRYPTION AND AES 128 EXECUTION TIME (MS)

Nb attrib	CP-ABE [25]	CP-ABE [13]	AES 128
5	892,9518	150,50145	0,0674
10	1902,03855	110,6723	0,0678
20	3310,6896	132,8921	0,0674
30	5233,14585	147,55785	0,0673
40	6854,60375	153,5809	0,0674

have performed a formal analysis of the proposed protocol and made an experimental test analysis that demonstrated the efficiency of our cloudlet-based architecture. To enhance security in the IoT side, a complementary work has been done in [26] to propose a computationally intelligent model to measure possible vulnerabilities based on bio-inspired intelligence of ant colony.

REFERENCES

[1] I. Chiuchisan, I. Chiuchisan, and M. Dimian, "Internet of Things for e-Health: An approach to medical applications," in *2015 International Workshop on Computational Intelligence for Multimedia Understanding (IWCIM)*, Oct. 2015, pp. 1–5.

[2] H. Lin, J. Shao, C. Zhang, and Y. Fang, "CAM: Cloud-Assisted Privacy Preserving Mobile Health Monitoring," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 6, pp. 985–997, 2013.

[3] H. S. G. Pussewalage and V. Oleshchuk, "A Patient-Centric Attribute Based Access Control Scheme for Secure Sharing of Personal Health Records Using Cloud Computing," in *2016 IEEE 2nd International Conference on Collaboration and Internet Computing (CIC)*, 2016.

[4] R. Zhang and L. Liu, "Security Models and Requirements for Healthcare Application Clouds," in *2010 IEEE 3rd International Conference on Cloud Computing*, Jul. 2010, pp. 268–275.

[5] A. L. Ferrara, G. Fachsbauer, B. Liu, and B. Warinschi, "Policy Privacy in Cryptographic Access Control," in *Computer Security Foundations Symposium (CSF), 2015 IEEE 28th*, Jul. 2015, pp. 46–60.

[6] D. Dolev and A. Yao, "On the security of public key protocols," *IEEE Transactions on Information Theory*, vol. 29, no. 2, pp. 198–208, Mar 1983.

[7] M. Li, S. Yu, K. Ren, and W. Lou, "Securing Personal Health Records in Cloud Computing: Patient-Centric and Fine-Grained Data Access Control in Multi-owner Settings," in *Security and Privacy in Communication Networks*. Springer Berlin Heidelberg, 2010, pp. 89–106.

[8] A. Botta, W. d. Donato, V. Persico, and A. Pescap, "On the Integration of Cloud Computing and Internet of Things," in *2014 International Conference on Future Internet of Things and Cloud*, Aug. 2014.

[9] T. Gong, H. Huang, P. Li, K. Zhang, and H. Jiang, "A Medical Healthcare System for Privacy Protection Based on IoT," in *2015 Seventh International Symposium on Parallel Architectures, Algorithms and Programming (PAAP)*, Dec. 2015, pp. 217–222.

[10] H. Khemissa and D. Tandjaoui, "A Lightweight Authentication Scheme for E-Health Applications in the Context of Internet of Things," in *2015 9th International Conference on Next Generation Mobile Applications, Services and Technologies*, Sep. 2015, pp. 90–95.

[11] J. Li, X. Huang, J. Li, X. Chen, and Y. Xiang, "Securely Outsourcing Attribute-Based Encryption with Checkability," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 8, Aug. 2014.

[12] L. Touati and Y. Challal, "Instantaneous proxy-based key update for cp-abe," in *2016 IEEE 41st Conference on Local Computer Networks (LCN)*, Nov 2016, pp. 591–594.

[13] Q. Huang, Y. Yang, and L. Wang, "Secure data access control with ciphertext update and computation outsourcing in fog computing for internet of things," vol. 5, pp. 12 941–12 950, 2017.

[14] O. Kocabas, T. Soyata, and M. K. Aktas, "Emerging Security Mechanisms for Medical Cyber Physical Systems," *IEEE/ACM transactions on computational biology and bioinformatics*, vol. 13, pp. 401–416, 2016.

[15] S. R. Hemalatha and Manickachezian, "Security Strength of RSA and Attribute Based Encryption for Data Security in Cloud Computing," *International Journal of Innovative Research in Computer and Communication Engineering*, 2014.

[16] F. Guo, Y. Mu, W. Susilo, D. S. Wong, and V. Varadharajan, "CP-ABE With Constant-Size Keys for Lightweight Devices," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 5, pp. 763–771, 2014.

[17] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based Encryption for Fine-grained Access Control of Encrypted Data," in *Proceedings of the 13th ACM Conference on Computer and Communications Security*, ser. CCS '06. New York, NY, USA: ACM, 2006, pp. 89–98.

[18] R. Materese, "Recommendation for Key Management, Part 1: General," Jan. 2016. [Online]. Available: https://www.nist.gov/node/786276

[19] X. Wang, J. Zhang, E. M. Schooler, and M. Ion, "Performance evaluation of Attribute-Based Encryption: Toward data privacy in the IoT," in *2014 IEEE International Conference on Communications (ICC)*, Jun. 2014, pp. 725–730.

[20] M. Ambrosin, M. Conti, and T. Dargahi, "On the Feasibility of Attribute-Based Encryption on Smartphone Devices," in *Proceedings of the 2015 Workshop on IoT Challenges in Mobile and Industrial Systems*. ACM, 2015, pp. 49–54.

[21] K. T. Nguyen, M. Laurent, and N. Oualha, "Survey on secure communication protocols for the Internet of Things," *Ad Hoc Networks*, vol. 32, 2015.

[22] "The AVISPA Project." [Online]. Available: http://www.avispa-project.org/

[23] PBC library - pairing-based cryptography. [Online]. Available: https://crypto.stanford.edu/pbc/

[24] tiny-AES-c: Small portable AES128/192/256 in c. [Online]. Available: https://github.com/kokke/tiny-AES-c

[25] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy Attribute-Based Encryption," in *Proceedings of the 2007 IEEE Symposium on Security and Privacy*, ser. SP '07. Washington, DC, USA: IEEE Computer Society, 2007, pp. 321–334.

[26] Y. Ould Yahia, S. Banerjee, S. Bouzefrane, and H. Boucheneb, "Exploring formal strategy framework for the security in IoT towards e-health context using computational intelgence," in *Internet of Things and Big Data Technologies for Next Generation Healthcare*, ser. Studies in Big Data. Springer International Publishing, 2017, pp. 63–90.