




Article

Granular Data Access Control with a Patient-Centric Policy Update for Healthcare

Fawad Khan ^{1,*} , Saad Khan ², Shahzaib Tahir ¹, Jawad Ahmad ³ , Hasan Tahir ¹  and Syed Aziz Shah ⁴

¹ Department of Information Security, National University of Sciences and Technology, Sector H-12, Islamabad 44000, Pakistan; shahzaib.tahir@mcs.edu.pk (S.T.); hasan.tahir@seecs.edu.pk (H.T.)

² Department of Computer Science & IT, Sarhad University of Science and Information Technology, Peshawar 25000, Pakistan; amlms1.de@suit.edu.pk

³ School of Computing, Edinburgh Napier University, Edinburgh EH11 4BN, UK; J.Ahmad@napier.ac.uk

⁴ Faculty Research Centre for Intelligent Healthcare, Coventry University, Coventry CV1 5FB, UK; syed.shah@coventry.ac.uk

* Correspondence: fawadkhan@mcs.edu.pk

Abstract: Healthcare is a multi-actor environment that requires independent actors to have a different view of the same data, hence leading to different access rights. Ciphertext Policy-Attribute-based Encryption (CP-ABE) provides a one-to-many access control mechanism by defining an attribute's policy over ciphertext. Although, all users satisfying the policy are given access to the same data, this limits its usage in the provision of hierarchical access control and in situations where different users/actors need to have granular access of the data. Moreover, most of the existing CP-ABE schemes either provide static access control or in certain cases the policy update is computationally intensive involving all non-revoked users to actively participate. Aiming to tackle both the challenges, this paper proposes a patient-centric multi message CP-ABE scheme with efficient policy update. Firstly, a general overview of the system architecture implementing the proposed access control mechanism is presented. Thereafter, for enforcing access control a concrete cryptographic construction is proposed and implemented/tested over the physiological data gathered from a healthcare sensor: shimmer sensor. The experiment results reveal that the proposed construction has constant computational cost in both encryption and decryption operations and generates constant size ciphertext for both the original policy and its update parameters. Moreover, the scheme is proven to be selectively secure in the random oracle model under the q-Bilinear Diffie Hellman Exponent (q-BDHE) assumption. Performance analysis of the scheme depicts promising results for practical real-world healthcare applications.

Keywords: multi message; hierarchal; policy update; constant computations; constant size ciphertext



Citation: Khan, F.; Khan, S.; Tahir, S.; Ahmad, J.; Tahir, H.; Shah, S.A. Granular Data Access Control with a Patient-Centric Policy Update for Healthcare. *Sensors* **2021**, *21*, 3556. <https://doi.org/10.3390/s21103556>

Academic Editor: Anthony Fleury

Received: 30 March 2021

Accepted: 13 May 2021

Published: 20 May 2021

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2021 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Cloud is a platform that provides on-demand availability, ubiquitous access to the data and a shared pool of configurable computing resources [1]. The outsourcing of data on the cloud is governed primarily through the principles of data sharing and data management. The benefits that the cloud offers prompt various organizations to outsource their data with reduced security management costs. The organizations and sectors that have already embrace the cloud and further explore its use cases include healthcare, telecommunication, and real-estate. Although the cloud offers many benefits, the remote third-party cloud servers are an active target as hackers may succeed to bypass their security firewalls to get unauthorized access. Even the cloud itself may be malicious and may try to exploit potential vulnerabilities to access the data or grant access to unauthorized users.

Healthcare is a collaborative environment that involves many organizations including pharmaceuticals, hospitals, and insurance companies, and therefore multiple users/multiple actors with different roles are accessing the same resources. Access to a patient's health

record is required for proper diagnosis and prescription [2], insurance claims and data analytics [3]. Since the patients' health data is sensitive in nature and requires proper management to avoid privacy breaches. To be more precise, the access and interaction of multiple users to the same data gives rise to the possibility of data theft. Therefore, the scope of this research is limited to healthcare in which threats related to unauthorized access are prevented through efficient handling of patients' data and access rights by limiting unauthorized data access. To attain these goals, a promising solution is the Ciphertext Policy-Attribute-based Encryption (CP-ABE) [4] which has been considered for enforcing cryptographic access control on data. Using CP-ABE the data owner can enforce an access policy in a ciphertext using attributes, and any user conforming to the policy can access the data. ABE either CP-ABE or Key Policy-ABE (KP-ABE) is a one-to-many access control paradigm, that grants the same data access to multiple sets of users upon successful satisfaction of a policy by them.

In existing healthcare access control schemes [5–9], CP-ABE generates the same data for all users due to the fact that against every message a single ciphertext is generated and all the authorized users can have access to that same data. To elaborate, users satisfying individual attribute sets of a monotonic access policy in CP-ABE have access to the same data. Consider a scenario where doctors from a hospital have access to all the patient's sensitive healthcare data, while the secondary stakeholders consisting of nurses and pharmaceutical firms are restricted to a limited chunk of insensitive data. This granular data access cannot be attained with the conventional CP-ABE mechanisms. Instead, a multi message CP-ABE is required in this context, so that multiple messages, i.e., hierarchically driven keys are encrypted with it for the same data access. More details regarding hierarchical keys derivation is presented Section 6.1. Another limitation of existing healthcare schemes [5–9] is their nature as they are based on single attribute authority, however, in real life attributes can be from multiple stakeholders belonging to different authority domains like hospitals, and universities.

We remark that in the existing health-centric schemes [5–9], the policies are static and predefined. Due to the absence of a policy update feature, CP-ABE cannot be considered as a complete access control enforcement tool. This issue motivates to dynamically increase or decrease the privileges of specific users over certain sets of files. However, if the process of policy update somehow tries to reduce or cancel the access rights of some users over particular attributes, they might refuse an update in their attribute keys to decrypt data even after the policy update. Hence, to address the problem of non-cooperation from users; existing approaches focus to update keys for all unrevoked users in order to update the policy [10]. However, this solution reduces efficiency because the number of revoked attributes is generally a few; therefore, most of the effort is concentrated on unrevoked attributes for a policy update. Moreover, it should not always be the case that attributes are just only revoked from a policy; instead, mechanisms should be developed to cater for both the addition and the revocation of attributes in policy updates. Another issue to be addressed should be that the underlying CP-ABE should have constant computation costs to accommodate the resource-constrained devices. To resolve the above-mentioned issues, our contributions are enlisted below.

1.1. Our Contributions

To simultaneously address the inclusion of hierarchical access control to CP-ABE and to dynamically update the access policy privileges with constant computation costs, this paper makes the following contributions:

- This research gives the notion of Patient-Centric Multi Message Ciphertext Policy-Attribute Based Encryption with Efficient Policy Update (PC-MM-CP-ABE-EPU).
- The proposed construction addresses the inclusion of hierarchical access control to CP-ABE and dynamically updates the access policy with constant computational overhead.

- A comprehensive security and performance analysis of the proposed construction is presented to depict its effectiveness for dynamic access control in healthcare.
- For security, we prove the proposed PC-MM-CP-ABE-EPU scheme to be selectively secure in the random oracle model under the q -Bilinear Diffie Hellman Exponent (q -BDHE) assumption.
- This paper also studies the feasibility of the proposed scheme in the healthcare sector, where a patient can utilize it to specify access rights to his confidential data for doctors, nurses, and insurance companies.
- For performance, real data is generated through a body wearable physiological sensor called the Shimmer [11]. The sensor is embedded with Micro-Electrical Mechanical System (MEMS) and physiological sensing components. The proposed scheme is tested using the data collected via the sensor.

1.2. Paper Organization

Rest of the paper is organized as follows. Section 2 highlights the existing works relating to the evolvement of attribute based encryption in general, and particularly for enforcing access control of data in healthcare. System Architecture is presented in Section 3, which discusses the roles of various actors in healthcare along with data access control policy specification. The preliminary cryptographic definitions, hardness assumptions, and concepts used to define the proposed PC-MM-CP-ABE-EPU scheme is stated in Section 4. The syntax and security model of the proposed PC-MM-CP-ABE-EPU scheme is listed in Section 5. Section 6, details the proposed cryptographic scheme for patient centric access control provision. In Section 7, we present the performance and security analysis of the scheme. Section 8 concludes the paper.

2. Related Work

After the notion of ABE was formalized by Sahai and Water [12], Bethencourt et al. [4] proposed its variant named as CP-ABE. The user decryption keys corresponded to attributes, while ciphertext was related to a policy defined over attributes in CP-ABE. However, the scheme [4] was proven secure in the generic group model. Later, Cheung and Newport [13] proposed a CP-ABE scheme to be secure in the standard model based on AND based access structure. The first decentralized multi authority CP-ABE [14] construction was formalized by Lewko and Water. The notion of multi message CP-ABE for providing access control to scalable media is proposed in [15] by extending the work of [4]. Later, Khan et al. [16] proposed multi message CP-ABE with multiple authorities working in a decentralized manner. However, both the schemes are proven secure in generic group and random oracle model. Zhang et al. [17,18] addressed the user's attributes information leakage issues.

In [19], each attribute has a feature expiry time. Attribute authority updates keys periodically according to this time parameter. Bethencourt et al. [4] comments that the expiry time should vary from one user to another, and be independent of the user's attributes. The authors in [20] introduced the concept of the users list so that even if any particular user satisfies the policy, but is excluded from the authorized list, he cannot have access to data. Further, the idea of the user ID revocation list is presented in [21]. However, both the time and ID based access control methodologies suffer from potential problems i.e., for the system controlling user privilege rights with respect to time needs to define the expiry time during the generation of user attribute decryption keys. Similarly, the authorized ID list needs to be generated along with ciphertext in encryption operation. Hence, any dynamic change of access control cannot be provisioned by employing these concepts. Yang et al. [10,22] proposed the concept of dynamic change of privileges by updating both the ciphertext and user decryption keys in case of attribute revocation. However, the incurred cost for both updating the ciphertext and user keys for non-revoked users is too much for practical considerations. Moreover, as stated in [23], the scheme presented in [22] is not collusion resistant after an update for attribute revocation is performed. Some

other recent works tackling the issue of policy updating, i.e., addition and revocation of attributes are [24–28]. The Linear Secret Sharing Scheme (LSSS) matrix based access structure is employed for ciphertext generation and update policy in [24,25]. Moreover, the scheme in [24] is based on composite order groups and proved to be adaptively secure in standard model. Jiang et al. [26] presented the notions of two constructions separately for both attribute addition and attribute revocation selectively secure under the MSE-DDH assumption. In [27], the authors proposed a threshold policy update based CP-ABE. Sign-cryption based CP-ABE with policy update and outsourced computations is proposed in [28]. However, the computational costs of these schemes [26–28] is much and not suitable for resource-constrained devices. The authors [29] have effectively demonstrated the significance of ABE for resource-constrained IoT devices. Some other enhanced CP-ABE schemes [30] with variant features include attribute based proxy re-encryption [7,31], accountable CP-ABE [32], online/offline CP-ABE [5,7] and outsourced CP-ABE [33].

ABE has been employed in healthcare domain to address concerns relating to resource constrained client [5], doctor centric access control [6] and searchable trapdoor for hospital data [8,9] as seen from Table 1. However, existing schemes failed to grant patients with user-centric access control and policy update features as seen from Table 1. Moreover, all existing schemes are based on a single attribute authority, making it less scalable for autonomous organizations. Also, all existing schemes encrypt only a single message over a policy, thereby limiting the provision of hierarchical access control. All these issues are addressed in our proposed scheme for which we have designed a system architecture along with the cryptographic scheme as discussed in Sections 3 and 6 that can be easily employed in any healthcare facility requiring patient-centric access control. Another similar line of work for health-centric access control provision is Georgakakis et al. [34]. The authors in [34] proposed a generic location and time aware role-based access control mechanism for healthcare. Moreover, in emergency cases, the data access can be provisioned by the proposed “break the glass” notion to allow users to access data that they were not entitled to access under normal conditions. However, the mechanism is generic in nature, and no concrete cryptographic scheme is detailed to enforce access control.

Table 1. Applications of CP-ABE schemes in Healthcare.

Scheme	AA	Security	Feature	PU
[5]	Single	SS-SM under decisional q parallel BDHE	online-offline encryption for resource constrained client	No
[6]	Single	FS-SM under 3 assumptions in composite order group	doctor centric key delegation decryption mechanism	No
[7]	Single	SS-SM under decisional q parallel BDHE, c-BDHE	online-offline attribute based proxy re-encryption	No
[8]	Single	FS-GGM	searchable trapdoor CP-ABE	No
[9]	Single	N/A	searchable trapdoor CP-ABE	No
This Work	Multiple	SS-ROM under q -BDHE	patient-centric CP-ABE with policy update & const costs	Yes

SS: Selective Secure, FS: Fully Secure, SM: Standard Model, GGM: Generic Group Model, BDHE: Bilinear Diffie Hellman Exponent Assumption, PU: Policy Update Feature of CP-ABE, ROM: Random Oracle Model.

3. System Architecture

This section is about the application of the proposed system in healthcare context with the help of a use-case scenario. This use-case presents a model according to which access rights and data security can be managed in a healthcare vicinity. To accomplish the desired objectives, this model is divided into four phases namely, data collection, policy specification/update and data aggregation, outsourced data access control and policy update, and data access whose details are provided below. Following that, the actors like a patient, doctor, professor, and insurance agent, who will use the system for

secure access of data are discussed. Thereafter, core functions of the model including contextual policy specification and its update are explained. Finally, the functionality of other major components of the model involved in the smooth delivery of health facilities including attributes authorities (AA), cloud, and gateway are detailed. Finally, the security requirements that will be achieved by the proposed system are discussed at the end of this section.

In a healthcare scenario, the role of IOT-enabled sensors is pivotal as they help in collecting, retrieving, analyzing, and monitoring patients' medical data in real-time, which eventually helps in dealing with chronic diseases. The proposed system is a novel patient-centric multi-layered model to secure access of data present in semi-trusted servers. The proposed model is a suite of mechanisms, which provides hierarchical access control by considering access control policy defined by patient based on the actor's attributes. It leverages CP-ABE techniques to secure personal health data of patients being outsourced to the cloud and other related servers. Figure 1 depicts the proposed model of PC-MM-CP-ABE-EPU which works in four phases including data collection, policy specification update and data aggregation, outsourced data access control and policy update, and data access provision. The first phase is concerned with data collection from different IoT-enabled sensory devices. The next phase aggregates data at the gateway node. Moreover, access policy along with policy updates have also been specified in this phase. The third phase outsources data being controlled by the access control policy modules to the cloud. The last phase is all about accessing patients' data by doctors, nurses, professors, students and insurance companies. A brief description of the involved actors implementing the above-mentioned functionalities is as follows:

- **Patient:** An entity seeking some medical treatment. This entity is responsible for encrypting data and defining/updating policy. For this, the patient executes Encrypt and Policy Update algorithms of PC-MM-CP-ABE-EPU, which are detailed in Section 6.2, and can be from Figure 1.
- **Doctor:** A medical practitioner providing general treatment.
- **Nurse:** A clinical personnel providing treatment and care to patients.
- **Professor:** An individual accessing medical data for research and development.
- **Student:** An entity requesting access to a subset of patient data for research.
- **Insurance company:** It assists patients in covering health expenses.
- **Insurance agent:** It assists patients by offering different healthcare plans based on their health condition and income.

In order to access the patient's data, all other actors except patient execute the Decrypt algorithm of PC-MM-CP-ABE-EPU, which are detailed in Section 6.2, and can be from Figure 1. Actors within a system require special access to the resources. For instance, doctors and nurses attending a particular patient may require access to the IOT-enabled sensors attached to it. Such access is generated based on the attributes of the actor. A cardiologist may entail access to heart monitors or ECG sensors only, while a neurologist acquires Electromyography (EMG), accelerometers, and gyroscopes. Hence, in the case of the proposed model, access would be granted based on the attributes of doctors and nurses. Since the proposed model provides hierarchical access control, therefore, the entities lower in privileges or hierarchy would have fewer rights in comparison to its parent. For instance, a nurse can access limited resources. Considering a scenario where a patient shares his specific data among the various actors including doctor, nurse and professor with the policy defined as $(Hospital \wedge Doctor) \vee (Hospital \wedge Nurse) \vee (University \wedge Professor)$. Later, the patient decides to allow the student at the university to have access to data for research purposes, and to an insurance agent for claims regarding his medical expenditure. The updated version of the policy is $(Hospital \wedge Doctor) \vee (Hospital \wedge Nurse) \vee (University \wedge Professor) \vee (University \wedge Student) \vee (Insurance-company \wedge Insurance-agent)$. Consider a scenario where doctors from a hospital have access to all the patient's sensitive healthcare data, while the secondary stakeholders consisting of pharmaceutical firms, insurance companies and government are restricted to a limited

chunk of insensitive data. This model is based on the concept of hierarchical access control, which means that each entity will acquire data based on its hierarchical position in the network. As shown in Figure 1 doctor can access all sensors of patient whereas nurse can only access 2, 4, and 5. It is because the nurse is lower in the hierarchy in terms of access privileges, and the patient has limited his access rights to certain specific sensors data only. Since the doctor is on top of hierarchy so he can easily view information accessible to his subordinates.

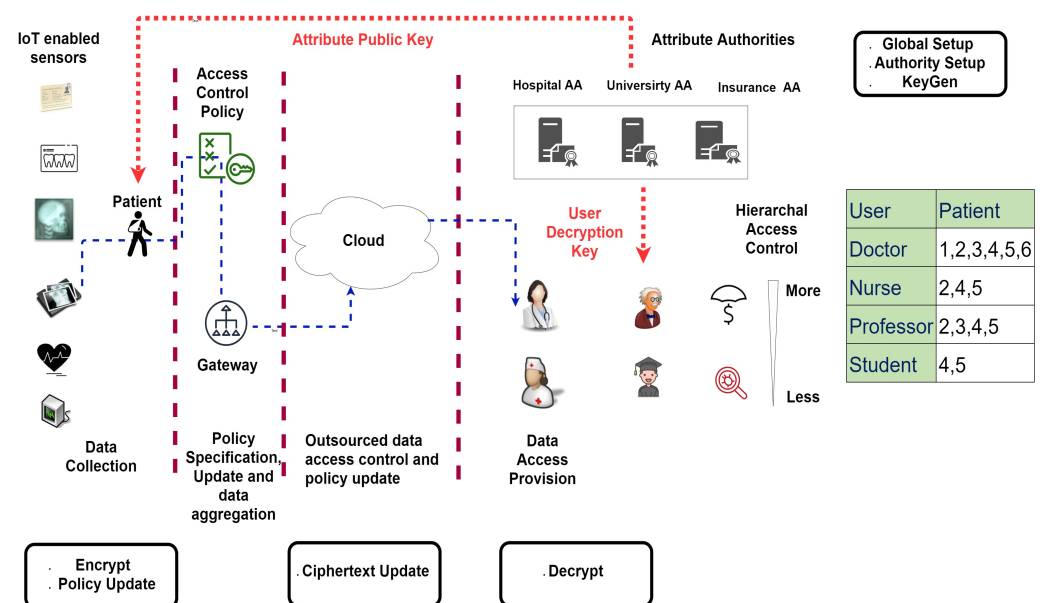


Figure 1. System Model of PC-MM-CP-ABE-EPU.

Apart from actors, other major components of the model involved in the smooth delivery of health facilities include attributes authorities (AA), cloud, and gateway whose major tasks are discussed below.

- **Attribute Authority:** It is an entity that generates the public key parameters for contextual attributes (like for doctor and nurse), and assign decryption keys to user's based on their Global Identifiers (GID) and possessed attributes. All the attribute authorities, like Hospital AA, University AA, Insurance Company AA works in a decentralized manner. The algorithms of PC-MM-CP-ABE-EPU including the Global Setup, Authority Setup, and KeyGen are executed at AA as seen from Figure 1, and are detailed in Section 6.2.
- **Gateway:** It acts as a trusted relay node to the cloud server with the help of a backbone network. The devices transmit generated data to the gateway.
- **Cloud server:** The cloud server is a semi-trusted entity possessing great storage capacities and high computing power. It aims at storing a volume of encrypted data collected from several devices. The algorithm of PC-MM-CP-ABE-EPU namely Ciphertext Update is executed by Cloud as seen from Figure 1, and is detailed in Section 6.2.
- **IoT enabled sensors:** These sensors are connected with the human body and collect biomedical data of patients. Some of these sensors include ECG, blood pressure, EEG, blood glucose, or pulse oximetry. Such sensors transmit biomedical data of patients to device, which will eventually be transmitted to the cloud.
- **Device:** A device with the help of its built-in sensors is efficient enough to sense, process, and communicate data being generated. Due to these capabilities, different objects can be inter-connected over the network. These devices produce and dispense data to the gateway through a wireless communication medium. Since such data is sensitive in nature, so to assure its confidentiality, it is essential for constrained devices to encrypt it.

The flow of activities of the proposed model is exhibited in Figure 2. However, this model is based on some assumptions. Firstly, the attribute authorities are reliable entities, which can be fully trusted. Secondly, gateway and cloud are honest bodies but are curious. The gateway does not connive with the unauthorized receiver. Cloud will follow the protocol run, but it will try to infer and analyze the encrypted data placed over it. The cloud is considered as an adversary, but we will prove in the security proof, that the challenge ciphertext will be indistinguishable from the perspective of the adversary before and after ciphertext update. The proposed model covers the following aspects of security requirements.

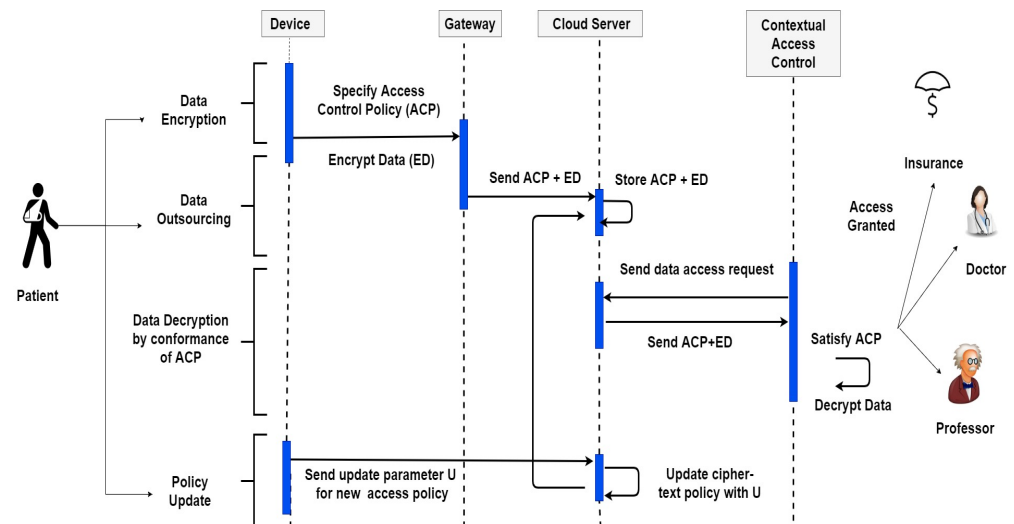


Figure 2. Flow Diagram of Access Control Actions.

- **Confidentiality and scalability:** As the data produced by the devices contain critical content, therefore it should be kept secured and protected from unauthorized entities and cloud servers. Moreover, the proposed model should be flexible enough to accommodate a large group of authorized users accessing their data.
- **Fine-grained access control:** The senders should define an access control policy for the transmitted data, which can be decrypted by the receivers possessing accurate attribute keys that comply with the access policy in the ciphertext.
- **Collusion resistance:** As the devices and applications accessing the system are not trusted, therefore it is significant to ensure that two or more receivers cannot access data by integrating their attribute keys which they can't access separately.
- **Secure policy updating:** The algorithm supporting policy update of ciphertext should never disclose critical information to the cloud server.

4. Preliminaries

In this section, we detail the definitions of Bilinear Pairing, q -BDHE hardness assumption, and access policy which is used to define a PC-MM-CP-ABE-EPU scheme in the forthcoming sections.

Definition 1. Bilinear Pairing Let G be a multiplicative cyclic group of large prime order p' , where generator $g \in_R G$, and G_T is multiplicative cyclic group of same order with its identity denoted by 1. Then, a bilinear pairing $e : G \times G \rightarrow G_T$ is a map with following properties:

1. **Bilinear:** $e(g^x, g^y) = e(g, g)^{xy} \forall x, y \in \mathbb{Z}_p$.
2. **Non-Degenerate:** There exists $g_1, g_2 \in G$ such that $e(g_1, g_2) \neq 1$.
3. **Computable:** Existence of an efficient algorithm to compute $e(g_1, g_2) \forall g_1, g_2 \in G$.

Definition 2. q -BDHE [35] Consider a bilinear group G of prime order p having two independent generators g and h selected at random from it. We represent $y_{g,h,q} = (g, g_1, g_2, \dots, g_q, g_{q+2},$

$, \dots, g_{2q}) \in G^{2q-1}$ for $g_i = g^{\alpha^i}$ for an unknown random $\alpha \in Z_p^*$. An algorithm \mathcal{B} which randomly selects $\beta = \{0, 1\}$ has advantage ϵ of solving the q -BDHE problem if $|\Pr[\mathcal{B}(g, h, y_{g,\alpha,q}, e(g_{q+1}, h) = 1)] - |\Pr[\mathcal{B}(g, h, y_{g,\alpha,q}, T = 1)]| \geq \epsilon$.

Definition 3. Access Policy A Disjunctive Normal Form (DNF) policy W , namely a ciphertext policy for CP-ABE is a rule that returns either 0 or 1 given a set L of attributes. We say that L satisfies W if and only if W answers 1 on L . We use the notation $L \models W$ to denote the fact that L satisfies W , and the case of L does not satisfy W is represented by $L \not\models W$. Formally, given an access policy $W = [W_1, W_2, \dots, W_{p'}] = \bigvee_{i \in I_W} W_i$, where $I_W = \{i | 1 \leq i \leq p'\}$ is a subscript index set of W . Moreover, for $1 \leq i \leq p'$ each of $W_i = [v_1, v_2, \dots, v_m] = \bigwedge_{j \in I_X} v_j$, where $I_X = \{j | 1 \leq j \leq m\}$ is a subscript index set of W_i . Given a user attribute list $L = [L_1, L_2, \dots, L_m]$, we say that $L \models W$ if $L_j = v_j$ for any one attribute set W_i of W for $1 \leq i \leq p'$, and for all $1 \leq j \leq m$.

5. Syntax and Security Model

This section details the syntax and security model of our proposed scheme. Notations used throughout the paper are listed in Table 2.

Table 2. Notations.

Symbol	Description
p	Bilinear group order
p'	Maximum number of attribute sets
W_i	A particular attribute set of policy
m	Number of attributes within an attribute set W_i
n	Total number of attributes in the access structure
W	Ciphertext Policy comprising of several W_i
L	User attribute set consisting of various attributes
$L \models W$	User attribute set satisfying policy
$L \not\models W$	User attribute set not satisfying policy
W'	Attributes for policy update
W^u	Updated Policy
GID	Global Identifier
S_{owner}	Owner secret t_i for setting access access control
\mathcal{U}	Policy update parameter
$IND - sCPA$	Indistinguishability under selective CPA

5.1. Syntax of PC-MM-CP-ABE-EPU

In this subsection, the algorithms that are part of Patient-Centric multi message CP-ABE with efficient policy update (PC-MM-CP-ABE-EPU) are discussed. Here, we detail only the syntax of the algorithms, the concrete cryptographic construction is presented in Section 6. Referring to Figure 1 in Section 3, the algorithms Global Setup, Authority Setup, KeyGen are executed by attribute authorities, Encrypt and Policy Update is executed by Patient, Ciphertext Update by Cloud, and Decrypt by contextual users like a doctor, nurse, and professor.

Global Setup(λ) $\rightarrow GP$: Taking the security parameter λ as input, the algorithm outputs the global parameters GP of system.

Authority Setup(GP) $\rightarrow SK, PK$: Taking GP as input, each authority generates a secret key SK and public key PK corresponding to the attribute belonging to the authority. This algorithm is executed at each attribute authority, i.e, hospital AA, and university AA.

Encrypt(M_i, W, PK) $\rightarrow CT$: Taking PK and an access policy $W = [W_1 \text{ OR } W_2 \text{ OR } \dots \text{ OR } W_{p'}]$ as input; the algorithm encrypts each message M_i correspondingly with attribute set W_i of policy for $1 \leq i \leq p'$ to output a ciphertext CT . This algorithm is executed by patient.

KeyGen(GID, PK, L, x, SK) $\rightarrow K_{x,GID}$: A user with a global identifier GID has an attribute set L , where $x \in L$. This algorithm generates a key $K_{x,GID}$ corresponding to an attribute x and identity GID of user. This algorithm is executed at each AA.

Decrypt($CT, PK, L, K_{x,GID}$) $\rightarrow M_i$: Taking the ciphertext and user attribute key set L as input, the algorithm outputs a message M_i corresponding to attribute set W_i of policy W ; if $L \models W$. This algorithm is executed by the user's with contextual attributes like doctor, nurse, professor, and insurance agent.

Policy Update(PK, S_{owner}, W, W') $\rightarrow \mathcal{U}$: The algorithm outputs the update parameter \mathcal{U} by taking as input the original policy W , update in policy W' , PK and owner secret S_{owner} embedded in ciphertext during encryption. This algorithm is executed by patient for updating the access control policy.

Ciphertext Update(CT, \mathcal{U}) $\rightarrow CT'$: The algorithm outputs the updated ciphertext CT' by taking as input the original CT and ciphertext update \mathcal{U} parameter. This algorithm is executed at cloud.

5.2. Formalized Security Model

In this section, we present the security model for proving our cryptosystem. The detailed security proof is in Section 7.1. We consider the following indistinguishability game under selective chosen-plaintext-attacks ($IND - sCPA$) between an adversary \mathcal{A} and challenger \mathcal{C} for PC-MM-CP-ABE-EPU scheme. **Init**

Adversary specifies and sends a challenge access policy structure W^* to \mathcal{C} .

Setup \mathcal{C} runs the global and authority setup algorithms to generate the global parameters GP and secret/public keys of attributes. It then gives the public keys and GP to \mathcal{A} .

Phase 1 \mathcal{A} queries for the secret keys by providing an attribute list L and identities GID . \mathcal{C} replies with secret keys if L does not satisfy W^* .

Challenge \mathcal{A} specifies two distinct equal length messages ($M_{0,i} \neq M_{1,i}$) correspondingly for each attribute set W_i^* in policy W^* and an update parameter \mathcal{U}^* . In response, \mathcal{C} chooses bit $\beta = \{0, 1\}$ at random, computes $CT^* = \mathbf{Encrypt}(M_{\beta,i}, W^*, GP, PK)$, and sends it to \mathcal{A} if $\mathcal{U}^* = \emptyset$. Otherwise, it sends $CT' = \mathbf{Update}(CT^*, \mathcal{U}^*)$ to \mathcal{A} .

Phase 2 \mathcal{A} continues to query for secret keys under the same constraint that the access structure W^* should not be violated.

Guess \mathcal{A} outputs a guess β' for β and wins the game if $\beta' = \beta$. Advantage of \mathcal{A} in winning the $IND-sCPA$ game is

$$Adv_{PC-MM-CP-ABE-EPU}^{IND-sCPA}(\mathcal{A}) = |Pr[\beta' = \beta] - \frac{1}{2}|$$

6. Proposed Scheme

In this section, firstly we discuss the intuition behind the multi message CP-ABE and hierarchical access control provision in Section 6.1, and later in Section 6.2 we detail a concrete cryptographic construction for enforcing patient centric access control.

6.1. Methodology

To illustrate our idea, we begin with a simple example of monotone policy and then further extend it to define our intuition. A monotone access policy in its Disjunctive Normal Form (DNF) representation itself contains the individual AND (\wedge) based access structures. Hence, combination of AND (\wedge) based access policy [35,36] by placing OR between them itself leads to an expressive monotone access policy [13]. Consider a patient-centric policy as $W = (\text{Hospital-1} \wedge \text{Doctor}) \text{ OR } (\text{Hospital-1} \wedge \text{Nurse}) \text{ OR } (\text{University-1} \wedge \text{Professor}) \text{ OR } (\text{University-1} \wedge \text{Student}) \text{ OR } (\text{Insurance company-1} \wedge \text{Insurance-agent})$. This policy $W = [W_1 \text{ OR } W_2 \text{ OR } W_3 \text{ OR } W_4 \text{ OR } W_5]$ is comprised of 5 attribute sets namely, $W_1 = (\text{Hospital-1}, \text{Doctor})$, $W_2 = (\text{Hospital-1}, \text{Nurse})$, $W_3 = (\text{University-1}, \text{Professor})$, $W_4 = (\text{University-1}, \text{Student})$, $W_5 = (\text{Insurance company-1}, \text{Insurance-agent})$. Any user conforming to the policy ($L \models W$) needs to satisfy at least one attribute set W_i of policy for $i = \{1, 2, 3, 4, 5\}$. A user attribute set L satisfies policy $L \models W$ if $W_i \subset L$ [37], i.e., any attribute set W_i of policy should be the subset of user attribute set L .

For further elaboration, Table 3 indicates five arbitrary user's along with their attribute sets L indicating whether or not they satisfy the policy W .

Suppose after sometime, the patient updates the policy W into W^u as $W^u = (\text{Hospital-1} \wedge \text{Doctor}) \text{ OR } (\text{Hospital-1} \wedge \text{ENT} \wedge \text{Nurse}) \text{ OR } (\text{University-2} \wedge \text{Professor}) \text{ OR } (\text{University-2} \wedge \text{Student})$. After policy update, some contextual user's who were previously granted data access cannot access data after policy update.

For updating the policy, the data owner generates an update parameter \mathcal{U} comprising of attributes that needs to be added or revoked from an existing attribute set W_i of policy W . Secret t_i values corresponding to W_i which were embedded in CT are utilized by data owner for generating the update parameter. Hence, an owner needs to keep a record of secret t_i values for policy updates in the future. The update \mathcal{U} is sent to the server, and it runs the update algorithm for updating CT corresponding to new policy. However, the server cannot exploit both \mathcal{U} and CT to get more information. Moreover, if any user satisfying the policy prior to its update has not decrypted CT ; so he will also not be able to decrypt it after update if now he does not satisfy the new policy.

Table 3. Users satisfying policy and access type (Partial/Full).

U	User Attribute Set L	$L \models W$	$L \models W^u$	DA
1	Doctor, Hospital-1, Clinic-X	Yes	Yes	F
2	Nurse, Hospital-2	No	No	P
3	Professor, University-1, University-2	Yes	Yes	F
4	Insurance-comp-1, Insurance-agent	Yes	No	F
5	Student, University-1	Yes	No	P

U: User, DA: Data Access, P: Partial, F: Full.

In traditional CP-ABE schemes [4,13,35,36] a single message is embedded into a ciphertext for all the attribute sets W_i of policy. So, all users satisfying any individual W_i of policy leads to the same secret “ s ” re-construction, and hence have access to the same data. However, this cannot be adopted in the provision of hierarchal access control because there is a need to embed multiple messages in a single ciphertext over policy. To cater, we embed multiple secrets t_i corresponding to attribute sets W_i of policy W for encrypting multiple messages. This enables users satisfying any different W_i to have access to different granularities of data. For enforcing hierarchal access control, data needs to be divided logically into chunks $m_1, m_2, \dots, m_{p'}$ and each chunk encrypted with hierarchically derived key [15,38–40]. In this technique, several chunk keys are obtained from parent-node key such that key derivation follows the top-down (1-way) approach, i.e., from the parent node to descendant child-nodes. We detail the hash based key derivation [15].

The key k_i generation corresponding to the i^{th} level of hierarchy is proceeded as:

$$k_i = H(k_{i+1}||i) \quad \text{for } i = p' - 1, \dots, 3, 2, 1$$

For generating p number of chunk keys at the same hierarchical level from key k is proceeded as:

$$k_i = H(k||i) \quad \text{for } i = 1, 2, 3, \dots, p'$$

where H is a standard one-way hash function. Table 3 depicts the granular data access control that doctor and professor have access to all data. However, student and nurse are restricted to a limited proportion of logical data as specified by the patient.

6.2. PC-MM-CP-ABE-EPU

In this subsection, we present our proposed Patient-Centric Multi Message Ciphertext Policy-Attribute Based Encryption with Efficient Policy Update (PC-MM-CP-ABE-EPU). We assume that there exist u attributes in the universe. Formally, in encryption, the public keys of involved attributes are aggregated to form a single attribute. Similarly, the decryption process includes an aggregation of user attribute keys satisfying policy. Hence, the construction leads to constant computational cost in encryption and decryption and

is independent of the number of attributes. Moreover, each user has a unique identity by mapping its GID to a random group element, thereby restricting users to collude their attribute keys. To construct multi-message CP-ABE in a single ciphertext over policy, multiple secrets corresponding to different attribute sets of policy are embedded in ciphertext; in-contrast to a single secret for traditional CP-ABE schemes. Moreover, data owner acts as an enforcer of policy updates, while the server updates the ciphertext. For policy update, i.e., the addition or revocation of attributes; data owner generates the update parameter requiring only 2 exponential group operations on its side, while a single multiplication of group elements is performed at the server side.

The algorithms of the proposed scheme is defined as:

Global Setup(λ) $\rightarrow GP$: In global setup, a bilinear group G of prime order p is chosen. Global parameters are set to $p, g, e(g, g)$ and H ; where g is a generator of group G and H is a hash function that maps global identities GID to elements in G .

Authority Setup(GP) $\rightarrow SK, PK$: For every attribute x that belongs to an authority, it chooses two random values $a_x, b_x \in Z_p$. It sets secret key as $SK = \{a_x, b_x \in Z_p\}$ and publishes public key as $PK = \{g^{-a_x}, e(g, g)^{b_x}\}$.

Encrypt(M_i, W, PK) $\rightarrow CT$: Data owner defines an access policy $W = [W_1 \text{ OR } W_2 \text{ OR} \dots \text{OR } W_{p'}]$, where W_i for $i = 1$ to p' corresponds to an attribute set in policy. All the attributes within an attribute set W_i have an AND operation between them stating the significance that all of them must be present for satisfaction of policy. For enforcing hierarchical (different) access control corresponding to different W_i of policy, data owner divides the data logically into chunks, where each data chunk M_i is encrypted with hierarchically derived key k_i for $1 \leq i \leq p'$ as illustrated in Section 6.1.

For notational simplicity, we represent keys k_i with messages M_i in the rest of the paper. For each message M_i corresponding to each attribute set W_i of policy it chooses a random owner secret $S_{owner} = t_i \in Z_p$. After then, it aggregates the PK of attributes from relevant authorities belonging to each W_i and computes the ciphertext as:

$$C_{1,i} = g^{t_i}, C_{2,i} = \left(\prod_{x \in W_i} g^{-a_x} \right)^{t_i}, C_{3,i} = M_i * \left(\prod_{x \in W_i} e(g, g)^{b_x} \right)^{t_i}$$

The owner then sends $CT = \{W, C_{1,i}, C_{2,i}, C_{3,i}\}$ for $1 \leq i \leq p'$ to the server.

KeyGen(GID, PK, x, SK) $\rightarrow K_{x,GID}$: To create a key for user GID corresponding to an attribute x of authority, the authority computes:

$$K_{x,GID} = g^{b_x} \cdot H(GID)^{a_x}$$

We remark that any user with a global identifier GID has an attribute set L , where $x \in L$, and a user can have more than one attributes keys based on his attributes in set L .

Decrypt($CT, PK, L, K_{x,GID}$) $\rightarrow M_i$: If user attribute set L satisfies the condition $W_i \subset L$ for an attribute set W_i in policy W ; then he satisfies the policy $L \models W$ and proceeds by calculating the aggregated key as $K = \prod_{x \in W_i} K_{x,GID}$. To retrieve plaintext message M_i for corresponding W_i , user computes:

$$C_{3,i} / e(H(GID), C_{2,i}) * e(K, C_{1,i}) = M_i$$

Policy Update(PK, S_{owner}, W, W') $\rightarrow U$: For policy update, it takes $W' = [W'_1 \text{ OR } W'_2 \text{ OR} \dots \text{OR } W'_{p'}]$; where W'_i contains the list of attributes to be added or revoked from the particular attribute set W_i in original policy W . Intuitively, the addition of attributes is performed when $W'_i \cap W_i = \emptyset$ resulting in an updated attribute set policy as $W_i^u = W'_i \cup W_i$. Similarly, for attribute revocation the condition $W'_i \subset W_i$ needs to be satisfied resulting in an updated policy as $W_i^u = W_i \setminus W'_i$ correspondingly for a particular attribute set in W for $i = \{1, 2, \dots, p'\}$. Moreover, it takes the product of public keys PK and sets the parameters

$$u_{1,i} = \left(\prod_{x \in W'_i} g^{-a_x} \right)^o, \quad u_{2,i} = \left(\prod_{x \in W'_i} e(g, g)^{b_x} \right)^o$$

correspondingly for attributes addition or revocation from an existing attribute set W_i . For performing the addition of attributes data owner sets o to $S_{owner} = t_i$; while for revocation of attributes it sets o as $-S_{owner} = -t_i$. Data owner then sets the update parameter as $\mathcal{U} = \{W_i^u, u_{1,i}, u_{2,i}\}$ where W_i^u contains the updated list of attributes after addition or revocation of attributes from the particular attribute set W_i in original policy W .

Ciphertext Update(CT, \mathcal{U}) $\rightarrow CT'$: This algorithm takes as input the original CT and update parameter $\mathcal{U} = \{W_i^u, u_{1,i}, u_{2,i}\}$. For policy update, it takes the parameters $u_{1,i}, u_{2,i}$ and multiply them correspondingly by original ciphertext CT components $C_{2,i}, C_{3,i}$ for a particular W_i for $i = \{1, 2, \dots, p'\}$ as

$$C'_{2,i} = C_{2,i} \cdot u_{1,i}, C'_{3,i} = C_{3,i} \cdot u_{2,i}$$

to obtain the updated ciphertext $CT' = \{W^u, C_{1,i}, C'_{2,i}, C'_{3,i}\}$ for the updated policy. Observe that, the distribution of CT' is similar to CT .

6.3. Correctness Decryption

In this subsection, we prove the correctness of the decryption algorithm.

$$\frac{C_{3,i}}{e(H(GID), C_{2,i}) * e(K, C_{1,i})} \cdot \frac{M_i * (\prod_{x \in W_i} e(g, g)^{b_x})^{t_i}}{e(H(GID), (\prod_{x \in W_i} g^{-ax})^{t_i}) * e(\prod_{x \in W_i} g^{b_x} H(GID)^{ax}, g^{t_i})} = M_i$$

6.4. Correctness Policy Update

For attribute's addition, $o = t_i$, hence updated policy is $W_i^u = W_i' \cup W_i$, and the shares of newly added attributes is aggregated to already present attributes to transform the final ciphertext policy as: $C'_{2,i} = \prod_{x \in W_i^u} g^{-ax}^{t_i}, C'_{3,i} = M_i * (\prod_{x \in W_i^u} e(g, g)^{b_x})^{t_i}$. For attribute's revocation, $o = -t_i$, hence updated policy is $W_i^u = W_i \setminus W_i'$, and the shares of revoked attributes are cancelled out (due to negative/negation operation) from already present attributes to transform the final ciphertext policy as: $C'_{2,i} = \prod_{x \in W_i^u} g^{-ax}^{t_i}, C'_{3,i} = M_i * (\prod_{x \in W_i^u} e(g, g)^{b_x})^{t_i}$. We remark that the updated ciphertext is similar to (in form) and indistinguishable from the original ciphertext in policy.

$$C'_{2,i} = C_{2,i} \cdot u_{1,i} = \left(\prod_{x \in W_i} g^{-ax} \right)^{t_i} \cdot \left(\prod_{x \in W_i'} g^{-ax} \right)^o$$

$$C'_{3,i} = C_{3,i} \cdot u_{2,i} = M_i * \left(\prod_{x \in W_i} e(g, g)^{b_x} \right)^{t_i} \cdot \left(\prod_{x \in W_i'} e(g, g)^{b_x} \right)^o$$

7. Analysis and Discussion

Security and performance are the two major metrics that need to be evaluated from the prospect of any secure and efficient cryptographic scheme. This section, therefore, discusses the security and performance of the proposed scheme with the help of security proof and experimentations.

7.1. Security

With reference to the security model presented in Section 5.2, here we prove the following theorem to exhibit the security of the proposed scheme.

Theorem 1. *We show that the proposed PC-MM-CP-ABE-EPU scheme is selectively secure under chosen-plaintext-attacks (IND-sCPA) by a game played between an adversary A and challenger C as described in Section 5.2.*

Proof of Theorem 1. We suppose the existence of an adversary \mathcal{A} to break the proposed construction with a non-negligible advantage. We thus build a simulator \mathcal{B} to interact with \mathcal{A} in the IND-sCPA game; where \mathcal{B} plays the role of challenger, and has an advantage ϵ to solve q-BDHE problem in group G . Suppose challenger inputs a q-BDHE instance $(g, h = g^s, y_{g,\alpha,q}, T)$ for a single encrypted message, where $y_{g,\alpha,q} = (g, g_1, g_2, \dots, g_q, g_{q+2}, \dots, g_{2q})$ for $g_i = g^{\alpha^i}$ where $\alpha \in Z_p^*$.

We consider a slight modification in q-BDHE instance where $h_i = g^{t_i}$ for different attribute sets W_i in policy W instead of $h = g^s$ for a single challenged attribute set in policy. Now, challenger inputs a modified q-BDHE instance $(g, h_i = g^{t_i}, y_{g,\alpha,q}, T_i)$. Infact, in the proof \mathcal{B} encrypts messages $M_{\beta,i}$ for all the different attributes sets W_i^* in the challenged access structure W^* .

Init \mathcal{A} specifies and sends a challenge access structure $W^* = [W_1, W_2, \dots, W_{p'}]$ to \mathcal{B} .

Setup \mathcal{B} selects randomly $j^* \in_R I_{X_i}$ for every attribute set W_i^* , where $I_{X_i} = \{1, 2, \dots, m\}$ is the index of the attributes appearing in W_i^* . \mathcal{B} picks $a_{j^*}, c_{j^*} \in_R Z_p$ for each $j^* \in_R I_{X_i}$, and $a_j, c_j \in_R Z_p$ for $k = \{1, 2, \dots, n\}$. We remind here, that all attribute authorities are working in a decentralized fashion, and all attribute authorities work in a similar fashion for parameters generation. Here, challenger acts on behalf of authorities to generate parameters. For setting the public parameters correspondingly for each attribute authority, \mathcal{B} proceeds as:

1. if $j = j^*$, then $(A_j, B_j) = (g^{-a_{j^*}} \prod_{j \in I_{X_i} - \{j^*\}} g_{q+1-j}, e(g, g)^{c_{j^*}} e(g, g)^{\alpha^{q+1}})$
2. if $j \in I_{X_i} - \{j^*\}$, then $(A_j, B_j) = (g^{-a_j} g_{q+1-j}^{-1}, e(g, g)^{c_j})$
3. if $j \notin I_{X_i}$, then $(A_j, B_j) = (g^{-a_j}, e(g, g)^{b_j})$

\mathcal{B} then sends public key (A_j, B_j) to \mathcal{A} for the all attributes belonging to different authorities.

Phase 1 \mathcal{A} submits the several key queries corresponding to particular GID and an attributes set L of his choice. Generally, for such queries we assume that there should be at-least one attribute $att_x \in L$ for which the key query cannot be made, such that $L \neq W_i^*$. Particularly, the constraint is that the set L should not satisfy any of attribute sets W_i^* in policy. In response, \mathcal{B} responds by selecting $z \in_R Z_p$ and sets $H(GID) = g_j g^z$. Further, it sets the decryption keys correspondingly for attributes belonging to different authorities. For each authority, \mathcal{B} sets the keys as:

1. if $j = j^*$, then $K_{j,GID} = (g_j)^{a_j} g^{c_j} (\prod_{j \in I_{X_i} - \{j^*\}} g_{q+1-j+j^*}^{-1}) (B_j)^{-z}$
2. if $j \in I_{X_i} - \{j^*\}$, then $K_{j,GID} = (g_j)^{a_j} g^{c_j} g_{q+1-j+j^*} (B_j)^{-z}$
3. if $j \notin I_{X_i}$, then $K_{j,GID} = (g_j g^z)^{a_j} g^{b_j}$

Finally, \mathcal{B} returns the keys $K_{j,GID}$ to \mathcal{A} for particular identities GID and user queried attribute set L .

Challenge In this phase, \mathcal{A} submits two distinct equal length messages $(M_{0,i} \neq M_{1,i})$ correspondingly for each attribute set W_i^* specified in policy W^* and an update parameter \mathcal{U}^* to \mathcal{B} . Simulator responds by setting $a_{1,i}$ and $c_{1,i}$; as $a_{1,i} = \sum_{j=1}^m a_j$ and $c_{1,i} = \sum_{j=1}^m c_j$. Then, \mathcal{B} chooses $\beta \in_R \{0, 1\}$ and calculates the ciphertext CT^* for the entire policy W^* . Moreover, accordingly to update parameter \mathcal{U}^* , it updates and sets the ciphertext CT' as:

$$C'_{1,i} = h_i = g^{t_i},$$

$$C'_{2,i} = (\prod_{j \in W_i} g^{-a_j})^{t_i} = h_i^{-a'_{1,i}},$$

$$C'_{3,i} = M_{\beta,i} \cdot (\prod_{j \in W_i} e(g, g)^{b_j})^{t_i} = M_{\beta,i} \cdot e(g_{q+1}, h_i) \cdot e(g, h_i)^{c'_{1,i}}$$

\mathcal{B} sends the ciphertext CT' to \mathcal{A} .

Phase 2 Similar to Phase 1.

Guess \mathcal{A} outputs a guess β' for β . For $\beta' = \beta$, \mathcal{B} outputs $v' = 0$, and vice-versa for other case.

Probability Analysis Given a q-BDHE instance $(g, h_i = g^{t_i}, y_{g,\alpha,q}, T_i)$ to \mathcal{B} , and an \mathcal{A} breaks our PC-MM-CP-ABE-EPU with advantage ϵ . Then we present the analysis of two cases below.

Case 1 ($\mathcal{U}^* = \emptyset$) In this case when there is no policy update, \mathcal{B} sets the ciphertext CT^* as:

$$\begin{aligned} C_{1,i}^* &= h_i = g^{t_i} \\ C_{2,i}^* &= (\prod_{j \in W_i} g^{-a_j})^{t_i} = (g^{-a_{j^*}} \prod_{j \in I_{X_i} - \{j^*\}} g_{q+1-j} \cdot \prod_{j \in I_{X_i} - \{j^*\}} g^{-a_j} g_{q+1-j}^{-1})^{t_i} = h_i^{-a_{t_i}} \\ C_{3,i}^* &= M_{\beta,i} \cdot (\prod_{j \in W_i} e(g, g)^{b_j})^{t_i} = M_{\beta,i} \cdot e(g, g)^{c_{j^*} + \alpha^{q+1}} \prod_{j \in I_{X_i} - \{j^*\}} e(g, g)^{c_j} \\ &= M_{\beta,i} \cdot e(g_{q+1}, h_i) \cdot e(g, h_i)^{c_{t_i}} \end{aligned}$$

We note that ciphertext $CT^* = \{C_{1,i}^*, C_{2,i}^*, C_{3,i}^*\}$ is a valid encryption of message $M_{\beta,i}$ if $T_i = e(g_{q+1}, h_i)$; otherwise, if it a random group element, i.e., $T_i \in G_T$, then CT^* is independent of β in \mathcal{A} view. For $v' = 0$, the ciphertext CT^* is valid and T_i is set as $e(g_{q+1}, h_i)$. \mathcal{A} can guess correct β' with a non-negligible advantage defined by $Pr[\beta' = \beta | v' = 0] = \frac{1}{2} + \epsilon$. For $v' = 1$, $T_i \in G_T$, CT^* cannot be identified and we have $Pr[\beta' \neq \beta | v' = 1] = \frac{1}{2}$. From the analysis, the probability with which \mathcal{B} succeeds in breaking the q-BDHE assumption is: $\frac{1}{2}Pr[\beta' = \beta | v' = 0] + \frac{1}{2}Pr[\beta' \neq \beta | v' = 1] = \frac{1}{2} + \frac{\epsilon}{2}$.

Case 2 ($\mathcal{U}^* = (att_1, att_2, \dots, m') \neq \emptyset$) In the case, when the \mathcal{A} has requested for a policy update, \mathcal{B} proceeds by first calculating the CT^* as above.

$$\begin{aligned} C_{1,i}^* &= h_i = g^{t_i} \\ C_{2,i}^* &= (\prod_{j \in W_i} g^{-a_j})^{t_i} = (g^{-a_{j^*}} \prod_{j \in I_{X_i} - \{j^*\}} g_{q+1-j} \cdot \prod_{j \in I_{X_i} - \{j^*\}} g^{-a_j} g_{q+1-j}^{-1})^{t_i} = h_i^{-a_{t_i}} \\ C_{3,i}^* &= M_{\beta,i} \cdot (\prod_{j \in W_i} e(g, g)^{b_j})^{t_i} = M_{\beta,i} \cdot e(g, g)^{c_{j^*} + \alpha^{q+1}} \prod_{j \in I_{X_i} - \{j^*\}} e(g, g)^{c_j} \\ &= M_{\beta,i} \cdot e(g_{q+1}, h_i) \cdot e(g, h_i)^{c_{t_i}} \end{aligned}$$

After then, for addition or revocation of attributes specified by \mathcal{A} in \mathcal{U}^* ; \mathcal{B} runs the $Update(CT^*, \mathcal{U}^*) \rightarrow CT'$ algorithm to update the ciphertext. \mathcal{B} proceeds by updating the $a_{I,i}$ and $c_{I,i}$ to $a'_{I,i}$ and $c'_{I,i}$ respectively because of addition and revocation of attributes from particular attribute sets in CT^* . Precisely, $a'_{I,i} = \sum_{j=1}^{m'} a_j$ and $c'_{I,i} = \sum_{j=1}^{m'} c_j$ and the distribution of the CT' is identical to CT^* . Finally, the set values of CT' is

$$\begin{aligned} C'_{1,i} &= g^{t_i} \\ C'_{2,i} &= h_i^{-a'_{t_i}} \\ C'_{3,i} &= M_{\beta,i} \cdot e(g_{q+1}, h_i) \cdot e(g, h_i)^{c'_{t_i}} \end{aligned}$$

We note that ciphertext $CT' = \{C'_{1,i}, C'_{2,i}, C'_{3,i}\}$ is a valid encryption of message $M_{\beta,i}$ if $T_i = e(g_{q+1}, h_i)$; otherwise, if it a random group element, i.e., $T_i \in G_T$, then CT' is independent of β in \mathcal{A} view. For $v' = 0$, the ciphertext CT' is valid and T_i is set as $e(g_{q+1}, h_i)$. \mathcal{A} can guess correct β' with a non-negligible advantage defined by $Pr[\beta' = \beta | v' = 0] = \frac{1}{2} + \epsilon$. For $v' = 1$, $T_i \in G_T$, CT' cannot be identified and we have $Pr[\beta' \neq \beta | v' = 1] = \frac{1}{2}$. From the analysis, the probability with which \mathcal{B} succeeds in breaking the q-BDHE assumption is: $\frac{1}{2}Pr[\beta' = \beta | v' = 0] + \frac{1}{2}Pr[\beta' \neq \beta | v' = 1] = \frac{1}{2} + \frac{\epsilon}{2}$.

Note: There is an assumption that attributes are not repeated in the policy W^* .

□

7.2. Performance Analysis

To demonstrate the performance of the proposed scheme, we firstly compare algorithmically our proposed scheme with the existing healthcare CP-ABE schemes. Moreover, to evaluate the effectiveness of the proposed scheme, the computation time of encryption, decryption, and policy update algorithms is evaluated by varying the number of attributes in the policy. In addition, for the effectiveness of model in real-time scenarios, a shimmer sensor has been employed, whose results are discussed below.

7.2.1. Algorithmic Complexity Analysis

Here, we give the performance analysis of our proposed scheme taking into consideration the existing relevant schemes. We remark that the encryption, decryption operations, and ciphertext size are the main factors affecting the communication and computation cost of the overall system. The user key generation is a one time process, hence it does not contribute significantly. Table 4 gives a comparison of our proposed scheme with existing multi message CP-ABE schemes [15,16], and healthcare centric CP-ABE schemes, [5–8]. None of the existing schemes facilitates the patient with defining access control policy. As seen from the Table 4, the encryption cost of the proposed scheme is constant with 3 exponential operations for an attribute set W_i in policy. The decryption process comprises 2 pairing operations. Moreover, for the proposed scheme both encryption, decryption operations, and ciphertext size are independent of the number of attributes n in the policy; in-contrast to its dependence on attributes in other relevant existing schemes.

Table 4. Computational Costs Comparison with existing relevant schemes.

Scheme	Encryption	Decryption	Ciphertext Size
[5]	$(5n + 2)E$	$(2z + 1)P + 2zE$	$ G_T + (3n + 1) G $
[6]	$((K + 2)n + 3)E$	$3zP + zE$	$ G_T + (2n + 1) G $
[7]	$(3n + 3)P + (5n + 2)E$	$(3z + 1)P + (z + 1)E$	$ G_T + (3n + 3) G $
[8]	$(2n + 2)E$	$(2z + 1)P + 2zE$	$ G_T + (2n + 1) G $
[15]	$(2n + 2p')E$	$(2z + 1)P + zE$	$(2n + p') G + p' G_T $
[16]	$(3n + p')E$	$zP + zE$	$n G + (n + p') G_T $
This Work	$(3p')E$	$2P$	$2p' G + p' G_T $

n : number of attributes in access structure, z : users attributes satisfying policy, p' : number of attribute sets in policy, E : Exponentiation, P : Pairing, G : Source group, i.e., g , G_T : Target group, i.e., $e(g,g)$, K : depth of attribute vector.

We compare the policy update feature of our scheme with Jiang et al. [26], Belguith et al., and [28] Li et al. [27] based on several parameters as seen from Table 5. The policy update operation is performed at the data owner/patient side, while the ciphertext update operation is performed at the server side. The encryption, ciphertext size, policy update, and ciphertext update costs is a function of p' in the proposed scheme, where p' is the number of attributes sets W_i in the policy. However, for [26–28] the costs varies based on variables u , n and t , where u is the total number of attributes in universe, n is the number of attributes in access structure, t is the number of revoked attributes from ciphertext. Typically u and n generally have large values like $u = 1000$ and $n = 30$ – 100 , and p' is smaller like 5–15; hence, the fact reveals that costs for the proposed scheme are fairly less in contrast to [26–28]. This fact has been demonstrated with experimental results below.

Table 5. Comparison of schemes based on policy update.

Scheme	Encryption	Decryption	Ciphertext	Policy Update	Ciphertext Update
[26]	$3p'E$	$2P$	$p'((u - n + 1 + t) G + G_T)$	$p'tE$	$(u - n - 1) G $
[27]	$(3n + 2)E$	$(2z + 2)P + zE$	$(2n + 1) G + G_T $	$3nE + nZ_p$	$2n G + nZ_p$
[28]	$(r + u + 6)E$	$8E + 6P$	$(6 + u + r) G $	$(3t + 1)E + P$	$(6 + u + r) G $
This Work	$3p'E$	$2P$	$p'(2 G + G_T)$	$p'2E$	$p'(G + G_T)$

E : Exponentiation, P : Pairing, G : Source group, i.e., g , G_T : Target group, i.e., $e(g,g)$, r : max number of revoked attributes, u : number of attributes in universe, n : number of attributes in access structure, t : number of revoked attributes from ciphertext.

7.2.2. Computational Complexity Analysis

In this section, we demonstrate our proof-of-concept prototype by implementing our proposed solution using a client-server architecture. All our simulation results presented here are carried on a Ubuntu 14.04 virtual machine with 2GB allocated Ram on a Dell Inspiron i3-6006U CPU@2GHz laptop with 8GB RAM. To test the feasibility of the proposed

scheme, we have used a physiological health sensor: Shimmer3 motion (IMU) coupled with biophysical units. Table 6 highlights the different data streams that can be gathered through the Shimmer sensor and their sampling rate. The sampling rate of 128 Hz by GSR sensor indicates it generates 128 samples per second. However, the parameter values generated by the sensors differ, like GSR generates only 1 parameter value per sample. In-contrast, the Gyroscope and ECG sensors generate 3 and 4 parameter values per sample respectively.

Table 6. Shimmer Sensor Specification.

Source	Sampling Rate
Gyroscope	512 Hz
ECG	1024 Hz
EMG	512 Hz
GSR	128 Hz
Optical Pulse PPG	128 Hz

The shimmer sensor was worn by one of the participant and the physiological data stream was gathered for testing the feasibility of the scheme presented in this paper. We simulated the CP-ABE based policy specification/update results on a pairing based crypto library Charm [41], and the physiological sensors data encryption using Advanced Encryption Standard (AES) by employing Cipher Block Chaining (CBC) mode in pycryptodomex library [42]. We employed “SS512” symmetric curve with a base field of 512 bit to implement CP-ABE based pairing operations in Charm. The time presented here is the average over ten iterations in Charm and pycryptodomex libraries.

The x-coordinate depicts the number of attributes in an attribute set of policy. To elaborate that the computation and policy update cost of proposed scheme is almost constant for any number of attributes to be specified under policy, the number of attributes needs to be gradually increased to depict this effect. For Figures 3–6 horizontal axis shows the gradual increase of attributes to depict the effect.

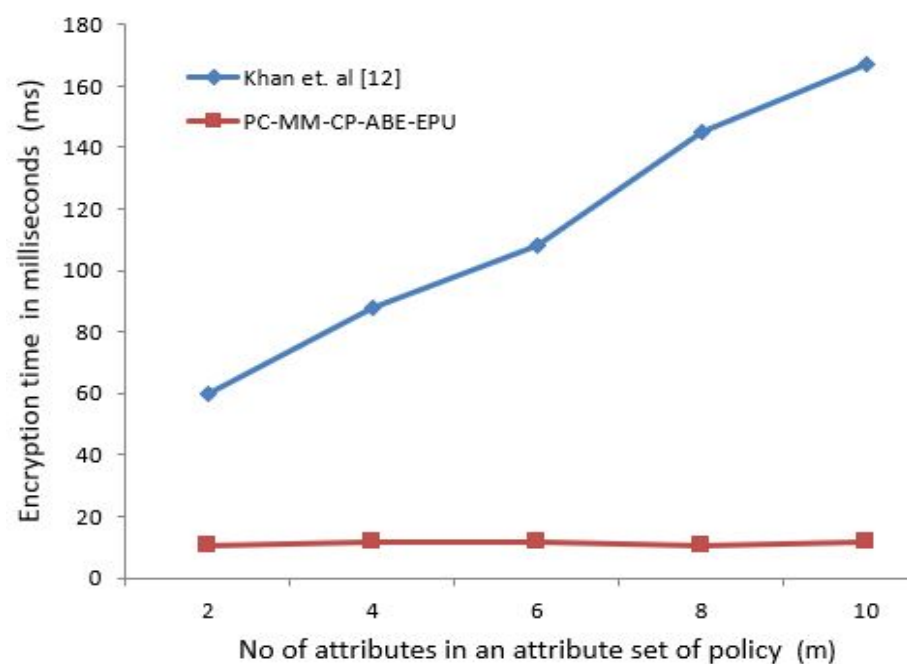


Figure 3. Patient Policy Encryption Time (ms) for # of attributes.

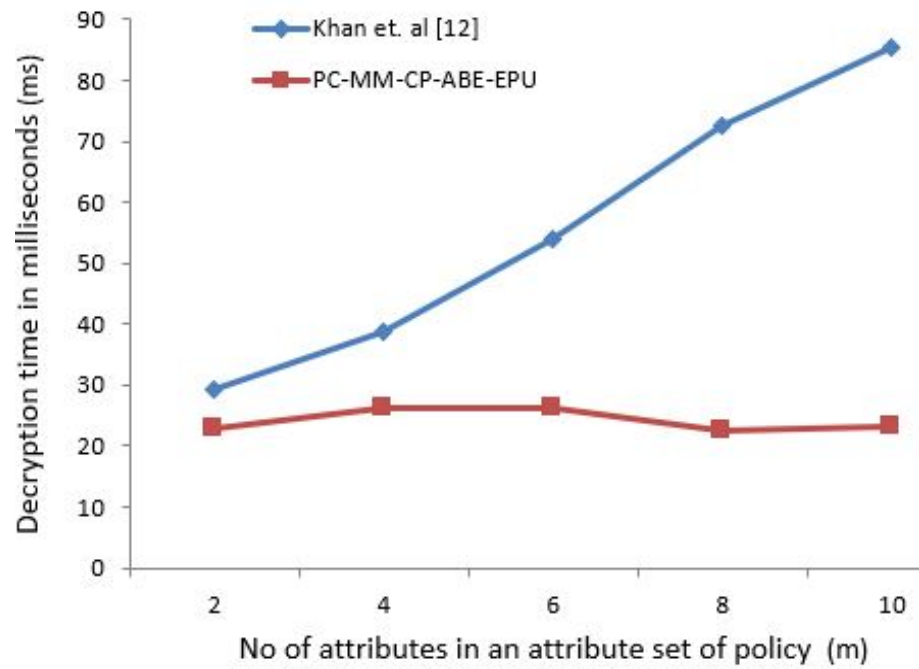


Figure 4. Contextual User’s Conforming Policy for data access.

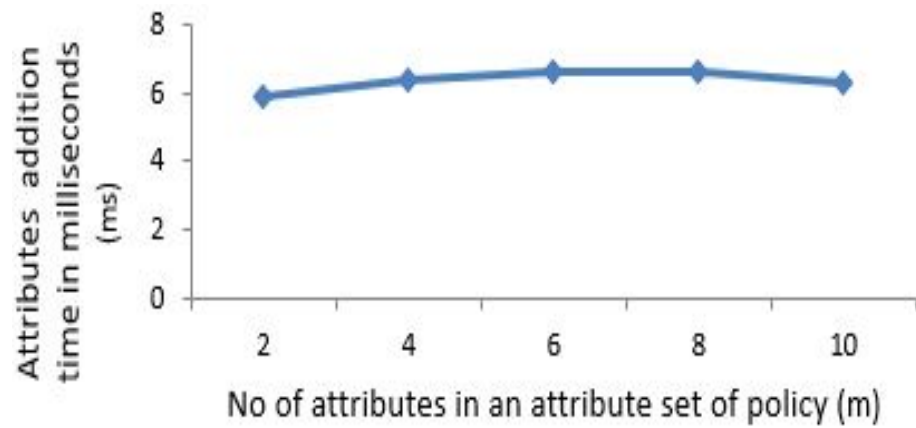


Figure 5. Attributes addition by patient for policy update.

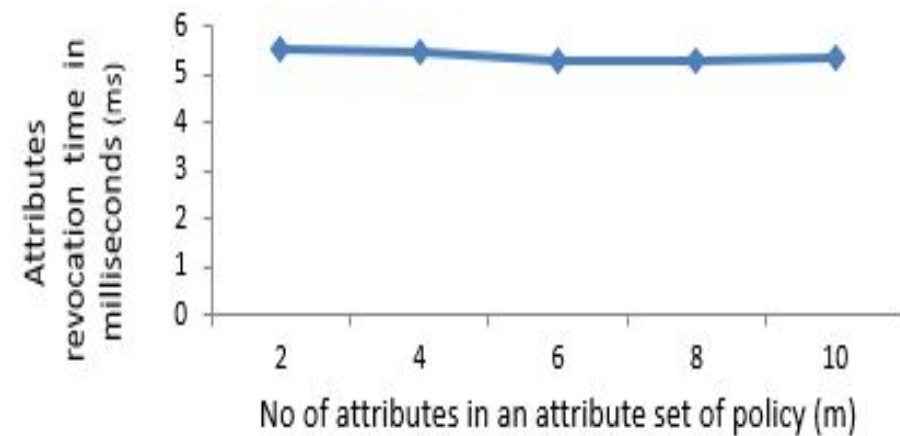


Figure 6. Attributes revocation by patient for policy update.

Figure 3 shows the encryption time in milliseconds (ms) for the number of attributes specified by the patient. Similarly, Figure 4 shows the decryption time in milliseconds (ms) for user's with contextual attributes, i.e., doctor, nurse, and professor. As our proposed scheme is independent of the involvement of the attributes in encryption and decryption operations, hence the time is almost constant in contrast to [16] as seen from Figures 3 and 4.

For updating the policy, the generation of update parameter U involves an exponential operation and several multiplications depending on the number of attributes addition or revocation for our proposed scheme. Figure 5 indicates the time in (ms) taken by the patient for adding additional number of attributes to an existing policy. Similarly, Figure 6 shows it for the case of attributes revocation by patient from an existing defined policy. Figures 5 and 6 exhibit a fractional change in time of around 1 ms (almost constant) which incurred due to multiplication of group elements while increasing attributes from 2 to 10.

Any contextual user satisfying the policy will have access to data, this literally means that contextual user will have access to AES data encryption/decryption key with which the data owner has performed encryption. Considering the role of patient, we encrypted the data generated by the shimmer sensor-GSR, Gyroscope, and ECG with AES in CBC mode for 1 s time span. Table 7 shows the average encryption, decryption time in (ms) for the selected sensors. As the sampling rate and parameters per sample vary for all three sensors, hence the ciphertext size is different for all of the sensors as presented in Table 7.

The policy specification/update or its conformance is normally a one time process, and takes similar amount of time as seen from Figures 3–6 in comparison to data encryption timings as seen from Table 7. For real-time health care data acquisition, monitoring, analysis, and diagnosis; the policy specification and data encryption time should be less, so that an uninterrupted synchronous data transmission can be achieved between both parties. This fact can also be validated from the worst-case ECG sensor encryption time of 68 ms which is less than 1 s. We affirm that the proposed scheme performance is independent of the sensor used to generate the data.

Table 7. Realtime Sensor's Data Encryption.

Source	Encryption (ms)	Decryption (ms)	Ciphertext (bytes)
GSR	0.19	0.10	1813
Gyroscope	0.27	0.19	23,541
ECG	0.68	0.48	63,797

8. Conclusions and Future Work

To address simultaneously the challenges of enforcing hierarchal access control and providing dynamic access privileges for healthcare, in this paper, we have proposed the notion of an efficient patient centric multi message CP-ABE with policy update. The proposed scheme can encrypt multiple messages to ensure access control for hierarchal groups of users resulting in users having access to different granularities of the same data. Moreover, the data owner can dynamically enforce addition or revocation of attributes from policy. Performance analysis of the scheme depicts that computation and communication costs incurred by the construction are almost constant; in contrast to depending on number of involved attributes in policy. Moreover, it is proven to be selectively secure under q -BDHE assumption in random oracle model. In future, we will extend the proof-of-concept prototype and integrate it with a public cloud platform.

Author Contributions: Conceptualization, F.K., S.T.; methodology, F.K., S.K.; validation, F.K., S.K., H.T.; writing—original draft, F.K., S.T.; writing—review and editing, F.K., J.A., S.A.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Peter, M.; Grance, T. *The NIST Definition of Cloud Computing*; Computer Security Division, Information Technology Laboratory, USA. 2011. Available online: <https://csrc.nist.gov/publications/detail/sp/800-145/final> (accessed on 1 May 2020).
2. Mongelli, M.; Orani, V.; Cambiaso, E.; Vaccari, I.; Paglialonga, A.; Braido, F.; Catalano, C.E. Challenges and Opportunities of IoT and AI in Pneumology. In Proceedings of the 23rd Euromicro Conference on Digital System Design (DSD), Kranj, Slovenia, 26–28 August 2020; pp. 285–292.
3. Yaqoob, I.; Salah, K.; Jayaraman, R.; Al-Hammadi, Y. Blockchain for healthcare data management: Opportunities, challenges, and future recommendations. In *Neural Computing and Applications*; Springer: Berlin/Heidelberg, Germany, 2021; pp. 1–16.
4. Bethencourt, J.; Sahai, A.; Waters, B. Ciphertext-Policy Attribute-Based Encryption. In Proceedings of the 2007 IEEE Symposium on Security and Privacy (SP '07), Berkeley, CA, USA, 20–23 May 2007.
5. Liu, Y.; Zhang, Y.; Ling, J.; Liu, Z. Secure and fine-grained access control on e-healthcare records in mobile cloud computing. *Future Gener. Comput. Syst.* **2018**, *78*, 1020–1026. [[CrossRef](#)]
6. Qin, B.; Deng, H.; Wu, Q.; Domingo-Ferrer, J.; Naccache, D.; Zhou, Y. Flexible attribute-based encryption applicable to secure e-healthcare records. *Int. J. Inf. Secur.* **2015**, *14*, 499–511. [[CrossRef](#)]
7. Gritti, C.; Susilo, W.; Plantard, T.; Liang, K.; Wong, D.S. Empowering Personal Health Records with Cloud Computing: How to Encrypt with Forthcoming Fine-Grained Policies Efficiently. 2014. Available online: <https://ro.uow.edu.au/cgi/viewcontent.cgi?article=4299&context=eispapers> (accessed on 15 March 2020).
8. Guo, C.; Zhuang, R.; Jie, Y.; Ren, Y.; Wu, T.; Choo, K.K.R. Fine-grained database field search using attribute-based encryption for e-healthcare clouds. *J. Med Syst.* **2016**, *40*, 235. [[CrossRef](#)] [[PubMed](#)]
9. Suresh, D.; Florence, M.L. Securing Personal Health Record System in Cloud Using User Usage Based Encryption. *J. Med Syst.* **2019**, *43*, 171. [[CrossRef](#)] [[PubMed](#)]
10. Yang, K.; Jia, X. Expressive, Efficient, and Revocable Data Access Control for Multi-Authority Cloud Storage. *IEEE Trans. Parallel Distrib. Syst.* **2013**, *25*, 1735–1744. [[CrossRef](#)]
11. Burns, A.; Greene, B.R.; McGrath, M.J.; O'Shea, T.J.; Kuris, B.; Ayer, S.M.; Stroiescu, F.; Cionca, V. SHIMMER™—A Wireless Sensor Platform for Noninvasive Biomedical Research. *IEEE Sens. J.* **2010**, *10*, 1527–1534. [[CrossRef](#)]
12. Sahai, A.; Waters, B. Fuzzy Identity-Based Encryption. In *Advances in Cryptology—EUROCRYPT*; Springer: Berlin/Heidelberg, Germany, 2005; pp. 457–473.
13. Cheung, L.; Newport, C. Provably secure ciphertext policy ABE. In Proceedings of the 14th ACM Conference on Computer and Communications Security (CCS '07), Alexandria, VA, USA, 29 October–2 November 2007.
14. Lewko, A.; Waters, B. Decentralizing Attribute-Based Encryption. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*; Springer: Berlin/Heidelberg, Germany, 2011; pp. 568–588.
15. Wu, Y.; Wei, Z.; Deng, R.H. Attribute-Based Access to Scalable Media in Cloud-Assisted Content Sharing Networks. *IEEE Trans. Multimed.* **2013**, *15*, 778–788.
16. Khan, F.; Li, H.; Zhang, L. Owner Specified Excessive Access Control for Attribute Based Encryption. *IEEE Access* **2016**, *4*, 8967–8976. [[CrossRef](#)]
17. Zhang, L.; Li, H.; Zhang, Y.; Khan, F. Efficient privacy-preserving decentralized ABE supporting expressive access structures. In Proceedings of the 2017 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHOPS), Atlanta, GA, USA, 1–4 May 2017; pp. 547–552.
18. Zhang, L.; Li, H.; Zhang, Y.; Khan, F. Privacy-preserving attribute-based encryption supporting expressive access structures. In Proceedings of the 2017 IEEE Second International Conference on Data Science in Cyberspace (DSC), Shenzhen, China, 26–29 June 2017; pp. 475–482.
19. Pirretti, M.; Traynor, P.; McDaniel, P.; Waters, B. Secure attribute-based systems. In Proceedings of the 13th ACM Conference on Computer and Communications Security—CCS '06, Alexandria, VA, USA, 30 October–3 November 2006.
20. Attrapadung, N.; Imai, H. Conjunctive Broadcast and Attribute-Based Encryption. In *Pairing-Based Cryptography, LNCS 5671*; Springer: Berlin/Heidelberg, Germany, 2009; pp. 248–265.
21. Lewko, A.; Sahai, A.; Waters, B. Revocation Systems with Very Small Private Keys. In Proceedings of the 2010 IEEE Symposium on Security and Privacy, Oakland, CA, USA, 16–19 May 2010.
22. Yang, K.; Jia, X.; Ren, K.; Zhang, B. DAC-MACS: Effective data access control for multi-authority cloud storage systems. In Proceedings of the 2013 Proceedings IEEE INFOCOM, Turin, Italy, 14–19 April 2013.
23. Hong, J.; Xue, K.; Li, W. Security Analysis of Attribute Revocation in Multiauthority Data Access Control for Cloud Storage Systems. *IEEE Trans. Inf. Forensics Secur.* **2015**, *10*, 1315–1317. [[CrossRef](#)]
24. Ying, Z.; Li, H.; Ma, J.; Zhang, J.; Cui, J. Adaptively secure ciphertext-policy attribute-based encryption with dynamic policy updating. *Sci. China Inf. Sci.* **2016**, *59*, 1–16. [[CrossRef](#)]
25. Yuan, W. Dynamic Policy Update for Ciphertext-Policy Attribute-Based Encryption. IACR Cryptology ePrint Archive 2016, p. 457. Available online: <https://eprint.iacr.org/2016/457.pdf> (accessed on 15 March 2020).
26. Jiang, Y.; Susilo, W.; Mu, Y.; Guo, F. Ciphertext-policy attribute-based encryption supporting access policy update and its extension with preserved attributes. *Int. J. Inf. Secur.* **2017**, *17*, 533–548. [[CrossRef](#)]
27. Li, J.; Wang, S.; Li, Y.; Wang, H.; Wang, H.; Wang, H.; You, Z.; Chen, J. An efficient attribute-based encryption scheme with policy update and file update in cloud computing. *IEEE Trans. Ind. Inform.* **2019**, *15*, 6500–6509. [[CrossRef](#)]

28. Belguith, S.; Kaaniche, N.; Hammoudeh, M.; Dargahi, T. Proud: Verifiable privacy-preserving outsourced attribute based signcryption supporting access policy update for cloud assisted iot applications. *Future Gener. Comput. Syst.* **2020**, *111*, 899–918. [[CrossRef](#)]
29. Ambrosin, M.; Anzanpour, A.; Conti, M.; Dargahi, T.; Moosavi, S.R.; Rahmani, A.M.; Liljeberg, P. On the feasibility of attribute-based encryption on internet of things devices. *IEEE Micro* **2016**, *36*, 25–35. [[CrossRef](#)]
30. Zhang, Y.; Deng, R.H.; Xu, S.; Sun, J.; Li, Q.; Zheng, D. Attribute-based encryption for cloud computing access control: A survey. *ACM Comput. Surv. (CSUR)* **2020**, *53*, 1–41. [[CrossRef](#)]
31. Liang, K.; Fang, L.; Susilo, W.; Wong, D.S. A ciphertext-policy attribute-based proxy re-encryption with chosen-ciphertext security. In Proceedings of the 2013 5th International Conference on Intelligent Networking and Collaborative Systems, Xi'an, China, 9–11 September 2013; pp. 552–559.
32. Ning, J.; Dong, X.; Cao, Z.; Wei, L. Accountable authority ciphertext-policy attribute-based encryption with white-box traceability and public auditing in the cloud. In *European Symposium on Research in Computer Security*; Springer: Cham, Switzerland, 2015; pp. 270–289.
33. Ning, J.; Cao, Z.; Dong, X.; Liang, K.; Ma, H.; Wei, L. Auditable σ -time outsourced attribute-based encryption for access control in cloud computing. *IEEE Trans. Inf. Forensics Secur.* **2017**, *13*, 94–105. [[CrossRef](#)]
34. Georgakakis, E.; Nikolidakis, S.A.; Vergados, D.D.; Douligieris, C. Spatio temporal emergency role based access control (STEM-RBAC): A time and location aware role based access control model with a break the glass mechanism. In Proceedings of the 2011 IEEE Symposium on Computers and Communications (ISCC), Corfu, Greece, 28 June–1 July 2011; pp. 764–770.
35. Zhang, Y.; Zheng, D.; Chen, X.; Li, J.; Li, H. Computationally Efficient Ciphertext-Policy Attribute-Based Encryption with Constant-Size Ciphertexts. In *International Conference on Provable Security*; Springer International Publishing: Berlin/Heidelberg, Germany, 2014; pp. 259–273.
36. Chen, C.; Zhang, Z.; Feng, D. Efficient Ciphertext Policy Attribute-Based Encryption with Constant-Size Ciphertext and Constant Computation-Cost. In *International Conference on Provable Security*; Springer: Berlin/Heidelberg, Germany, 2011; pp. 84–101.
37. Khan, F.; Li, H.; Zhang, L.; Shen, J. An Expressive Hidden Access Policy CP-ABE. In Proceedings of the 2017 IEEE Second International Conference on Data Science in Cyberspace (DSC), Shenzhen, China, 26–29 June 2017.
38. di Vimercati, S.D.C.; Foresti, S.; Jajodia, S.; Paraboschi, S.; Samarati, P. A data outsourcing architecture combining cryptography and access control. In Proceedings of the 2007 ACM workshop on Computer security architecture—CSAW '07, Fairfax, VA, USA, 1 November 2007; pp. 63–69.
39. Atallah, M.J.; Blanton, M.; Fazio, N.; Frikken, K.B. Dynamic and Efficient Key Management for Access Hierarchies. *ACM Trans. Inf. Syst. Secur.* **2009**, *12*, 1–43. [[CrossRef](#)]
40. di Vimercati, S.; Foresti, S.; Jajodia, S.; Paraboschi, S.; Samarati, P. Over-encryption: Management of access control evolution on outsourced data. In Proceedings of the 33rd International Conference on Very Large Data Bases, VLDB Endowment, Vienna, Austria, 23–27 September 2017; pp. 123–134.
41. Akinyele, J.A.; Garman, C.; Miers, I.; Pagano, M.W.; Rushanan, M.; Green, M.; Rubin, A.D. Charm: A framework for rapidly prototyping cryptosystems. *J. Cryptogr. Eng.* **2013**, *3*, 111–128. [[CrossRef](#)]
42. PyCrypto. Available online: <https://pypi.org/project/pycryptodomex/> (accessed on 15 March 2020).