An Efficient and Secure Revocation-Enabled Attribute-Based Access Control for eHealth in Smart Society

Shahzad Khan 1,2, Waseem Iqbal 1, Abdul Waheed 3,4,*, Gulzar Mehmood 5, Shawal Khan 6, Mahdi Zareei 7 and Rajesh Roshan Biswal 7

1 Department of Information Security, Military College of Signals (MCS), NUST, Islamabad 44000, Pakistan; skhan.phdismsc@student.nust.edu.pk (S.K.); waseem.iqbal@mcs.edu.pk (W.I.)
2 Department of Computer Science, Shaheed Benazir Bhutto University Sheringal, Dir 18000, Pakistan
3 Department of Computer Science, Northern University, Nowshera 24100, Pakistan
4 School of Electrical and Computer Engineering, Seoul National University, Seoul 08826, Korea
5 Department of Computer Science, IQRA National University, Swat Campus 19220, Pakistan; gulzar.mahmood@uom.edu.pk
6 Department of Computer Science, COMSATS University, Islamabad 44000, Pakistan; shawalsbb@gmail.com
7 Tecnologico de Monterrey, School of Engineering and Sciences, Zapopan 45201, Mexico; m.zareei@tec.mx (M.Z.); roshanb@tec.mx (R.R.B.)

* Correspondence: abdul@netlab.snu.ac.kr

Abstract: The ever-growing ecosystem of the Internet of Things (IoT) integrating with the ever-evolving wireless communication technology paves the way for adopting new applications in a smart society. The core concept of smart society emphasizes utilizing information and communication technology (ICT) infrastructure to improve every aspect of life. Among the variety of smart services, eHealth is at the forefront of these promises. eHealth is rapidly gaining popularity to overcome the insufficient healthcare services and provide patient-centric treatment for the rising aging population with chronic diseases. Keeping in view the sensitivity of medical data, this interfacing between healthcare and technology has raised many security concerns. Among the many contemporary solutions, attribute-based encryption (ABE) is the dominant technology because of its inherent support for one-to-many transfer and fine-grained access control mechanisms to confidential medical data. ABE uses costly bilinear pairing operations, which are too heavy for eHealth’s tiny wireless body area network (WBAN) devices despite its proper functionality. We present an efficient and secure ABE architecture with outsourcing intense encryption and decryption operations in this work. For practical realization, our scheme uses elliptic curve scalar point multiplication as the underlying technology of ABE instead of costly pairing operations. In addition, it provides support for attribute/users revocation and verifiability of outsourced medical data. Using the selective-set security model, the proposed scheme is secure under the elliptic curve decisional Diffie–Hellman (ECDDH) assumption. The performance assessment and top-ranked value via the help of fuzzy logic’s evaluation based on distance from average solution (EDAS) method show that the proposed scheme is efficient and suitable for access control in eHealth smart societies.

Keywords: access control; attribute-based encryption; elliptic curve; wireless body area networks; smart society

1. Introduction

The transformative effect of eHealth on smart society (shown in Figure 1) enables wearable medical devices for a vast number of applications, such as wearable fitness trackers, smart health watches, electrocardiogram (ECG) monitors, blood pressure monitors, biosensors, etc. On the other front, advances in wireless communication lead to the emergence of the solidified and specialized wireless area network for these worn-on or implanted devices; the wireless body area network (WBAN). A WBAN typically consists of tiny biosensors or sensors (wearable and/or implanted) to collect/forward vital signs to
the mobile or fixed gateway. It was developed to enable around-the-clock availability of a patient’s medical data to healthcare professionals. This unremitting availability of data will efficiently utilize healthcare resources and makes in-home monitoring for patients having chronic diseases [1]. Unlike conventional sensor networks, a WBAN operates on more critical and sensitive patient information that demands significant security and privacy preservation from the practical aspect of this technology. This concern leads to the desire for more control of their data from the data owner end. This self-contradicting aspect results in severe security challenges for its practical adaptation. In the presence of its underlying Internet of Things (IoT) infrastructure, conventional encryption techniques preclude its adaption for WBAN security. Specifically, public-key encryption suffers from high computation, certificate, and key management overhead issues. The dynamic secret key management hinders the application of symmetric encryption as well. Considering the nature of WBAN healthcare systems, it is inevitable to provide this crucial data to its concerned healthcare professionals. Hence, traditional role-based access control and identity-based encryption (IBE) cannot guarantee fine-grained and one-to-many data transfer. Recently, attribute-based encryption (ABE) has gained popularity for secure access control mechanisms to confidential data because of its inherent support for fine-grained access and one-to-many transfer. ABE is a particular type of IBE; the user’s ID is described by the set of attributes, in which the data is encrypted for all those users who are the possessors of that specific set of attributes. The ABE schemes are categorized into two variants: ciphertext policy (CP-ABE) and key-policy (KP-ABE). Using CP-ABE, the data owner embeds access policy inside ciphertext and the private key of the end user is attached to the attribute set. Anyone can perform the decryption operation if his/her attributes matched with the specified access policy. While in KP-ABE, private keys are attached with the access control policy and ciphertext are attached with the attribute set [2]. In the context of WBAN, ciphertext policy ABE (CP-ABE) is more appropriate because it provides more control to the data owners (patient in WBAN) over the recipients [3] (medical stuff in WBAN) as opposed to its other type, i.e., key-policy ABE (KP-ABE) [4]. The only series concern for most contemporary ABE schemes is that they rely heavily on expensive bilinear pairing and exponentiation operation in the encryption and decryption algorithm. This intense computation hinders its deployment for WBAN resource-constrained sensors [3,5]. This leads to the development of non-pairing ABE schemes in the research community. As a result, the most recent work equips the ABE with the elliptic curve cryptography (ECC) algorithms, which have much stronger bit security and also replace the ten times more expensive bilinear pairing operation with scalar point multiplication on an elliptic curve [3]. At the same time, because of underlying ABE technology, linearity properties entrust the ECC algorithm with heavy operations. As we know, the number of operations linearly increases with the number of attributes and hence incurs a heavy load on WBAN sensors. Therefore, a secure and efficient management mechanism is needed, which stands this operation to an acceptable and minimum constant range for WBAN sensors nodes. In this paper, by utilizing Hu et al.’s [4] secure framework for WBAN, we have proposed an efficient and secure ECC-based CP-ABE scheme for WBAN.
Figure 1. eHealth in smart societies.

Our Contribution

The primary contribution of our work is as follows:

1. Considering the resource-scarce nature of WBAN, we have proposed an efficient and secure ABE scheme with outsourcing intense encryption and decryption operations without revealing the secret key/data content to the WBAN data sink node and cloud server digital signal processing (DSP), respectively.

2. Our proposed scheme is based on elliptic curve point scalar multiplication instead of costly bilinear pairing operations to address the resource-constrained nature of WBAN, especially the sensors. This feature makes it more appealing to smart healthcare.

3. Our proposed scheme supports indirect attribute/users revocation without the need for maintaining a private channel between the trusted attribute authority and the non-revoked users for disseminating updated decryption keys.

4. The proposed scheme inherently supports the integrity check, thus increasing the security and reliability of medical data.

5. The proposed scheme is secure under the elliptic curve decisional Diffie–Hellman (ECDDH) assumption using the selective-set security model.

6. The performance assessment of our scheme shows a significant overall efficiency in storage, computation, and communication.

2. Related Work and Background Knowledge

This section presents a brief overview of existing work and all the cryptographic primitives used to construct our proposed scheme.

2.1. Related Work

With the emerging use of e-healthcare systems, patients are not only concerned for the security of their personal information but also worry for the privacy of their biological characteristics [6,7]. To improve the performance, early approaches utilized cloud computing models for e-healthcare systems. For example, in [8] they have proposed a patient-oriented four-layer cloud-based e-healthcare system. With the emergence of edge computing and its proximity to resource-constrained devices, many edge-based e-healthcare systems [9,10] are proposed. In [11], the author developed a first-aid service to provide emergency aid to the patients rapidly. However, the early approach lacks the much-needed security re-
quirements. For the realization of security in smart healthcare, the author in [12] utilizes fully homomorphic encryption (FHE) to encrypt the data. For better security, Cai et al. [13] create a novel medical record based on the mobile cloud without compromising too much performance. Still, the above system does not devise any proper access control mechanism for these medical records. So, to better protect data privacy, some schemes equipped with access control were proposed [14,15]. For example, in [15], the author suggests a role-based access control with the capability of origin tracing and further scrutinizing the authorization of access made to the system resources. However, fine-grained access control is needed for better and flexible access, which requires the exposure of specific portions of data to the relevant medical professionals. Attributed to its inherent expressiveness and fine-grained access support, attribute-based encryption (ABE) has emerged. Sahi and waters [16] were the first to interpret the identity of users as a set of attributes and were able to propose a fuzzy variation of identity-based encryption (IBE). Attributed to the placement of access policy, ABE has two variations, namely key-policy ABE (KP-ABE) [17] and ciphertext policy ABE (CP-ABE) [18]. Li et al. [19] propose the outsourcing of encryption with MapReduce to relieve local computation overhead. Li et al. [20] construct a novel ABE scheme which outsourced both the key-issuing and decryption with the verification of the results returned from the cloud server. Asim et al. [21], with the help of a semi-trusted proxy, outsourced the computation of message encryption by utilizing the El-Gamal cipher. However, the scheme is proven in the generic group model. Zong et al. [22] utilize the edge-enabled environment for outsourcing part of encryption and decryption to the edge node for the smart healthcare system. Zhidan et al. [23] propose the construction of an ABE scheme with verifiable delegation both for encryption and decryption to an untrusted encryption service provider (ESP) and a decryption service provider (DSP), respectively. Khan et al. [24] propose an online/offline-aided attribute-based multi-keyword search (OOABMS) scheme to delegate most heavy computation operations to the offline phase before acquiring the attribute-based access control policy or keywords. However, all of these ABE schemes were heavily dependent on a costly bilinear pairing operation [25]. Later, in [26], the author proposed a free-pairing lightweight KP-ABE scheme using ECC for resource constraint of IoT infrastructure. Consequently, Tan et al. [27] introduces the concept of key out-sourcing property in [26] for better efficiency without compromising its security. Several body sensor network (BSN) [28,29], are proposed for the cloud environment that exhibits their usability and favorability for the key-policy type of ABE in different scenarios. KP-ABE transferred the computation overhead of access policy formulation to the medical attribute authority (MAA) from the patient but at the same time offered no control over it. CP-ABE offers complete control over who has access to the sensitive medical data, making it conceptually similar to the role-based access control [30] model.

These appealing characteristics for WBAN resulted in the basis for many proposed [18] schemes with various features such as policy update, hidden access policy, traceability, and revocability. These schemes mainly utilized costly pairing operations. Considering the resource constraint nature of a WBAN, pairing-free ABE schemes should be the first choice of a WBAN. In this direction, Ref. [31] proposed a pairing-free ECC-based CP-ABE scheme. However, similar to most of the schemes, this also suffers from the inherent linearity property of ABE. For the sake of practical deployment, we have designed a pairing-free CP-ABE scheme based on ECC with a minimal constant number of scalar point multiplication.

Basar et al. [32] present an image segmentation method based on pulse coupled neural network (PCNN) and local binary pattern (LBP) components. The proposed method is robust because the presented model’s parameters can be modified for different situations. The proposed algorithm has been tested on a dataset that consists of 1000 defocused images. The results show that the proposed algorithm outperforms contemporary algorithms on different evaluation metrics such as accuracy and precision. A fuzzy logic-based ranking based on EDAS has been used for ranking. The experimental results and evaluation show
that the proposed scheme outperforms contemporary schemes in terms of time complexity and accuracy.

Mehmood et al. [33] developed a trust-based energy-efficient and reliable communication scheme named trust-based ERCS for remote patient monitoring in eHealth applications. A cooperative communication strategy is used in the proposed scheme to ensure trust and reliability. Furthermore, privacy preservation and a fuzzy-logic rank-based method have been used in the proposed scheme. The detailed experimental results and ranking demonstrated that the proposed scheme outperforms the available contemporary schemes.

Similarly, Basar et al. [34] present a method for an RGB histogram-based K-means clustering initialization for unsupervised color image segmentation. In this method, an adaptive initialization approach has been used to determine the number of clusters and initial central points of each cluster to solve the segmentation issues of color images. The proposed method is compared with well-known unsupervised segmentation methods on various segmentation parameters. Furthermore, the EDAS (evaluation based on distance from average solution) technique is used to rank segmentation integrity. The experimental results show that the proposed method outperformed the contemporary methods. However, due to classification errors, the proposed method is not recommended for healthcare medical applications.

2.2. Background Knowledge

This section presents all the cryptographic primitives used for the construction of our proposed ECC-based ABE scheme, including elliptic curve cryptosystem, lagrange interpolation for secret reconstruction, and access control structure.

2.3. Elliptic Curve Cryptosystem and Its Related Complexity Assumptions

An elliptic curve E over a prime finite field $\mathbb{Z}_p$ is defined by a cubic equation

$$y^2 \pmod{p} = x^3 + a \cdot x + b \pmod{p}$$

while the set of parameters $(p,a,b,G,n)$ can be used for its description, where $x,y,a,b \in \mathbb{Z}_p$, and $4a^3 + 27b^2 \neq 0$. All the point operations in ECC must be define to form a cyclic group $G_E$ over E.

Definition 1 (Elliptic curve discrete logarithm problem (ECDLP)). Given points $P$ and $Q$ on the curve, i.e., $P, Q, G \in G_E$, it is intractable for a polynomial time algorithm to get the random chosen value $K \in \mathbb{Z}_q$ such that $Q = K \cdot P$.

Definition 2 (Elliptic curve computational Diffie–Hellman problem (ECCLP)). For generator $G$ of $G_E$ and randomly chosen values $c,d \in \mathbb{Z}_q^*$, given $(c \cdot G,d \cdot G,G)$ it is intractable for a polynomial time algorithm to get $c \cdot d \cdot G$.

Definition 3 (Elliptic curve decisional Diffie–Hellman problem (ECDLP)). Given randomly chosen values $c,d \in \mathbb{Z}_q^*$ and generator $G$ and any point $Z$ of $G_E$, it is impossible to distinguish between the two probability distributions $(c \cdot G,d \cdot G,c \cdot d \cdot G)$ and $(c \cdot G,d \cdot G,Z)$.

Definition 4 (Access tree). Access tree [17]. Let a tree $T$ represent an access structure. Each non-leaf node of $T$ is identified by a threshold gate, associated by its corresponding threshold value and its children. In this case, if $d_x$ is the threshold value of node $x$ and $\text{num}_x$ is its number of children, then $1 \leq d_x \leq \text{num}_x$. When $d_x = \text{num}_x$, the threshold gate is an AND gate, and when $d_x = 1$, it is an OR gate. Each leaf node $x$ of $T$ is identified by a threshold $d_x = 1$ value and an attribute. Further, definitions and notations can be obtained from [35].

In ABE, the lagrange interpolation is used for secret reconstruction. The lagrange coefficient $\Delta_{i,s}$ for a random number in $\mathbb{Z}_p^*$ and a set of random elements corresponding to each element in $\mathbb{Z}_p^*$ is given by $\Delta_{i,s(x)} = \Pi_{j \in s,j \neq i} \frac{x-j}{i-j}$.
3. System and Security Model

Figure 2 depicts the main components of our proposed scheme, namely the medical attribute authority (MAA), cloud service provider (CSP), body area network (BAN), data sink (DS), and medical data user (MDU). This section presents an overview of the roles played by each component.

Figure 2. System model.

**MAA:** The MAA acts as a key generation center (KGC) and the only fully trusted entity in the system model. KGC is responsible for the registration of all system users [36]. Through the initialization phase, it produces public parameters (PARAMS), a system master key (SMK), and secret key components (SK) against a set of attributes $S_u$ specific to each user.

**CSP:** This entity is providing services for storage and partial decryption via sub-entities storage service provider (SSP) and decryption service provider (DSP), respectively. The SSP stores the encrypted health-related data for each registered patient and serves as a repository for all the uploaded data. DSP performs partial decryption service to the interested MDU’s without knowing the actual data contents.

**BAN:** Body area network is a wireless network consisting of small biosensors. It could be implanted (placed inside the human body), wearable (on the body), or carried based on its specific use. Its deployment aims to persistently measure and notice the abnormal changes in the vital body parameters. Subsequently, consult in real time the healthcare professional for life support. Sensors are suffering from a scarcity of vital resources in memory, battery power, and computation power. In the traditional framework, these [31] resource-constrained sensors are entrusted with the expensive secret distribution mechanism for access formulation along with its prime tasks of sensing, processing, and transmission. Moreover, because of the ABE linearity property, the encryption complexity grows with the size of the access policy. Exploiting the delegation property of the CP-ABE mode of encryption, we offload most of the computation to the gateway. More specifically, retaining part of the secret for little processing locally while exposing part of it to the gateway for most processing still ensures information-theoretical security of a secret.
**DS**: DS acts as a gateway for aggregation and dissemination of its corresponding sensor data to the MAA. It could be a mobile device such as a smartphone or a specialized BAN controller. Hence, it has significantly more memory, processing, and transmission capacity as opposed to the sensors. These features make us compel in our proposed framework to delegate most of the processing overhead from sensors to the DS. The traditional framework [31] devotes this unit to the function of forwarding only, which is not a judicious use of this entity considering its resources.

**MDU**: It could be a doctor, nurse, or any other healthcare expert. To be registered into the system, each MDU must prove its credentials and affiliation in a set of attributes to the KGC. The KGC needs to verify the validity of these claimed attributes, subsequently computes its corresponding secret key components, and sends it via a secure channel to its concerned user. These secret key components are uniquely generated to prevent collision attacks by associating a random number to them. As long as the MDU poses the required set of attributes, it can access any patient’s encrypted data. MDU is usually a device, such as a mobile phone, with limited resources. In our framework, we shift most of the decryption overhead to the DSP of MAA. As a result, after retrieving the partially encrypted data from the DSP, it needs to perform a minor operation on its full decryption.

In our threat model, we take the CSP honest-but-curious, adapted by most of the ABKS schemes, which means they will honestly run the algorithm and infer privacy information based on the available data. The medical attribute authority and the data owner (DO) are fully trusted entities in our system model. Corrupted data users (DU) may also collide with each other. To prove the security of an ABE scheme, the selective-set security model generally makes use of a game between the challenger \( C \) and an attacker \( A \). In this game, the attacker faces challenges posed by the challenger to solve the underlying security assumption. Following are the six steps defined in our security game for our proposed scheme against a chosen-plaintext attack [35].

**Initialization**: \( A \) declares the encryption attribute set in the form of an access structure \( T^* \) that he wants to be challenged upon.

**Setup**: To generates the system parameters, \( C \) runs the setup algorithm, keeps the SMK to itself and sends the public parameter PARAMS to adversary \( A \).

**Phase 1**: The adversary \( A \) is allowed to adoptively ask for a set of secret key components \( K_A^1, K_A^2, \ldots, K_A^n \) of attribute sets \( \Omega_1, \Omega_2, \ldots, \Omega_n \) such that all the attribute sets associated to the corresponding secret key components do not satisfy the \( T^* \).

**Challenge**: Now, \( A \) submits two equal length messages \( M_0 \) and \( M_1 \) to \( C \) with \( T^* \). \( C \) flips binary coin \( b \in \{0, 1\} \) to encrypt \( M_b \) under \( T^* \) and sends the generated ciphertext \( CT^* \) to \( A \).

**Phase 2**: Both adversary \( A \) and challenger \( C \) adoptively repeat the same steps as they did in phase 1.

**Guess**: \( A \) outputs a guess \( b' \) of \( b \) to \( C \).

The advantage \( e \) gained by \( A \) in the above game is defined by \( e = (pr[b' = b]) - \frac{1}{2} \).

Table 1 lists all the notations used in this work.
4. Proposed Model

In this section, a detail description of our proposed scheme algorithms (i.e., Setup, KeyGeneration, Encryptlocal, Encryptesp, Decryptesp, Decryptlocal) is presented.

Setup (λ) → PK, MK: Run by MAA, the Algorithm 1 takes EEC domain parameters as an implicit security parameter λ as input. Define the universal attribute set \( U = \{ att_1, att_2, \ldots, att_n \} \) for attribute space in the system. A secure hash function \( H : \{0,1\}^* \rightarrow \mathbb{Z}_q^* \) is chosen to map global identity GID. MAA for each attribute \( att_i \in U \), chooses \( \beta_i \in \mathbb{Z}_q^* \) uniformly at random. The public key components corresponding to each system attribute \( att_i \) is given by \( PK_i = \beta_i \cdot G \). Moreover, it chooses \( a \in \mathbb{Z}_p^* \) uniformly at random to be the master secret key (MSK). Thereafter, setting accordingly, the master public key (MPK) is \( PK = a \cdot G \). Finally, the algorithm sets the MSK = \( (a, \beta_i | i \in U) \) and PARAMS = \( (U, H, PK, \{PK_i | i \in U\}) \).

Algorithm 1: Setup (λ).

Input Implicit security parameter \( \lambda \).

Output System secret key (SMK) and public parameter.

1. Define an elliptic curve \( E \) over a finite field \( \mathbb{Z}_r \) with a prime order \( r \).
2. Generate a cyclic group \( \mathbb{G}_E \) of subgroup over \( E \) with generator \( G \) of order \( q \).
3. Generate universal attribute set \( U = \{ att_1, att_2, \ldots, att_n \} \).
4. For each \( att_i \in U \), it randomly chooses element \( \beta_i \in \mathbb{Z}_q^* \).
5. MAA subsequently computes public key components corresponding to each attribute \( i \) as \( \{PK_i = \beta_i \cdot G | i \in U\} \).
6. Randomly chooses \( a \in \mathbb{Z}_p^* \) as a master secret key.
7. Accordingly, compute master public key by \( PK = a \cdot G \).
8. Set the PARAMS = \( (U, H, PK, \{PK_i = \beta_i \cdot G | i \in U\}) \).
9. Set the MSK = \( (a, \{\beta_i | i \in U\}) \).

Encryption: To preserve the data privacy and delegate most of the computation of encryption, this algorithm specifies the access control policy tree in the form of \( T = T_{local} \land T_{esp} \), where \( T_{local} \) and \( T_{esp} \) are two subtrees of \( T \) connected by an AND logical operator \( \land \). This division of access control tree leads to two algorithms: local encryption (Algorithm 2) and outsource encryption (Algorithm 3).
Encrypt_{local} (\mathcal{T}, M, PK) \rightarrow CT_{local} \text{ For optimal efficiency, the } \mathcal{T}_{local} \text{ attaches only one virtual attribute, as shown in Figure 3. The algorithm randomly specify a 1-degree polynomial } q_R(\cdot) \text{ and set } q_R(0) = S, q_R(1) = S_1 \text{ and } q_R = S_2, \text{ where } S, S_1, S_2 \in \mathbb{Z}_q.

Let } \Omega_{local} \text{ be the set of leaf nodes in } \mathcal{T}_{local}. \text{ This algorithm encrypts } M \text{ by computing } SK = SK = (S_x, S_y) \text{ such that } SK \neq 0. \text{ Let } S_x \text{ serve as the encryption key and } S_y \text{ be the integrity key for } M, \text{ then } C_M \text{ and } INT_M \text{ can be computed } Enc(S_x, M) \text{ and } HMAC(S_y, M), \text{ respectively. Finally, the algorithm outputs temporal ciphertext}

CT_{local} = (\mathcal{T}_{local}, C_M, INT_M, \forall y \in \Omega_{local} : C_y = q_y(0) \cdot PK_y).

Encrypt_{ESP} (\mathcal{T}_{esp}, s_1, CT_{local}, PK) \rightarrow CT.

Figure 3. Access policy with subtree.

Let } \Omega_{ESP} \text{ be the set of leaf nodes in } \mathcal{T}_{esp}. \text{ Beginning at the root node } R_1 \text{ of the subtree } \mathcal{T}_{esp}, \text{ this algorithm chooses a polynomial } q_x \text{ of degree } d_x - 1 \text{ for each node } v. \text{ Note that the value for root node } R_1 \text{ has been set as } q_{R_1}(1) = S_1. \text{ The value of the inner node } x \text{ is calculated by the equation as } q_x(0) = q_{parent(x)}(index(q)) \text{ and randomly chooses } k_x - 1 \text{ coefficients to build the polynomial } q_x. \text{ Then, the algorithm generates the temporal ciphertext } CT_{ESP} = (\mathcal{T}_{esp}, \forall y \in \Omega_{ESP} : C_y = q_y(0) \cdot PK_y). \text{ Combining the above generated ciphertext with the received ciphertext from } DO, \text{ the whole ciphertext is given as:}

\langle \mathcal{T} = \mathcal{T}_{local} \land \mathcal{T}_{esp}, C_M; \forall y \in \Omega_{local} \cup \Omega_{ESP} : C_y = q_y(0) \cdot PK_y \rangle.

Key Generation (S_u, MSK) \rightarrow K_u \text{ The Algorithm 4 runs by } MAA, \text{ and is used to generate the secret key } K_u \text{ under the valid attribute set } S_u \text{ by the corresponding } DU. \text{ More specifically, upon receiving the claimed attribute set, the } MAA \text{ needs to check its validity and assign a unique global identity } GID \text{ to this } DU. \text{ It selects a random } t \in \mathbb{Z}_p \text{ and computes local private key } K_{local} = a^{1-t}. \text{ This algorithm for each attribute } i \in S_u \text{ generates its corresponding key components, a delegate key given by } DK = \{vi \in S_u : K_i = H(GID) \cdot a \cdot \beta_i^{-1}\}. \text{ Here, } \beta_i^{-1} \text{ is the inverse of element } \beta_i \in \mathbb{Z}_p \text{ chosen in setup phase.}
Algorithm 2: Encrypt_{local}.

**Input** Access structure $\mathcal{T}$, the message $M$ and public parameters $\text{PARAMS}$.  
**Output** Local version of ciphertext $CT_{local}$.
1. Randomly specify a 1-degree polynomial $q_{R}(x)$ corresponding to the root $R$ of $\mathcal{T}$.  
2. Randomly choose $S, S_1$ and $S_2 \in \mathbb{Z}_q^*$.  
3. Set the root node $R$ value to $q_{R}(0) = S$.  
4. For the root nodes $R_1$ and $R_2$ of subtrees set $q_{R}(1) = S_1$ and $q_{R}(2) = S_2$, respectively.  
5. Use ECC scalar point multiplication to compute $S \cdot PK = (S_x, S_y)$. We let $S_x$ and $S_y$ represent the encryption and integrity key for $M$, respectively.  
6. Compute message $M$ encryption $C_M = \text{Enc}(S_x, M)$ using secure symmetric cipher.  
7. Compute message $M$ authentication code $INT_M = \text{HMAC}(S_y, M)$ using HMAC function.  
8. Let $\Omega_{local}$ be a set of leaf nodes in $\mathcal{T}_{local}$.  
9. For each $att_x \in \Omega_{local}$ do.  
10. $CT_{local} = q_{x}(0).PK_x$ using ECC point multiplication End for.  
11. Set the ciphertext $CT_{local} = \langle \mathcal{T}_{local}, C_M, INT_M, \forall y \in \Omega_{local} : C_y = q_y(0) \cdot PK_y \rangle$.  

Algorithm 3: Encrypt_{ESP}.

**Input** Access structure $\mathcal{T}_{esp}, S, CT_{local}$, and public parameters $\text{PARAMS}$.  
**Output** $CT$.
1. Randomly specify a polynomial $q_{R_i}$ with degree $K_{R_i} - 1$, where $K_{R_i}$ is the threshold of root node of subtree $\mathcal{T}_{esp}$.  
2. Set the value of root node $R_i$ to $\mathcal{q}_{R_i}(0) = S_i$.  
3. Randomly select $K_{R_i} - 1$ coefficients to uniquely define $q_{R_i}$.  
4. For inner node $v$ in $\mathcal{T}_{esp}$ do.  
5. Set $q_v(0) = q_{parent(v)}(\text{index}(v))$.  
6. Randomly select $K_v - 1$ coefficients to uniquely define $q_v$.  
7. End For.  
8. Let $\Omega_{ESP}$ be the set of leaf nodes in $\mathcal{T}_{esp}$.  
9. For each $att_x \in \Omega_{ESP}$ do.  
10. $CT_{ESP} = q_{x}(0).PK_x$ using ECC point multiplication.  
11. End For.  
12. The whole ciphertext is given by $CT = \langle \mathcal{T} = \mathcal{T}_{local} \land \mathcal{T}_{esp}, C_M, INT_M, \forall y \in \Omega_{local} \cup \Omega_{ESP} : C_y = q_y(0) \cdot PK_y \rangle$.  

Algorithm 4: KeyGen.

**Input** $DU$ claimed attribute set $S_u$, system master key $\text{SMK}$ Output $DU$ keys: $K_{local}$ and $DK$.
1. After the confirmation of the claimed attribute set $S_u$, the $\text{MAA}$ assigned a global unique identity $\text{GID}$ to its $DU$.  
2. Select a random $t \in \mathbb{Z}_p$, compute $a^t$.  
3. Compute and set $K_{local} = a^{1-t}$.  
4. For each $att_i \in S_u$ do.  
5. Compute $\beta_i^{-1}$ of $\beta_i \in \mathbb{Z}_p$.  
6. Compute $K_i = H(\text{GID}) \cdot a^t \cdot \beta_i^{-1}$.  
7. End For.  
8. Set the keys $K_{local} = (a^{1-t})$, $DK = (\{\forall i \in S_u : K_i = H(\text{GID}) \cdot a^t \cdot \beta_i^{-1}; H(\text{GID})\})$.  

Finally, the algorithm makes use of two algorithms DecryptDSP (Algorithm 5) and DecryptDSP (Algorithm 6).

Decryption: Realizing a CP-ABE scheme via ECC scalar point multiplication instead of bilinear pairing operations still faces a deployment challenge for lightweight devices, especially for sensors. The ECC scheme makes use of threshold secret sharing for secret distribution. Subsequently, the reconstruction makes use of polynomial interpolation, a heavy computation operation. MDU is usually a device such as a mobile phone with limited resources. Hence, this phase delegates most of the decryption load to the DSP. This phase makes use of two algorithms Decryptlocal (Algorithm 5) and DecryptDSP (Algorithm 6).

DecrypDSP (DK, PARAM, CT) → CT_temp

This algorithm is run by DSP, which makes use of a recursive function DecNode(CT, DK, y). If y is leaf node, let i = alt(y), DecNode(CT, DK, y) is defined as:

\[
\text{DecNode}(CT, DK, y) = \begin{cases} 
\frac{K_i}{H(GID)}, & \forall i \in S_u \\
\bot, & \text{ otherwise.}
\end{cases}
\]

which states that the output of DecNode() must be an element in EC group \( \mathbb{G}_E \) or null.

For a leaf node \( y \in S_u \), the function DecNode() proceeds as follows:

\[
\text{DecNode}(CT, DK, y) = \frac{K_i}{H(GID)} = a^t \cdot \beta_{i}^{-1} \cdot q_y(0) \cdot \beta_i \cdot G = q_y(0) \cdot a^t \cdot G.
\]

For a non-leaf node \( y \), it calls DecNode() for each child \( x \) and stores the result as \( F_x \) in \( ky \)-sized set \( S_y \) of child node \( x \). To reconstruct the value of \( F_y \) at nodes \( y \) using lagrange interpolation, the algorithm proceeds as follows:

\[
F_y = \sum_{x \in S_y} \Delta_{i, s_y}(0) \cdot \text{DecNode}(CT, DK, x)
\]

where \( i = index(x), s'_u = \{index(x), x \in S_u\} \) and \( \Delta_{i, s_y}(0) \) is the lagrange coefficients

\[
= \sum_{x \in S_y} \Delta_{i, s_y}(0) \cdot q_x(0) \cdot a^t \cdot G \\
= \sum_{x \in S_y} \Delta_{i, s_y}(0) \cdot q_{parent(x)}(index(x)) \cdot a^t \cdot G \\
= \sum_{x \in S_y} \Delta_{i, s_y}(0) \cdot q_y(i) \cdot a^t \cdot G \\
= q_y(0) \cdot a^t \cdot G.
\]

Accordingly, the recursive function DecNode(CT, DK, R) at root node \( R \) returns \( q_R(0) \cdot a^t \cdot G \). Finally, the temporal ciphertext CT_temp set as: CT_temp = \{F_R\}.

Decryplocal (K_local, CT_temp) \rightarrow M. After receiving the intermediate ciphertext CT_temp, MDU calculates \{F_R\} × DK = q_R(0) \cdot a^t \cdot G = s \cdot PK = (S_x, S_y). Here, \( S_x \) and \( S_y \) are the recovered keys for decryption and integrity of message M, respectively. Therefore, after decrypting \( M' = Dec(S_x, C_M) \) we can confirm, whether HMAC(S_y, M') = INT_M to assure that the M is correctly received and not being tempered. Hence, the proposed scheme provides confidentiality, authenticity, and integrity of encrypted data, which is the top most priority of any health-related application.
Algorithm 5: DecryptDSP.

Input Delegate key component DK, system public parameter PARAM and CT.

Output Temporal ciphertext CT\textsubscript{temp}.

1. Let \( y \) be a node in \( \mathcal{T} \).
2. If \( i = \text{att}(y) \) is leaf node AND \( i \in S_u \) then.
3. Compute \( F_y = \frac{K_i C_i}{H(GID)} \). 
   \[ H(GID) \cdot \beta_i^{-1} \cdot q_y(0) \cdot PK_i \]
   \[ = \alpha \cdot \beta_i^{-1} \cdot q_y(0) \cdot \beta \cdot G \]
   \[ = q_y(0) \cdot \alpha \cdot G. \]
4. Else
5. Set \( F_y = \text{Null} \).
6. End if.
7. For each non-leaf node \( y \) in \( \mathcal{T} \) do.
8. Let \( s_y \) represent \( k_y \)-sized set of child node \( x \).
9. If no such set exist then
10. Set \( F_y = \text{Null} \).
11. Else
12. Compute lagrange coefficient 
   \[ F_y = \sum_{x \in s_y} \triangle_{i,s_y}(0) \cdot \text{DecNode}(CT, DK, x) \]
   where \( i = \text{index}(x), s_y = \{ \text{index}(x), x \in S_u \} \) and \( \triangle_{i,s_y}(0) \) is the lagrange coefficients
   \[ = \sum_{x \in s_y} \triangle_{i,s}(0) \cdot q_x(0) \cdot \alpha^t \cdot G \]
   \[ = \sum_{x \in s_y} \triangle_{i,s}(0) \cdot q_{\text{parent}(x)}(\text{index}(x)) \cdot \alpha^t \cdot G \]
   \[ = \sum_{x \in s_y} \triangle_{i,s}(0) \cdot q_y(i) \cdot \alpha^t \cdot G \]
   \[ = q_y(0) \cdot \alpha^t \cdot G. \]
13. End if.
14. End for.
15. Let \( R \) represent the root node of \( \mathcal{T} \).
16. If \( F_R \neq \text{Null} \) then recursively compute \( F_R = q_R(0) \cdot \alpha^t \cdot G. \)
17. End if
18. Set the temporal ciphertext \( CT_{\text{temp}} = \{ F_R \} \).

Algorithm 6: Decryptlocal.

Input DU local secret key \( K_{\text{local}} \), and temporal ciphertext \( CT_{\text{temp}} \).

Output Message \( M \).

1. Compute \( F_R \cdot K_{\text{local}} = q_R(0) \cdot \alpha^t \cdot G \times \alpha^{1-t} \)
2. \[ = q_R(0) \cdot \alpha \cdot G \]
3. \[ = s \cdot \alpha \cdot G \]
4. \[ = s \cdot PK \]
5. \[ = (S_x, S_y) \text{ Decrypt } M' = \text{Dec}(S_x, C_M) \text{ and compute } \]
   \[ INT_M' = \text{HMAC}(S_y, M') \].
6. If \( INT_M' = INT_M \) then
7. \( M \) is valid.
8. End if.
9. Return \( M \).

5. Security Analysis

This section, along with security proof, also assesses the proposed scheme’s collision resistance and attribute/user revocation features.
5.1. Security Proof

The security proof of our scheme in the selective security model is presented as a game between the challenger C and an attacker A. In this game, the attacker confronts challenges posed by the challenger to break the underlying hardness assumption. Since our scheme is based on ECC, hence, the attacker’s goal is to reduce the hardness of the elliptic curve decisional Diffie–Hellman (DDH) assumption.

Theorem 1. If an adversary A in the selective-set model successfully attacks our proposed scheme with, at most, advantage ϵ, then it can also build a simulator Sβ that can distinguish an elliptic curve DDH tuple with non-negligible advantage ϵ′.

Proof. Let there exist an adversary A, in the particular set security model that in polynomial time with non-negligible advantage ϵ can break our scheme, then we can build a simulator Sβ to play the ECDDH with advantage ϵ′ in polynomial time.

Firstly, the challenger C generates a EC group G życie with order q and sets over the finite field Z_q^* having a base point G. Then, challenger C takes a fair binary coin μ ∈ {0, 1}, flips it outside of Sβ’s view for some random choices a, b, z ∈ Z_q^*. Now, the choices for μ is given as:

- Case 1. if μ = 0, then ECDDH challenge instance as,
(Α, Β, Ζ) = (c · G, d · G, c · dG), and sent to Sβ.
- Case 2. if μ = 1, then ECDDH challenge instance as,
(Α, Β, Ζ) = (c · G, d · G, z · G), and sent to Sβ.

Initialization: The simulator Sβ runs adversary A, to gets an access structure Τ* that the adversary A wants to be challenged upon.

Setup: The simulator Sβ needs to send the public parameters to adversary A as follows:

1. Sβ at first sets the system parameters Υ = Α = c · G.
2. Then, for ∀ i ∈ U, Sβ sets Yi according to the following condition:
   - If i ∈ U it sets Yi = r_i · G and y_i = r_i where r_i is randomly chooses from Z_q^*.
   - If i ∈ (U − U), it sets Yi = β_i, where β_i is randomly chooses from Z_q^*.
3. Sends the system public parameters {Υ, Y_i, i ∈ U} to A and keeps the secret parameter y_i as secret.

In the above scenario, A does not observe any change as {Υ, Y_i} and y_i are analogous to {PK, PK_i} and β_i of the proposed scheme.

Phase 1: A adoptively calls for a number of secret key components K^1_A, K^2_A, . . ., K^n_A of attribute sets U_1, U_2, . . ., U_n such that all the attribute sets associated to the corresponding secret key components do not satisfy the Τ*. Now, Sβ sends the secret key components K_i to A as follows:

Case 1. if i ∈ U, it sets K_i as
K_i = H(GID) · α^1 · r_i^{-1}  \hspace{5cm} (1)

Case 2. if i ∈ (U − U), it sets K_i as
K_i = H(GID) · α^1 · (β_i · d)^{-1}  \hspace{5cm} (2)

The distribution for both the terms in Equations (1) and (2) is uniform, thus, in A’s perspective, the key components generated by Sβ are the same as the basic scheme.

Challenge: A submits two equal length messages M₀ and M₁ to Sβ. First Sβ sets Τ* = T_{local} ∧ T_{esp} and then sends T_{local} to the DO. It randomly selects S, S₁, S₂ ∈ Z_q^* and sets g_R(0) = S for root node R according to the proposed scheme. Sβ is also sends T_{esp} along with S₁ to ESP (i-e sink node) to distribute it for the remaining attributes in Τ* · Sβ randomly selects a bit b ∈ {0, 1} to encrypt M_b and generates the ciphertext CT* as follows:
\[ SK_{\beta} = S \cdot Y = (S_x, S_y) \]

Hence, \( S_x \) and \( S_y \) represent the encryption and integrity K for message \( M \), respectively. Afterwards, \( S_{\beta} \) computes \( C'_i = r_i \cdot B \).

\( S_{\beta} \) after computing \( C_{\beta} = Enc(M_b, S_x) \) and \( INT_{M_b} = HMAC(M_b, S_y) \) transmits below ciphertext to adversary \( A \).

\[ CT^* = (T^* = T^{*\text{local}} \cup T^{*\text{esp}} \cdot C_{\beta}, INT_{M_b}, C'_i) \]

The challenger \( C \) flips coin \( \mu \in \{0, 1\} \), thus the following cases arises:

- If \( \mu = 0 \); satisfies case 1, which is identical to our original encryption, then \( Z = c \cdot d \cdot G \).

Therefore, if \( S \) is set to \( d \), there should be \( SK_{\beta}' = d \cdot Y = d \cdot c \cdot G = Z \), and \( C_i = G \cdot Y_i = d \cdot r_i \cdot G = r_i \cdot B \), where \( i \in \hat{\Omega} \).

- If \( \mu = 1 \); satisfies case 2, which is different from our proposed scheme, then \( Z = z \cdot G \).

Therefore, if \( S \) is set to \( z \), it turns out that \( SK_{\beta}' = z \cdot Y = z \cdot c \cdot G = Z \), and \( C_i = z \cdot Y_i = z \cdot r_i \cdot G = r_i \cdot Z \).

**Phase 2:** Both \( A \) and \( S_{\beta} \) follow the same steps as they did in Phase 1.

**Guess:** \( A \) output a guess \( b' \) of \( b \) to \( S_{\beta} \).

- If \( b' = b \), \( S_{\beta} \) output \( \mu' = 0 \), which indicates a valid ECDDH instance, \( (A, B, Z) = (c \cdot G, d \cdot G, c \cdot d \cdot G) \).

- If \( b' \neq b \), \( b' \) output \( \mu' = 1 \), which indicates a random instance, \( (A, B, Z) = (c \cdot G, d \cdot G, z \cdot G) \).

Now, according to the security game, where \( \mu = 1 \), the adversary \( A \) cannot predict the \( M_b \), thus we have

\[ Pr[\mu = 1 | b' \neq b] = \frac{1}{2} \quad (3) \]

Since \( S_{\beta} \) outputs \( \mu' = 1 \) when \( b' \neq b \), it gives

\[ Pr[\mu' = 1 | \mu = 1] = \frac{1}{2} \quad (4) \]

When \( \mu = 0 \), the adversary \( A \) can predict the correct \( M_b \), thus we have

\[ Pr[\mu = 0 | b' = b] = \frac{1}{2} + \epsilon \quad (5) \]

Since \( S_{\beta} \) outputs \( \mu' = 0 \) when \( b' = b \), we have

\[ Pr[\mu' = 0 | \mu = 0] = \frac{1}{2} + \epsilon \quad (6) \]

According to the selective set security model of our proposed scheme, the overall advantage using Equations (8) and (10) of \( S_{\beta} \) in this game is

\[ e' = \frac{1}{2} Pr[\mu' = \mu | \mu = 0] + \frac{1}{2} Pr[\mu' = \mu | \mu = 1] - \frac{1}{2} \]

or,

\[ e' = \frac{1}{4} (\frac{1}{2} + \epsilon) + \frac{1}{4} (\frac{1}{2}) - \frac{1}{2} \]

or,

\[ e' = \frac{1}{4} + \frac{\epsilon}{4} + \frac{1}{4} - \frac{1}{2} \]

or,

\[ e' = \frac{\epsilon}{2} \]

Hence, it conflicts with our assumption, which proves the security of our proposed scheme under the ECDDH assumption. \( \square \)
5.2. Secure against Collusion Attack

One of the most anticipated attacks on any attribute-based system is a collision attack. Therefore, it is required of the designers of such a system to implicitly avoid it in their proposed scheme. Let us assume that multiple users possess some secret key components, where no individual secret key has access to the message. If they play the role of an attacker to launch a collision attack (i.e., a combination of their secret keys) by trying to decrypt a message that is encrypted under the intersects (common attributes) of their attributes sets. It is assumed that they constitute secret key components labeled to their common attribute set in the form of

\[
SK_u = (K_0 = \{a^{1-t}\}, K_i = H(GID) \cdot a^t \cdot \beta^{-1})
\]

Even after collectively generating secret keys among themselves, still, they are unable to decrypt the message because of the random selection of \(GID\) for each user to satisfy the equation

\[
\frac{K_i \cdot C_i}{H(GID)} \quad \forall \ i \in \emptyset
\]

Hence, the association of the secret key component with attributes along with a unique global identity \(GID\) and a random number \(t \in Z_p^*\) for each user makes the proposed scheme resistant to collusion attack.

5.3. Attribute/User Revocation

Nowadays, revocation is a desirable property on the part of an ABE-based scheme. Considering the following aspects, equipping the ABE scheme with revocation is not a simple task: First, the attribute authority labeled each user secret key from a universal set of attributes instead of a unique user-specific attribute. As a result, a malicious user cannot simply be singled out on an attribute or set of attributes; second, after the revocation of a misbehaving user, the system must avoid the collusion attack even if there exists the overlapping of attributes with non-revoked users. The ABE scheme supports two types of revocation, direct revocation and indirect revocation, to address these issues. Indirect revocation incurs the liability on TAA to update and distribute the non-revoked users’ secret key with every revocation event. In direct revocation, we do not need to perform updation on the secret key of non-revoked users. All contemporary direct revocation schemes require system users to maintain an updated and long list of revoked users, which must be labeled to ciphertext. This computation and storage overhead linearly increases with the increase in revoked users in the encryption and decryption algorithms system.

Given the resource-constrained and medical-centric characteristics of our proposed scheme MAA, the indirect revocation fits aptly into our eHealth practical scenario. The computation and storage cost of our scheme is independent of the number of revoked users. The KGC of MAA explicitly maintains the list of global IDs GID and its associated attribute lists for each registered user. To revoke the system attribute from its universal set of attributes, the KGC deletes the associated system attribute’s public key. Similarly, to revoke the user-specific attribute, the KGC must delete the corresponding secret key component for that specific user. Further, KGS deletes the entire attribute set and the GID assigned to that user to revoke a user. For all of these revocation scenarios, the MAA needs to update the delegated key \(DK\) with the help of MSK and the revoked \(DK_\beta\) of the revoked attribute \(\beta\) and produces a new delegate key \(DK_\beta^*\) of the revoked attribute \(\beta\). Furthermore, our proposed scheme avoids the need for maintaining a private channel between the MAA and the non-revoked user for the dissemination of the updated delegated key \(DK_\beta^*\).

6. Performance Analysis

In this section, we compare our proposed scheme with five related schemes in [19–23], in terms of its features, communication overhead, and computation overhead. Moreover, for the sake of fair comparison, we set \(n = 20\) and \(m = 10\) representing attributes in universal set and encryption, respectively.
6.1. Features Analysis

Table 2 depicts the comparison of various features of our scheme with related schemes for a WBAN from four perspectives: encryption delegation, decryption delegation, integrity check, and attribute revocation. Additionally, our proposed scheme lacks time-based access control and hierarchical access control support. In some practical scenarios, it is inevitable to provide access control for a specific time interval. For instance, a medical document may have different privacy requirements for a different period. More specifically, fewer medical experts have access to the medical record at an early time, while more experts can get access to it at a later time point. Similarly, the hierarchical access permission ensures access to the corresponding documents based on the specific role of the data users. For example, the hospital president can access all the information of the patients and doctors, while the medical experts can access his/her patient information only.

| Scheme                          | [19] | [20] | [21] | [22] | [23] | Proposed |
|---------------------------------|------|------|------|------|------|----------|
| Encrypt Delegation              | ✓    | ✓    | ✓    | ✓    | ✓    | ✓        |
| Decrypt Delegation              | ×    | ✓    | ✓    | ✓    | ✓    | ✓        |
| Integrity Check                 | ×    | ×    | ×    | ✓    | ✓    | ✓        |
| Attribute Revocation            | ×    | ×    | ×    | ×    | ×    | ✓        |

6.2. Communication Overhead

Communication overhead relates to the transfer of the message. In the most commonly adopted architectures of ABE, the least number of messages that should be transmitted are of the public key, private key, and ciphertext. For the sake of analysis, we take the length of these messages as a metric to determine and compare the relative communication overhead.

Most contemporary ABE schemes use bilinear pairing; a map involves two groups $G_1, G_T$. Because of the underlying modular exponentiation, these are termed RSA-based ABE schemes. Accordingly, we call our scheme an ABE ECC-based scheme.

As we know, ECC has much stronger hit security; we considered 160-bit, i.e., secp160r1 elliptic curve, which has up to 1024-bit RSA security strength. Based on the above-stated assumptions, the size of both public and private keys in the ABE RSA-based scheme is 1024-bit, while the size of an element in $G_1$ and $G_T$ is 1024 bits and 2048-bits. Accordingly, the size of an elliptic curve point is 320 bits, corresponding to both its coordinates. As a result, the 160 bits and 320 bits constitute the private key and public key size, respectively, in ABE ECC-based schemes. For comparison, the communication overhead is identical for each ABE RSA-based scheme. Therefore, we compute the [23] overhead for illustration purposes. The ciphertext in [23] scheme is given by $CT = (C = Me(g, g)^{\alpha s}, C' = g^{\alpha t}, \{C_i = g^{\alpha h_i}g^{-r_i}H^{\text{att}(o)}, D_i = g^{\alpha i} | i \in m\})$, where $m$ represents the maximum number of attributes attached to the ciphertext. According to the setup phase of this scheme, $g$ and $e(g,g)$ belong to the group $G_1$ and $G_T$, respectively. As a result, the size of each ciphertext component $C, C', C_i, r_i$ and $D_i$ is 2048, 1024, $(2m \times 1024)$ and $(m \times 1024)$ bits, respectively. In this way, the length of ciphertext CT is $(3m + 3) \times 1024 \approx 33,792$ bits. Here, the public key is set to $PK = \{g, e(g,g)^s, g^s, H\}$, so its length is $4 \times 1024 \approx 4096$ bits. In addition, the private key is given by $K = \{g^s, I = g^{t_i}, \{K_x = g^{H^{\text{att}(o)}x} | x \in S\}\}$ where $S$ represents the user set of attributes associated to the key $K$. Therefore, the length of the private key of scheme [23] computes to $(m + 3) \times 1024 \approx 13,312$ bits.

Similarly, we compute the public key, private key, and ciphertext length in our scheme. According to the encryption process of our proposed scheme, the ciphertext is $CT = (T, C_m, INT_m, C_y = q_y(0) \cdot PK_y | y \in T)$. The size of attribute set T is taken constantly for all schemes and, hence, rolled out of the total ciphertext size. Here, $C_m$ and $INT_m$ are the single coordinates on the elliptic curve, each having 160 bits in length. Similarly, $C_y$ consists of 320 bits, a single point on the elliptic curve. Thus, the length of the ciphertext in our proposed scheme computes to $(m + 1) \times 320 \approx 3520$ bits. The public key components in
our scheme are \((PK, \{PK_i | i \in U\})\), and consists of \((n + 1) \times 320 \approx 6720\) bits, as each of its components is a single point on the elliptic curve. The private key of our scheme is 
\(K_{\text{local}} = (\alpha^{1-t})\), \(DK = (\forall i \in S_u: K_i = H(GID) \cdot a^t \cdot \beta^{-1})\). Hence, its length computes to \((m + 1) \times 160 \approx 1760\) bits.

We can see from Table 3 that the ciphertext and private key sizes of our proposed scheme are significantly lower than those of all other schemes. We can observe from Table 3 that only the length of the public key in our proposed scheme is higher than the scheme with a constant-size public key [19,23]. However, overall communication overhead for the private key, the public key, and ciphertext size in our scheme is significantly lower than that of [19]. Moreover, the scheme in [23] is based on KP-ABE as opposed to our CP-ABE-based scheme, which provides more control to the patient over the recipient of its sensitive medical data. Moreover, the generation of the public key is a one-time process in the lifetime of the system.

### Table 3. Parameters size (bits).

| Scheme  | Private Key Size | Public Key Size | Ciphertext Size |
|---------|-----------------|-----------------|-----------------|
| [19]    | \((2m + 2) \times 1024 \approx 22,522\) | \((3 \times 1024) \approx 3072\) | \((2m + 2) \times 1024 \approx 22,528\) |
| [20]    | \((5m + 3) \times 1024 \approx 54,272\) | \((n + 3) \times 1024 \approx 23,552\) | \((2m + 3) \times 1024 \approx 23,552\) |
| [21]    | \((m + 4) \times 1024 \approx 14,336\) | \((n + 4) \times 1024 \approx 24,576\) | \((2m + 3) \times 1024 \approx 23,552\) |
| [22]    | \((3m + 1) \times 1024 \approx 31,744\) | \((n + 3) \times 1024 \approx 23,552\) | \((2m + 1) \times 1024 \approx 21,504\) |
| [23]    | \((m + 3) \times 1024 \approx 13,312\) | \((4 \times 1024) \approx 4096\) | \((3m + 3) \times 1024 \approx 33,792\) |
| Proposed| \((m + 1) \times 160 \approx 1760\) | \((n + 1) \times 320 \approx 6720\) | \((m + 1) \times 320 \approx 3520\) |

### 6.3. Computation Overhead

The computation overhead is mainly caused by the ABE scheme operations, including bilinear pairing, ECC-based scalar point multiplication, exponentiation, hashing, basic arithmetic, and logical operations. We have considered the most expensive exponentiation operations, bilinear pairing, and elliptic curve base scalar point multiplications. Comparatively, the cost of other least costly operations can be ignored [3]. For the sake of simplicity, Table 4, based on [37], is constructed, which shows the execution time (in millisecond) required by each group operation. According to work in [37], single bilinear pairing and modular exponentiation operation is about 10 and 2 times ECC-based scalar point multiplication, respectively.

To evaluate the computation overhead of the proposed scheme, we need the individual computation overhead of users and service providers on both the encryption and decryption sides. Therefore, in Table 5, we compare the computation overhead incurred on MDO and ESP in the encryption offloading and the MDU and DSP in the decryption offloading. As our scheme is free from costly pairing operations, all matrices’ execution time is comparatively less than other schemes. We can also see from Table 5 that the unwanted linearity property of ABE is shifted to comparatively resource-rich server providers (DSP and ESP). Hence, the data users are left with a significantly less and constant number of operations. Thus, based on the performance assessments, our scheme demonstrates more efficiency and the best solution for a WBAN in terms of communication, computation, and security.

### Table 4. Execution time for cryptographic operations.

| Operations | \(T_{BP}\) | \(T_{EXP}\) | \(T_{PM}\) |
|------------|-----------|-------------|-----------|
| Time (ms)  | 20.04     | 5.31        | 2.21      |
Table 5. Computational overhead (ms).

| Scheme     | KeyGen     | $\text{Enc}_{\text{Local}}$ | $\text{Enc}_{\text{Out}}$ | $\text{Dec}_{\text{Local}}$ | $\text{Dec}_{\text{Out}}$ |
|------------|------------|-----------------------------|-----------------------------|-----------------------------|-----------------------------|
| [19]       | ($1 + 3m$) $T_{EX} \approx 164.61$ | $5T_{EX} \approx 26.55$ | $2mT_{EX} \approx 106.2$ | $2m(T_{BP} + T_{EX}) \approx 507$ | - |
| [20]       | ($7m + 5$) $T_{EX} \approx 398.25$ | $4 + 2m$ $T_{EX} \approx 127.44$ | - | $T_{EX} \approx 5.31$ | $2m(T_{BP} + T_{EX}) + 2T_{BP} \approx 547.08$ |
| [21]       | ($3m + 7$) $T_{EX} \approx 196.47$ | ($2m + 3$) $T_{EX} \approx 122.13$ | ($2m + 1$) $T_{EX} \approx 111.51$ | ($T_{EX}) \approx 5.31$ | ($2m + 1)$ $T_{BP} + (3m + 1)$ $T_{EX} \approx 584.61$ |
| [22]       | ($1 + 4m$) $T_{EX} \approx 217.71$ | ($5T_{EX}) \approx 26.55$ | ($2m - 2$) $T_{EX} \approx 95.98$ | ($T_{BP} + 2T_{EX}) \approx 30.66$ | $2m(T_{BP} + T_{EX}) \approx 508.8$ |
| [23]       | ($m + 4$) $T_{EX} \approx 127.44$ | $4T_{EX} \approx 21.24$ | $3mT_{EX} \approx 159.3$ | $T_{BP} \approx 20.04$ | $2mT_{EX}mT_{BP} \approx 306.4$ |
| Proposed   | ($m + 1$) $T_{EX} \approx 111.51$ | $2T_{PM} \approx 4.42$ | ($m - 2$) $T_{PM} \approx 17.68$ | $T_{PM} \approx 2.21$ | $2mT_{PM} \approx 44.2$ |

6.4. Rank-Based Evaluation of Performance Matrices

In this research work, a fuzzy logic-based evaluation, which is constructed on the method distance from average solution (EDAS), is used for calculating the ranking of the proposed scheme with state-of-the-art algorithms in terms of computational cost operations, such as KeyGen, $\text{Enc}_{\text{Local}}$, $\text{Enc}_{\text{Out}}$, $\text{Dec}_{\text{Local}}$, and $\text{Dec}_{\text{Out}}$, on both the sides of the sender and receiver to find the top rank efficiency of these schemes. The above-stated performance matrices/operations are compared with existing state-of-the-art schemes, including the proposed scheme in this section.

In this evaluation, the authors use the EDAS approach to collect the cross-efficient values of numerous parameters of five schemes, including the proposed scheme. The aggregate of appraisal scores ($\lambda$) can be measured for ranking of given schemes to compute the positive distance from the average solution, which is represented in the equation as ($P_\beta$) and the negative distance from the average solution is represented by the symbol ($N_\beta$).

In Table 6 below, the performance matrices are deliberated as the criteria of state-of-the-art schemes.

Table 6. Analysis results of average.

| Scheme     | Performance Metrics |
|------------|---------------------|
|            | KeyGen  | $\text{Enc}_{\text{Local}}$ | $\text{Enc}_{\text{Out}}$ | $\text{Dec}_{\text{Local}}$ | $\text{Dec}_{\text{Out}}$ |
| [19]       | 0.1877  | 0.5148              | 0                         | 0                         | 1                         |
| [20]       | 0       | 0                    | 1                         | 0.9441                    | 0                         |
| [21]       | 0       | 0                    | 0.3                      | 0.7350                    | 0                         |
| [22]       | 0       | 0.5148              | 0                         | 0.6725                    | 0                         |
| [23]       | 0.3711  | 0.6118              | 0.7383                   | 0.9767                    | 0.8666                    |
| Proposed   | 0.4497  | 0.9192              | 0.7838                   | 0.9767                    | 0.8666                    |

**Step 1**: Calculate the solution of the average value ($\psi$) of all matrices in Equation (7);

$$ (\psi_\beta) = [\psi_\beta]_{1 \times \delta} \tag{7} $$

where,

$$ (\psi) = \frac{\sum_{i=1}^{x} X_{i\beta}}{x} \tag{8} $$

The above steps define the performance matrices as benchmarks of various schemes. The calculation of aggregate in Equations (7) and (8) can be gained as the average value ($\psi$) for each calculated benchmark value against each given value in Table 7.
Table 7. Cross-efficient values.

| Scheme       | KeyGen | EncLocal | EncOut  | DecLocal | DecOut  |
|--------------|--------|----------|---------|----------|---------|
| [19]         | 164.61 | 26.55    | 106.2   | 507      | 0       |
| [20]         | 398.25 | 127.44   | 0       | 5.31     | 547.08  |
| [21]         | 196.47 | 122.13   | 111.51  | 5.31     | 584.61  |
| [22]         | 217.71 | 26.55    | 95.98   | 30.66    | 506.8   |
| [23]         | 127.44 | 21.24    | 159.3   | 20.04    | 306.4   |
| Proposed     | 111.51 | 4.42     | 17.68   | 2.21     | 44.2    |
| $\psi_\beta$ | 202.665| 54.7216  | 81.7783 | 95.0883  | 331.515 |

Step 2: In this step of the EDAS method, the positive distance from the average is denoted as $(P_\alpha)$, and is calculated as shown in Equations (9)–(11) as given below:

\[ P_\alpha = [(P_\alpha)_{\alpha\beta}]_{\delta \times \delta} \]  
\[ (P_\alpha)_{\alpha\beta} = \text{Maximum}(0, \frac{(A_{\beta} - X_{\alpha\beta})}{A_{\beta}}) \]  
\[ (P_\alpha)_{\alpha\beta} = \text{Maximum}(0, \frac{(X_{\alpha\beta} - A_{\beta})}{A_{\beta}}) \]

The results replicate in Table 8 following as:

Step 3: In this step of the EDAS, the negative distance from the average is denoted as $(N_\alpha)$, and is calculated using Equations (12), (13) and (15) as follows:

\[ (N_\alpha) = [(N_\alpha)_{\alpha\beta}]_{\delta \times \delta} \]  
\[ (N_\alpha)_{\alpha\beta} = \text{Maximum}(0, \frac{(A_{\beta} - X_{\alpha\beta})}{A_{\beta}}) \]  
\[ (N_\alpha)_{\alpha\beta} = \text{Maximum}(0, \frac{(X_{\alpha\beta} - A_{\beta})}{A_{\beta}}) \]

The results reproduced are shown in Table 8 as:
Table 8. Analysis results of average \((N_3)\).

| Scheme | Performance Metrics | KeyGen | Enc\textsubscript{Local} | Enc\textsubscript{Out} | Dec\textsubscript{Local} | Dec\textsubscript{Out} |
|--------|---------------------|--------|-----------------|-----------------|-----------------|-----------------|
| [19]   |                     | 0      | 0               | 0.2986          | 4.3318          | 0               |
| [20]   |                     | 0.9650 | 1.3288          | 0               | 0               | 0.6502          |
| [21]   |                     | 0      | 1.2318          | 0.3635          | 0               | 0.7634          |
| [22]   |                     | 0.9523 | 5.0067          | 4.4287          | 12.8733         | 10.4660         |
| [23]   |                     | 0      | 0               | 0.9479          | 0               | 0               |
| Proposed |                   | 0      | 0               | 0               | 0               | 0               |

Step 4: In this step, the weighted sum of \((P_3)\) for the rated algorithms in Table 9 is shown below:

\[
(SP_3)_\alpha = \sum_{\beta=1}^{\chi} y_\beta (P_3)_{\alpha\beta}
\]  

Table 9. Analysis results of the aggregate \((P_3)\).

| Criteria (W) | 0.4176 | 0.2850 | 0.1453 | 0.0844 | 0.0676 |
|--------------|--------|--------|--------|--------|--------|

| Scheme | Performance Metrics | KeyGen | Enc\textsubscript{Local} | Enc\textsubscript{Out} | Dec\textsubscript{Local} | Dec\textsubscript{Out} |
|--------|---------------------|--------|-----------------|-----------------|-----------------|-----------------|
| [19]   |                     | 0.0784 | 0.1467          | 0               | 0               | 0.0676          |
| [20]   |                     | 0      | 0               | 0.1453          | 0.0796          | 0               |
| [21]   |                     | 0.0127 | 0               | 0               | 0.0796          | 0               |
| [22]   |                     | 0      | 0               | 0               | 0               | 0               |
| [23]   |                     | 0.1550 | 0.1743          | 0               | 0.0666          | 0.0051          |
| Proposed |                   | 0.1878 | 0.2619          | 0.1139          | 0.0824          | 0.0586          |

Proposed 0 0 0 0 0 0

Step 5: In this step, the weighted sum of \((N_3)_{\alpha\beta}\) for the rated algorithms in Table 10 is shown below in Equation (16):

\[
(SN_3)_\alpha = \sum_{\beta=1}^{\chi} y_\beta (N_3)_{\alpha\beta}
\]  

The results obtained are reflected in Table 10 as shown:

Table 10. Analysis results of the aggregate \((N_3)\).

| Criteria (W) | 0.4176 | 0.2850 | 0.1453 | 0.0844 | 0.0676 |
|--------------|--------|--------|--------|--------|--------|

| Scheme | Performance Metrics | KeyGen | Enc\textsubscript{Local} | Enc\textsubscript{Out} | Dec\textsubscript{Local} | Dec\textsubscript{Out} |
|--------|---------------------|--------|-----------------|-----------------|-----------------|-----------------|
| [19]   |                     | 0      | 0               | 0.0434          | 0.3656          | 0               |
| [20]   |                     | 0.4030 | 0.3787          | 0               | 0               | 0.0439          |
| [21]   |                     | 0      | 0.3510          | 0.0528          | 0               | 0.0516          |
| [22]   |                     | 0      | 0               | 0               | 0               | 0               |
| [23]   |                     | 0      | 0               | 0.1377          | 0               | 0.1377          |
| Proposed |                   | 0      | 0               | 0               | 0               | 0               |

Proposed 0 0 0 0 0
Step 6: In this step, the normalized scores of $(SPI)\alpha$ and $(SNI)\alpha$ for the rated algorithms are calculated as presented in Equations (17) and (18):

$$N(SP\alpha) = \frac{(SP\alpha)}{\text{maximum}_\alpha((SP\alpha))}$$  \hspace{1cm} (17)

$$N(SNI\alpha) = 1 - \frac{(SNI\alpha)}{\text{maximum}_\alpha((SNI\alpha))}$$  \hspace{1cm} (18)

Step 7: In this step, the scores of $N(SP\alpha)$ and $N(SNI\alpha)$ to receive an appraisal score ($AS$) is calculated, which is equal to $(\lambda)$ for the rated algorithms given in Equation (19).

$$\lambda_\alpha = \frac{1}{2}(N(SP\alpha) - N(SNI\alpha))$$  \hspace{1cm} (19)

where $0 \leq \lambda_\alpha \leq 1$.

The $(\lambda)$ is determined by the aggregate score of $NSP_m$ and $NSN_m$.

Step 8: In this step, measurement of the appraisal scores $(\lambda)$ in terms of decreasing order and then concluding of the ranking of rated algorithms is performed. The paramount ranking algorithms have the higher $(\lambda)$. Thus, in Table 11 below, the proposed algorithm has the highest $(\lambda)$.

The final results of the overall ranking are represented in Table 11:

| Scheme | $(SP\alpha)_a$ | $(SNI\alpha)_a$ | $N(SP\alpha)_a$ | $N(SNI\alpha)_a$ | $\lambda_\alpha$ | Ranking |
|--------|----------------|-----------------|----------------|----------------|----------------|---------|
| [19]   | 0.2927         | 0.4090          | 0.4154         | 0.5046         | 0.4600         | 4       |
| [20]   | 0.2250         | 0.8257          | 0.3192         | 0              | 0.1596         | 6       |
| [21]   | 0.0924         | 0.4555          | 0.1311         | 0.4483         | 0.2897         | 5       |
| [22]   | 0              | 0               | 0              | 1              | 0.5            | 3       |
| [23]   | 0.4011         | 0.1377          | 0.5691         | 0.8331         | 0.7011         | 2       |
| Proposed | 0.7047        | 0               | 1              | 1              | 1              | 1       |

The ranking shows that the proposed algorithm is the best out of five total state-of-the-art algorithms in the stated research domain.

7. Conclusions and Future Work

In summary, we present a secure and efficient ABE architecture with outsourcing intense encryption and delegation operations. Further, leverage on the lightweight features of ECC and the primitive syntax of CP-ABE, our scheme reduces the computation cost of both encryption and decryption on the user side into a constant. Our solution enables the resource-scarce and lightweight WBAN sensors to securely upload and retrieve sensitive medical data in public clouds with a minimum constant cost. The inherent features of attribute/user revocation and verifiability of outsourcing data further strengthen the security of our scheme. The proposed scheme is found to be secured under the ECDDH assumption using the selective-set security model. The performance assessment of our scheme shows a significant overall efficiency in terms of storage, computation, and communication. Further, for better clarification and evaluation, the final outputs of the EDAS ranking method show that the proposed approach is on the top rank that noticeably reported the proposed scheme’s outperformance than the other reference schemes. We will investigate the incorporation of time-based access control and hierarchical access control in our research work as future work.
Author Contributions: Formal analysis, S.K. (Shahzad Khan), A.W., G.M. and S.K. (Shawal Khan); funding acquisition, M.Z. and R.R.B.; investigation, G.M.; methodology, S.K. (Shahzad Khan), W.I. and S.K. (Shawal Khan); project administration, R.R.B.; supervision, W.I.; writing—original draft, S.K. (Shahzad Khan); writing—review and editing, A.W. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the School of Engineering and Sciences at Tecnologico de Monterrey.

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

References
1. Ali, S.T.; Sivaraman, V.; Ostry, D. Zero reconciliation secret key generation for body-worn health monitoring devices. In Proceedings of the Fifth ACM conference on Security and Privacy in Wireless and Mobile Networks, Tucson, AZ, USA, 16–18 April 2012; pp. 39–50. [CrossRef]
2. Khan, S.; Khan, S.; Zareei, M.; Alanazi, F.; Kama, N.; Alam, M.; Anjum, A. ABKS-PBM: Attribute-Based Keyword Search With Partial Bilinear Map. IEEE Access 2021, 9, 46313–46324. [CrossRef]
3. Yao, X.; Chen, Z.; Tian, Y. A lightweight attribute-based encryption scheme for the Internet of Things. Future Gener. Comput. Syst. 2015, 49, 104–112. [CrossRef]
4. Hu, C.; Li, H.; Huo, Y.; Xiang, T.; Liao, X. Secure and efficient data communication protocol for wireless body area networks. IEEE Multi-Scale Comput. Syst. 2016, 2, 94–107. [CrossRef]
5. Belguith, S.; Jemai, A.; Attia, R. Enhancing data security in cloud computing using a lightweight cryptographic algorithm. In Proceedings of the 11th International Conference on Autonomic and Autonomous Systems, Rome, Italy, 24–29 May 2015; pp. 98–103.
6. Li, Y.; Wang, G.; Nie, L.; Wang, Q.; Tan, W. Distance metric optimization driven convolutional neural network for age invariant face recognition. Pattern Recognit. 2018, 75, 51–62. [CrossRef]
7. Nogueira, R.F.; de Alencar Lotufo, R.; Machado, R.C. Fingerprint liveness detection using convolutional neural networks. IEEE Trans. Inf. Forensics Secur. 2016, 11, 1206–1213. [CrossRef]
8. Zhang, Y.; Qiu, M.; Tsai, C.W.; Hassan, M.M.; Alami, A. Health-CPS: Healthcare cyber-physical system assisted by cloud and big data. IEEE Syst. J. 2015, 11, 88–95. [CrossRef]
9. Shi, W.; Cao, J.; Zhang, Q.; Li, Y.; Xu, L. Edge computing: Vision and challenges. IEEE Internet Things J. 2016, 3, 637–646. [CrossRef]
10. Zhang, Q.; Zhang, Q.; Shi, W.; Zhong, H. Distributed collaborative execution on the edges and its application to amber alerts. IEEE Internet Things J. 2018, 5, 3580–3593. [CrossRef]
11. Zhang, Q.; Sun, H.; Wu, X.; Zhong, H. Edge video analytics for public safety: A review. Proc. IEEE 2019, 107, 1675–1696. [CrossRef]
12. Sun, X.; Zhang, P.; Sookhak, M.; Yu, J.; Xie, W. Utilizing fully homomorphic encryption to implement secure medical computation in smart cities. Pers. Ubiquitous Comput. 2017, 21, 831–839. [CrossRef]
13. Cai, Z.; Yan, H.; Li, P.; Huang, Z.a.; Gao, C. Towards secure and flexible EHR sharing in mobile health cloud under static assumptions. Clust. Comput. 2017, 20, 2415–2422. [CrossRef]
14. Green, M.; Hohenberger, S.; Waters, B. Outsourcing the decryption of abe ciphertexts. In Proceedings of the USENIX Security Symposium, San Francisco, CA, USA, 8–12 August 2011; Volume 2011, no.3.
15. Chen, L.; Hoang, D.B. Novel data protection model in healthcare cloud. In Proceedings of the 2011 IEEE International Conference on High Performance Computing and Communication, Banff, AB, Canada, 2–4 September 2011; pp. 550–555.
16. Waters, B. Efficient identity-based encryption without random oracles. In Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, 22–26 May 2005.
17. Goyal, V.; Pandey, O.; Sahai, A.; Waters, B. Attribute-based encryption for fine-grained access control of encrypted data. In Proceedings of the 13th ACM Conference on COMPUTER and Communications Security, Alexandria, VA, USA, 30 October 30–November 2006; pp. 89–98.
18. 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; pp. 321–334.
19. Li, J.; Jia, C.; Li, J.; Chen, X. Outsourcing encryption of attribute-based encryption with mapreduce. In Proceedings of the International Conference on Information and Communications Security, Chongqing, China, 17–19 September 2012; pp. 191–201.
20. Li, J.; Huang, X.; Li, J.; Chen, X.; Xiang, Y. Securely outsourcing attribute-based encryption with checkability. IEEE Trans. Parallel Distrib. Syst. 2013, 25, 2201–2210. [CrossRef]
21. Asim, M.; Petkovic, M.; Ignatenko, T. Attribute-based encryption with encryption and decryption outsourcing. In Proceedings of the 12th Australian Information Security Management Conference, Perth, Australia, 1–3 December 2014.
22. Zhong, H.; Zhou, Y.; Zhang, Q.; Xu, Y.; Cui, J. An efficient and outsourcing-supported attribute-based access control scheme for edge-enabled smart healthcare. Future Gener. Comput. Syst. 2021, 115, 486–496. [CrossRef]
23. Li, Z.; Li, W.; Jin, Z.; Zhang, H.; Wen, Q. An efficient ABE scheme with verifiable outsourced encryption and decryption. IEEE Access 2019, 7, 29023–29037. [CrossRef]
24. Khan, S.; Zareei, M.; Khan, S.; Alanazi, F.; Alam, M.; Waheed, A. OO-ABMS: Online/Offline-Aided Attribute-Based Multi-Keyword Search. *IEEE Access* **2021**, *9*, 114392–114406. [CrossRef]

25. Pang, L.; Yang, J.; Jiang, Z. A survey of research progress and development tendency of attribute-based encryption. *Sci. World J.* **2014**, *2014*, 193426. [CrossRef]

26. Catarinucci, L.; De Donno, D.; Mainetti, L.; Palano, L.; Patrono, L.; Stefanizzi, M.L.; Tarricone, L. An IoT-aware architecture for smart healthcare systems. *IEEE Internet Things J.* **2015**, *2*, 515–526. [CrossRef]

27. Tan, S.Y.; Yeow, K.W.; Hwang, S.O. Enhancement of a lightweight attribute-based encryption scheme for the internet of things. *IEEE Internet Things J.* **2019**, *6*, 6384–6395. [CrossRef]

28. Tan, Y.L.; Goi, B.M.; Komiya, R.; Tan, S.Y. A study of attribute-based encryption for body sensor networks. In Proceedings of the International Conference on Informatics Engineering and Information, Kuala Lumpur, Malaysia, 14–16 November 2011.

29. Tian, Y.; Peng, Y.; Peng, X.; Li, H. An attribute-based encryption scheme with revocation for fine-grained access control in wireless body area networks. *Int. J. Distrib. Sens. Netw.* **2014**, *10*, 259798. [CrossRef]

30. Coyne, E.J.; Feinstein, H.; Sandhu, R.; Youman, C.E. Role-based access control models. *IEEE Comput.* **1996**, *29*, 38–47.

31. Sowjanya, K.; Dasgupta, M. A ciphertext-policy Attribute based encryption scheme for wireless body area networks based on ECC. *J. Inf. Secur. Appl.* **2020**, *54*, 102559. [CrossRef]

32. Basar, S.; Ali, M.; Ochoa-Ruiz, G.; Waheed, A.; Rodriguez-Hernandez, G.; Zareei, M. A Novel Defocused Image Segmentation Method based on PCNN and LBP. *IEEE Access* **2021**, *9*, 87219–87240. [CrossRef]

33. Mehmood, G.; Khan, M.Z.; Waheed, A.; Zareei, M.; Mohamed, E.M. A trust-based energy-efficient and reliable communication scheme (trust-based ERCS) for remote patient monitoring in wireless body area networks. *IEEE Access* **2020**, *8*, 131397–131413. [CrossRef]

34. Basar, S.; Ali, M.; Ochoa-Ruiz, G.; Zareei, M.; Waheed, A.; Adnan, A. Unsupervised color image segmentation: A case of RGB histogram based K-means clustering initialization. *PLoS ONE* **2020**, *15*, e0240015. [CrossRef]

35. Sahai, A.; Waters, B. Fuzzy identity-based encryption. In Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, 22–26 May 2005.

36. Cao, Q.; Li, Y.; Wu, Z.; Miao, Y.; Liu, J. Privacy-preserving conjunctive keyword search on encrypted data with enhanced fine-grained access control. *World Wide Web* **2020**, *23*, 959–989. [CrossRef]

37. Karati, A.; Amin, R.; Biswas, G. Provably secure threshold-based abe scheme without bilinear map. *Arab. J. Sci. Eng.* **2016**, *41*, 3201–3213. [CrossRef]