




Article

# An IoT-Based Anonymous Function for Security and Privacy in Healthcare Sensor Networks

Xiao Chun Yin <sup>1</sup>, Zeng Guang Liu <sup>2</sup>, Bruce Ndibanje <sup>3</sup>, Lewis Nkenyereye <sup>4,\*</sup> and S. M. Riazul Islam <sup>5</sup>

<sup>1</sup> Facility Horticulture Laboratory of Universities in Shandong, Weifang University of Science & Technology, Shouguang 262700, China

<sup>2</sup> College of Computer Science and Engineering, Shandong University of Science and Technology, Qingdao 266590, China

<sup>3</sup> Research and Development Center, Cyber Threat Intelligence Lab, YangJae Innovation Hub, 114 Taebong-Ro, Seocho-Gu, Seoul 06754-601, Korea

<sup>4</sup> Department of Computer and Information Security, Sejong University, Seoul 05006, Korea

<sup>5</sup> Department of Computer Science and Engineering, Sejong University, Seoul 05006, Korea

\* Correspondence: nkenyele@sejong.ac.kr

Received: 6 June 2019; Accepted: 15 July 2019; Published: 17 July 2019



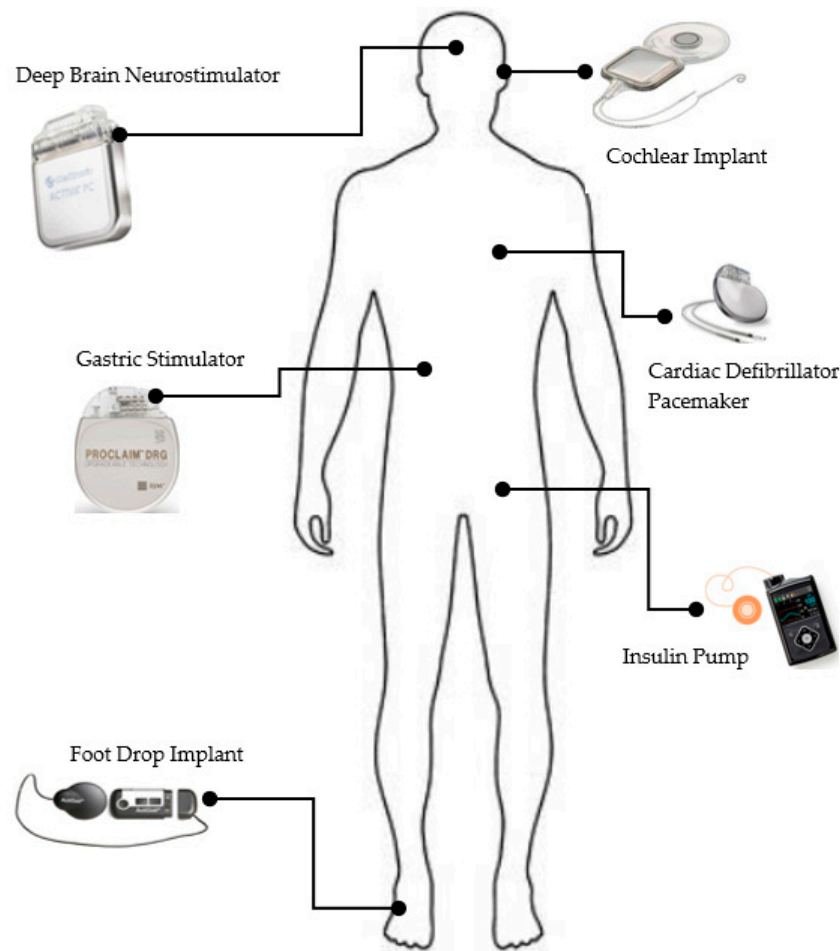
**Abstract:** In the age of the Internet of Things, connected devices are changing the delivery system in the healthcare communication environment. With the integration of IoT in healthcare, there is a huge potential for improvement of the quality, safety, and efficiency of health care in addition to promising technological, economical, and social prospects. Nevertheless, this integration comes with security risks such as data breach that might be caused by credential-stealing malware. In addition, the patient valuable data can be disclosed when the perspective devices are compromised since they are connected to the internet. Hence, security has become an essential part of today's computing world regarding the ubiquitous nature of the IoT entities in general and IoT-based healthcare in particular. In this paper, research on the algorithm for anonymizing sensitive information about health data set exchanged in the IoT environment using a wireless communication system has been presented. To preserve the security and privacy, during the data session from the users interacting online, the algorithm defines records that cannot be revealed by providing protection to user's privacy. Moreover, the proposed algorithm includes a secure encryption process that enables health data anonymity. Furthermore, we have provided an analysis using mathematical functions to valid the algorithm's anonymity function. The results show that the anonymization algorithm guarantees safety features for the considered IoT system applied in context of the healthcare communication systems.

**Keywords:** IoT; security; privacy; anonymous function; healthcare; wireless sensor networks

## 1. Introduction

Nowadays, medical caregivers are able to monitor the patient's status in real-time and the relevant status can be updated time-to-time using applications and infrastructures. The connectivity protocol based on the IPv6 low-power wireless personal area network is the most used in the IoT environment to support healthcare mobility via wireless approaches [1]. Modern healthcare is reshaping the presence and evolution of the IoT that support technology, economy, and social networks. The IoT state-of-the-art reflects an inter-connection of people, anything, accessing any service anytime, anywhere and on any network. It is seen as a megatrend technology in information and communication technology (ICT) that is influencing the entire business spectrum with more advantages going beyond machine-to-machine (M2M) states [2]. The solutions provided by the IoT are now exploitable in multiple areas of applications like logistics, industrial control, smart cities, transportation, retails and healthcare systems [3–7].

Among the aforementioned applications areas and others, the attention is given to the healthcare system, which represents the most attractive application for developers and consumers [8]. The main reason is that the human being is much involved for applications such as elderly care, fitness programs, remote health care monitoring and chronic diseases surveillance. Figure 1 gives a generic illustration of a body area network consisting of IoT medical sensors.



**Figure 1.** Overview of a patient's body with IoT medical sensors.

The health devices collect and transmit patient health data to the medical service providers for data analytics and visualizations to facilitate health monitoring and treatment. As shown in Figure 1, the sensors can be embedded into the body. They are smart electronic devices equipped with a micro-controller to compute different functions. Therefore, in IoT-based health care, the devices are inter-connected, embedded with software and use a wireless communication system to exchange the data [9].

However, security and privacy are highly discussed in such context given that devices or/and software's compromises directly leads to the safety of the user (here, patient) and can thus cause harmful consequences, even a death. Most of the privacy and security solutions for healthcare systems are discussed in Section 2. Using wireless technologies, any user with his sensitive data such as bank transactions, health data, and email should exchange via a platform that provide the user's privacy and ensures the security of their information. Nevertheless, in a centralized system such as IoT-based health care, the services providers can access the data and have capabilities to possibly perform a-priori or a-posteriori control or reveal the sender's message in their system to other entities, irrespective of the concerned privacy level. Unfortunately, such a situation usually happens when the relevant institutions abuse the user information. With this comportment, it is obvious that privacy and data protection

need more attention as long as any misuse can lead to a threat. Therefore, security experts have developed applied solutions to support the confidentiality of the information that protects sensitive information in IoT-based health-care domain. With the said issues, this paper presents an approach to the solution based on the anonymization process that provides features such as privacy and security of sensitive health dataset.

On that, the main contributions of this paper are the following:

- We develop an IoT algorithm that provides an anonymous function.
- We present a strong mathematical basis to prove the privacy and security functions that protect the data being exchanged over the internet using a wireless communication system. This method follows the homomorphism equation via the Identity-based Encryption (IBE).
- We provide an algorithm on computational complexity to evaluate the proposed anonymization algorithm whether it satisfies the complexity requirements during algorithm execution.
- Conversely, the proposed method has a couple of limitations that introduces some opportunities for further research in the IoT-based health care system:
- The anonymization algorithms work within a standalone healthcare system and third party. As many services and providers gradually adopting cloud-based operations, further research are required to overcome the limitation in our algorithm. This would require an additional function to communicate with a cloud provider with anonymization as security service.
- Taking of privacy for data anonymization into account, the user should have the ability to choose his anonymous parameters. However, our method does not offer the option that is reserved for future work.

The remainder of this paper is organized as follows: related work is briefly summarized in Section 2, while the proposed algorithm is presented in Section 3. The proposed IBE related to our algorithm is outlined in Section 4, along with the mathematical basis. The final section concludes our work.

## 2. Related Work

Since the Internet of Thing has been emerging in the health care system, personal health records have become prey for cyber-attackers or hackers. This is a dangerous situation because any data breach leads to exposure of sensitive information and patients can no longer trust the system nor the medical staff anymore. Consequently, the patients may take drastic measures such as a denial of any healthcare service, hiding information, or staying home to avoid seeking medical help [10]. In this section, we present different solutions that are applied in IoT-based health care to solve the issue of privacy and security of patient records.

Lightweight solutions (to overcome resources constrain in IoT devices) that support authentication and authorization have been proposed by Lee et al. in [11], where they develop a method to encrypt the data using logic operations for the encryption processes. Gong et al. [12] developed a scheme that includes a homomorphism system enhanced from the DES algorithm with a model system related to the lightweight scheme. In the same research way, a protocol for IoT in the electronic health is proposed by Seyed et al. [13] and outlined security features like authentication, key agreement, access control, and energy-efficient are available.

Data anonymizing with denaturing framework has been developed with the following aspects: (a) the users have possibility to define rules before the algorithm is deployed, (b) personal data masking system, (c) analytic system to allow denaturing, deletion inference anonymization and mobility data privacy function and a wide range of research has been proposed to satisfy these features [14–19].

Furthermore, interesting research by Langheinrich [20,21] has contributed to the field of privacy-preserving security. The work consists of a system in which a customer or user has some options to select instead of having negotiations with a computerized procedure in order to have an adequate agreement. The architecture provides data privacy and ensures that collected data is kept

confidential by notifying the user what kind of data has been collected. With this acknowledgment, the user has the ability to decide on the actions to be taken regarding the data. The same author [21] incorporated a function to preserve the privacy ubiquitously. The architecture is mainly composed by four elements: (a) the choice and consent provided by machine-readable privacy policies, (b) a notice mechanism based on a policy announcement, (c) access control supported by the privacy proxies, (d) resource protection provided by a policy-based on data access.

Kavenesh et al. [22] proposed a framework that models and considers the main privacy concepts suitable for the healthcare applications in IoT. The proposed compliance scale presents essential privacy principles that can be considered in the development of novel IoT health applications. The proposed compliance scale would be significant for policymakers and applications developers to measure understand and respect the privacy principles of consumers towards novel IoT-based health applications.

A Privacy Protector framework that protects collected data from the patient has been developed in the IoT network. This framework consists of sensors that collect the patient's body data, a communication service provider to prepare security scheme, a storage system to receive data from sensors and finally a system of data access control to get access to the user data. The main idea is based on secret sharing and shares paring for patients' data privacy [23]. Besides anonymization techniques, other methods to protect medical data have been presented in previous researches. A Context-Aware Access Control (CAAC) models have been developed, extending the basic Role-Based Access Control (RBAC) model where the author develop methods based on the access and privacy control policies to manage sensitive data and determine whether users' requests to limit data access permissions based on the contextual conditions as developed in the recent works [24–26]. Furthermore, Kayes et al. [27,28] have developed CAAC models including features such as sensitive and streaming data management which are applied in today's IoT-based smart spaces. In their works, they considered a wide variety of contextual conditions, for example, the situational and relationship context, utilizing the process of inferring implicit knowledge from the currently available context information.

### 3. Proposed IoT-Based Anonymization Algorithm for Security and Privacy in Health Care

#### 3.1. System Model and Overall Description

This section describes in detail the proposed anonymization algorithm that preserves security and privacy in IoT-based health care system. Two algorithms compose the whole system and the main steps are depicted in Algorithm 1. The description of some parameters are given in Table 1 and other parameters are described throughout the algorithm.

**Table 1.** Main parameters used in Algorithm 1.

Parameters	Description
HSys with P & PKG	Health care System with Public & Private Key Generator
Sick Person <Sp>, Physician <Ph>	Users <U> in the HSys
<m <sub>s</sub> , n <sub>s</sub> >	Secret Pair Key of each user
HDS	Health Data-Set
HTP	Health Third Party
∨	Or: Sp ∨ Ph

First of all, we describe the system model which includes two main parts: the Healthcare System (HSys) and HealthThird Party (HTP) as given in Figure 2. The HSys includes the data owner such as patients and physicians with their databases (DB). Furthermore, the system possesses a security engine to encrypt the data with the defined parameter. The HTP host the anonymization engine with the parameters to perform the data anonymization process. The anonymous data is available once all steps described in the algorithm are executed. In the end, the HTP can return the anonymized data to the HSys where the corresponding user can then decide when and where to share his data.

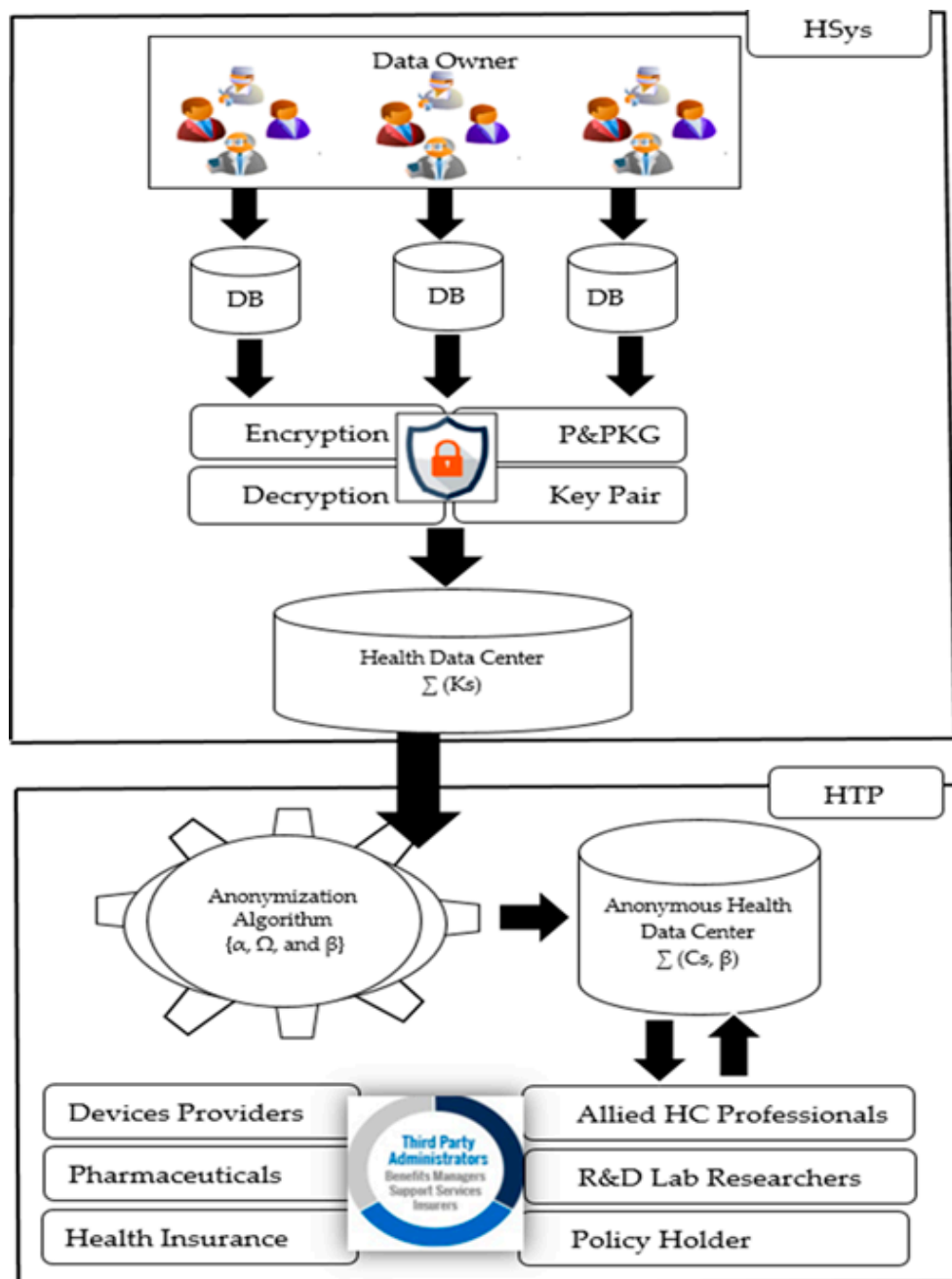


Figure 2. Overview of a patient’s body with IoT Medical Sensors.

Algorithm 1 is the overall scheme from the step in which the users interact via the HSys using their sensor or mobile devices to exchange the HDs. Let HSys be the Health care System environment (e.g., clinic, hospital, remote care . . . ) where the data owners are playing a part in. Further, let be Sick Person <Sp> and Physician <Ph> be the users in the HSys. The system requires each user participating to have a secret key pair <math>m\_s, n\_s</math>.

**Algorithm 1:** Overall Algorithm (Tripartite: <User, HSys and HTP>)**Input:** Health Data Set (HDS)**Output:**  $\beta$ -anonym parameter associated with the HDS encrypted**Pre-processing:** HSys encrypts HDS

```

1: for each U ∈ HSys
2:    $K_s \leftarrow f(\text{HDS}, m_s)$  // The encryption takes one key from the pair parameters
3:   for every  $Sp \vee Ph \in \text{HSys}$ 
4:     The HSys transmit  $K_s$  to  $Ph \vee Dr$ 
5:      $Sp \vee Ph$  sends  $K_s \leftarrow (K_s, m_{Sp \vee Ph})$  to HSys // User request to send the data
6:     each U ∈ HSys sends  $K_s$  to HTP
7:     HTP system executes Algorithm ( $K_1, \dots, K_{|\text{HSys}|}, \beta$ ) to create anonymized
8:     and encrypted datasets  $Cs_1, \dots, Cs_{|\text{HSys}|}$  //  $\beta$ -anonym parameter is generated
9:     for each U ∈ HSys,
10:      HTP forward  $Cs$  to U // The  $Cs$  is the anonymized data
11:      for each  $Sp \vee Ph \in \text{HSys}$ 
12:        HSys sends  $Cs$  to  $Sp \vee Ph$ 
13:         $Sp \vee Ph$  sends  $C_s \leftarrow (C_s, n_{Sp \vee Ph})$  to HSys // The last key from the pair
14:         $C_s \leftarrow F(\text{HDS}, n_s)$ 
15:      end for
16:    end for
17:  end for
18: end for

```

**Statement 1.** Each user  $U \in \text{HSys}$   $\xleftarrow{\text{Possesses}}$  a private key pair  $\langle m_s, n_s \rangle$  and private dataset denoted as  $\text{HDS}_s$  with  $s$  generated by HSys.

Statement 1 denotes that a user that belongs to the healthcare system has a private key pair to be used for cryptographic functions to secure his data. Within his private keys, the system generates its random private key too.

During the first operation of the session when the user wants to exchange the data, it is encrypted by the HSys' key. The anonymization comes in when the data is sent out of the HSys to the HTP or collaborating hospital or other health organizations. In this case, the algorithm generates an anonymization parameter  $\beta$  that is assigned to the encrypted data. The parameter is required for additional steps and the HTP returns a response message to the HSys that the data has been anonymized with  $\beta$ . The user with secret pair key is the only one to whom the data can be disclosed as long as he holds the secret pair keys. At this end of operations, the user system holds his encrypted ( $C_s$ ) data with a  $\beta$ -anonym parameter.

### 3.2. Process of Health Data-Set Anonymization

As long as the data is being exchanged inside of the HSys, the users are confident. However, when IoT comes in, the data handling or exchange becomes problematic with all attack types over the internet. The anonymization process is triggered when the user is in the position of sending his data to the HTP or other collaborating organizations. The negotiation is tripartite: User, HSys and HTP and final decision is made by the HTP where the  $\beta$ -anonym parameter is generated to the other entities.

**Statement 2.** Each user  $U \in \text{HSys}$   $\xrightleftharpoons[\text{Receiving a } \beta\text{-anonym parameter}]{\text{Sending HDS}}$  to HTP using HSys, the data is encrypted and anonymized.

Statement 2 indicates that a user belongs to the healthcare systems and can send his data to the third party. Before that, the user makes sure that his data is encrypted and anonymized.

The HSys, after getting the data from the user (here: <Sp> or <Ph>), the system encrypts the data and afterward, transmit the cipher to the designated HTP. The system then analyzes the request and generates an anonymized dataset. In the beginning, the user systems pre-analyze which data is designed to be anonymized so that it is not revealed to the rest of the networks. The proposed method's details are given in the pseudo-code of Algorithm 2.

### 3.3. Description of the Algorithms

As the very first step consists of a request of anonymization function, in this case, we consider the response to the HSys as health data set from the HTP. Therefore, to get back or construct the responses, heuristic and approximation methods have been utilized for data allocation.

- To boost the allocations number with a no-null response, the heuristic method is designed and can be observed in Algorithm 2. From step 5, some *d-encrypted* samples are allocated to the HSys from its submission to its response. This operation is done until each considered health system (in a distributed environment such as IoT-based healthcare [29,30]). It is not allowed that in case a sample is put on the reply, a similar action cannot be computed on the rest of the responses in the health system. Partial data (samples) is allocated to the HSys, which performs the big data of the user through the probability of the prediction. The observation of a chosen sample has probably a low value when it is randomly submitted. The steps 16 to step 18, show such case when it is not possible for a response to be allocated *d* samples, therefore the systems ensures that null samples are allocated. During this process of the operation, the algorithm guarantees that any location should provide a user data within *d* size otherwise *d-anonymity* rules are not satisfied.
- The approximation method can be seen at step 21 where it processed using a minimally sized submission allocation to the rest if the encrypted sample from the HSys submission. According to a distributed IoT-based healthcare in [29,30] where more than one health system is interacting, these samples are removed from other entities in which all system have no samples to send until no more system can be allocated samples to release. When all steps of the algorithms are completed, the HTP broadcast a message to each contributing HSys that a sample has been designed to be public or/and which one is anonymized.

### 3.4. Algorithm Complexity Computation

The evaluation of the algorithm is done by the so-called time complexity in algorithm execution procedures. "Time complexity of an algorithm quantifies the amount of time taken by an algorithm to run as a function of the length of the input." For instance, in step 1, the health datasets are reduced considering the result of the intersection tests. This process is computed in  $O(|HSys|\log HSys)$  assessments. For step 6, in every HSys the user data is assigned *d* answers but, they are no longer in the session because they are cleaned from all participating entities in the health network system. Consequently, this necessitates  $O(|HSys|)$  phases at the condition of *d* to be fairly enough the smallest value. The step 18 shows clearly that the datasets are zeroed due to the lacking of size, the complexity is  $O(|HSys|)$  of the linearity function. The complexity at step 21 is  $O(\log |HSys|)$  after considering the assignment of the data during round two in addition to data cleaning. The complexity of the algorithm, once the maximum steps are computed, is  $O(\log |HSys|)$ . This result is within the allowed standard complexity during algorithm execution.

According to [31–33], the complexity analysis of an algorithm is determined by the resources like time and storage which are required to execute the algorithm. Furthermore, most algorithms are designed to be executed based on the inputs of random length or size. Often, the complexity is defined as a function of the input or size given a number of fundamental steps (in here: time complexity) with sometimes the fundamental storage (called space complexity). To this end, notations such "O" (Big O) and theta notation ( $\Theta$ ) are usually utilized and in this paper, we have used only big-O. For example,

the logarithmic time {noted  $O(\log(n))$ } in the binary search operation running, means that there a list is a proportional number of steps being searched off to the length logarithm.

---

**Algorithm 2:** Anonymization Process ( $\alpha$ ,  $\Omega$ , and  $\beta$ -anonym parameter)
 

---

**Input:**  $\alpha = \{K_{S1}, \dots, K_{S|HSys|}\}$ , The  $U1 \dots U_{|HSys|}$  sends a set of  $K_s$  to HTP  
**Output:**  $\Omega_1, \dots, \Omega_{|HSys|}$  HTP sends back a set of anonymized data to  $U1 \dots U_{|HSys|}$ ,  $\beta$

```

1: for each  $K_{Si}, K_{Sj} \in \alpha$ 
2:   if  $|K_{Si}| - |K_{Si} \cap K_{Sj}| < l$ , then
3:      $K_{Si} \leftarrow K_{Si} \cap K_{Sj}$ 
4:   endif
5: Let  $DB \leftarrow \emptyset$  // Make sure the DataBase is initialized to zero
6: for  $b \leftarrow 1$  to  $|HSys|$ 
7:   Let  $B \leftarrow$  user data of minimum size  $|K_s| \geq d$ , so as  $T \notin DB$ 
8:    $DB \leftarrow DB \cup \{T\}$ 
9:   Let  $K_{ST}^l$  be the  $d$ -data example of  $K_{ST}$  // This appears to the end of
10:  user data from  $\alpha$ 
11:  for  $B \leftarrow 1$  to  $|HSys|$ 
12:    if  $b \neq d$ , then,  $K_{Su} \leftarrow K_{Su} - (K_{Su} \cap K_{ST}^l)$ 
13:  end for
14:  endif
15: end for
16: for  $b \leftarrow 1$  to  $|HSys|$ 
17:   if  $|K_{Si}| < d$ , then
18:      $K_{Si} \leftarrow \emptyset$ 
19:   endif
20: end for
21: for  $i \leftarrow 1$  to  $|HSys|$ 
22:    $B \leftarrow$  user data of minimum size  $|K_s| > \theta$ 
23:   if  $b \neq i$ , do
24:      $K_{Su} \leftarrow K_{Su} - (K_{Su} \cap K_{Si})$ 
25:   endif
26: end for
27: Return  $\Omega_1 \leftarrow K_{S1}, \dots, \Omega_{|HSys|} \leftarrow K_{S|HSys|}$ ,  $\beta$ 
28: end for

```

---

From this observation, we have clarified our results of the complexity analysis in the following algorithms: quicksort (step 1:  $O(n \log n)$ ), linear search (step 6:  $O(n)$ ), Linear search (step 18:  $O(n)$ ) and binary search (step 21:  $O(\log n)$ ). Figure 3 gives the overview classification of the result from our algorithm where Y-Axis represents the operations in the algorithms and X-Axis represents the elements or inputs in the algorithm.



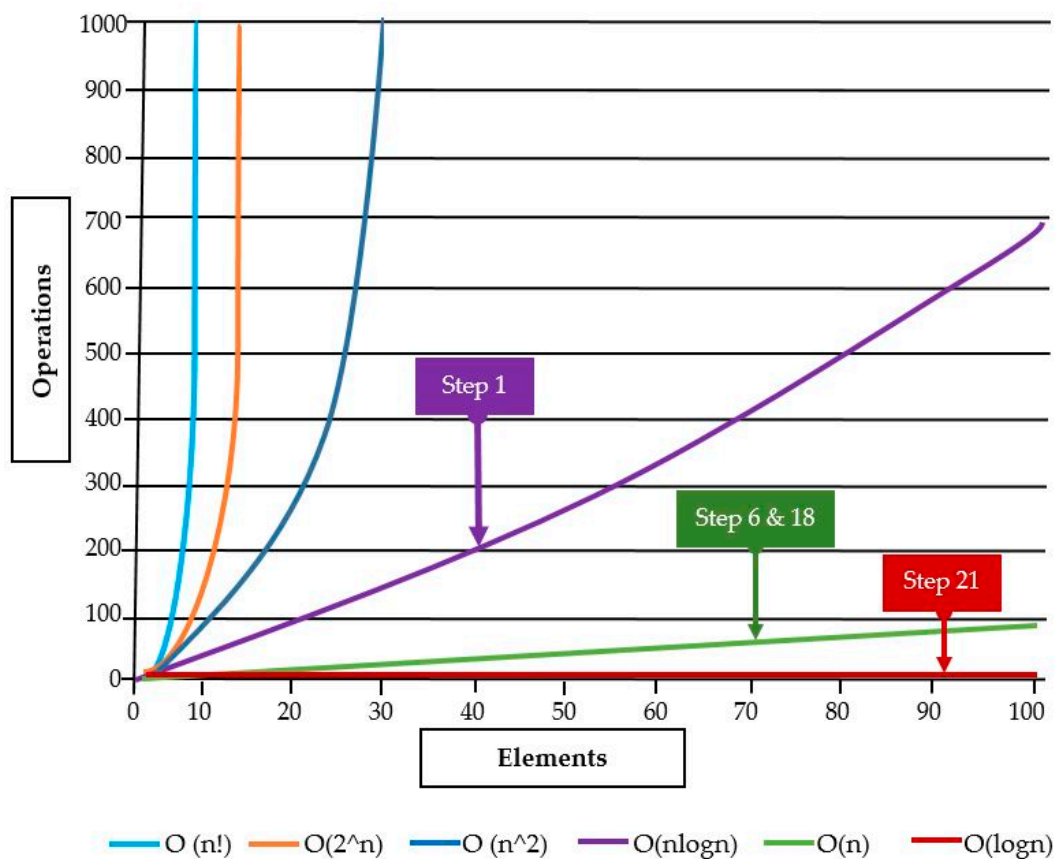


Figure 3. Big-O Complexity and result classification.

#### 4. Algorithm Evaluation Based on Mathematical Concepts

This section describes an evaluation of the proposed algorithm using a mathematical approach based on an encryption process to prove the correctness in a communication environment. The evaluation follows Shamir's idea in [34] where we incorporate the main parameters used in the IoT-based healthcare algorithm. The idea is based on the IBE algorithm as it supports anonymity functions for sensitive information passing through wireless communication.

##### 4.1. Preliminary

The notion of the algorithm based on IBE is able to give the users the ability to utilize their identity to generate the public key to encrypt the data in addition of an easy approach of public key certificates management. The infrastructure managing public key is usually used in case of the non-cryptographic model. This infrastructure is used to legitimate the public key and it is called certificate authority where it authenticates and distributes to the users their matching certificate of the public key. During IBE key exchange session, a user can utilize any string to encrypt his data but there exist other encryption methods which do not require a Public Key Encryption (PKE) infrastructure.

##### 4.2. Generation of Homomorphism Equation via IBE

Fundamentally [35], the IBE method is characteristically a tuple-algorithms denoted as  $\langle I-B-E \rangle = (\text{Set-up}, \text{Extract}, \text{Encr}, \text{Decr})$  and described as follows:

- **Set-up:** The responsible of key generation runs Setup to generate a secret parameter  $a$  where it receives an ensemble of parameters (parames) and main key. In this early stage, the parames comprise a space of message with limitations denoted  $P$  together with  $L$  as a crypto-message. To have the main key as a private element, the PKG is involved.

- Extract: This algorithm is about input parames, including the main key with  $Id$  belongs to  $[0, 1]^*$  where it receives  $f$  as a private key. During this phase, the  $id$  and public key are an arbitrary sequence with  $f$  as a private key.
- Enc: Basically, any algorithm with the encryption phase takes some parameter to encrypt and in this case, they are as follow: The input is  $\langle \text{parames}, Id, \text{ and } P_0 \in P \rangle$ , the output is a cipher-message  $\langle L_0 \in L \rangle$ .
- Dec: In the same way, the decryption is the counter-part algorithm with parameters such as the input is  $\langle \text{parames}, L_0 \in L, \text{ the private key } d \rangle$ , where the output is  $\langle P_0 \in M \rangle$ .

The  $\langle I-B-E \rangle$  is designed to be reliable which implies that any  $Id$ , during the extraction of  $f$  as private key (during the 2nd algorithm: extract), the operation is as follow:  $\text{Dec}(\text{parames}, L_0, f) = P_0$ , with  $P_0 \in P$  and  $L_0 = \text{Encry}(\text{parames}, Id, P_0)$ .

### Homomorphism Equation

The proposed anonymized algorithm in the IoT-bases healthcare needs a homomorphism equation (encryption) which is mathematically computed using the IBE. Fully homomorphic encryption can take two operations: addition and multiplication [36], in this paper, we define a homomorphic equation with two products:

- Init step: Let be  $\varepsilon$  a prime order of  $\langle \mathbb{P}_1, \mathbb{P}_2 \rangle$  the two cyclic groups, and  $\widehat{u}: \mathbb{P}_1 \times \mathbb{P}_2 \rightarrow \mathbb{P}_2$  as an acceptable bilinear map of group  $\mathbb{P}_1$  with generator  $Q$ . Now, consider  $s$  a secret factor and  $t$  to be  $\omega$ -bit prime. Assuming that  $\tau$ -bit strings represented all identities (where  $\tau$  is polynomial in  $\omega$ ). With  $B: [0, 1]^\tau \rightarrow \mathbb{P}_1$  as an algorithm for data mapping ( $B$  is the hash function). Next,  $\forall \delta \in \{0, 1, \dots, \varepsilon - 1\}$ , the computation of the public key relies on a random choice of  $\delta$  homogeneously and it gives  $PbKey = \delta Q$ . From this computation, the only parameter  $\delta$  is the secret main key but the rest of the parameters remain public.
- Secret Key Generation Step: This is the step where the  $\langle I-B-E \rangle$  scheme computes the main keys such as secret (or private) and its corresponding public key as follow: For  $\forall Id, \exists \Phi_{Id} = B(\delta_{Id}, Id)$  and  $\Theta_{Id} = B(\delta Q, Id)$  as main secret and public keys respectively. Here  $B$  is a cryptographic hash function to compute the keys.
- Cipher Process Step: The cipher message is the result of the secret key with the encryption process over the message itself from the sender. This operation is done as follow: Let  $\sigma$  be a sample data  $\in \mathbb{P}_2$  and  $Id$  the user identity,  $\Psi = \text{Enc}_{Id}(\sigma, \mu) = (\sigma \cdot \widehat{u}(\mu_{Id}, Id), \Theta_{Id})$ , where  $\mu \in \{0, 1, \dots, q - 1\}$  is a secret parameter which is arbitrary selected consistently. The cipher from this encryption process generates a result denoted  $\Psi$ .
- Decipher Process Step: To complete the  $\langle I-B-E \rangle$  full cycle algorithm, the system must provide a function to retrieve the original message from the sender. This operation is called decryption. Let  $Id$  be the user identity and  $\Psi$  the cipher such as  $\Psi = \{\Psi', \Psi''\}$ , the decryption process is a function of  $\rho$  (plaintext) and  $\Psi$  (cipher):

$$\rho_{\Psi} = \frac{\Psi'}{\widehat{u}(\Phi_{Id}, \Psi'')} \quad (1)$$

The Equation (1), leads to the homomorphism Equation (2), which is needed for the anonymization algorithm in the further steps. The homomorphism equation satisfies the following:

$$\begin{aligned} \text{Enc}_{Id} &= (\sigma' \otimes \sigma'', \mu' \oplus \mu'') \\ &= \text{Enc}_{Id}(\sigma', \mu') \text{Enc}_{Id}(\sigma'' \otimes \mu'') \end{aligned} \quad (2)$$

### 4.3. Theoretical Proof with Mathematical Analysis

The theoretical proof presents the mathematical concepts, which are applied in order to generate the anonymization function used in the IoT-based healthcare algorithm.

Therefore, we recall the main parameters involved in this process such as Users such as  $Sp$  and  $Ph$  with  $Id_{Sp}$  and  $Id_{Ph}$ , which are the ids of the users respectively in the HSys. We assume that there is no exploitation of the user's health data between the system communication and HTP as they may collaborate to expose the data.

Considering HSys, there are  $\eta$  users, the total of users that are playing part in the communication system with  $\langle N \rangle$  the total number of all corresponding  $Ids$ . Given that a single identification is assigned to every user has a unique identity  $a$  (unique identity usually is such as ID-NUMBER), we define a network  $\langle V \rangle$  with all identities and users such  $\langle a \rangle$  user has only and only one identity  $\langle 1 \rangle$  with the condition that two users in  $\langle V_{(a,b)} \rangle$  cannot have matching identity defined as follows:

$$\forall(a, b) \in \{Users\} \neg \exists V_{(a,b)} = V_{(1)} \\ V = \{Users_{(a,b,\dots,\eta)} \cup Ids_{(1,2,\dots,N)}\}$$

While submitting the data, the system performs a comparison task. Let the user  $\langle a \rangle$  in  $V$  ( $V_{(a)}$ ) compares his identity  $\langle 1 \rangle$ , in  $n$ -th data transfer rounds that correspond to the initial process, the system performs the comparison, if the condition is satisfied, the  $\langle a \rangle$  user computes and send:

$$\chi_{1,a} = Enc_{Id_{Sp}+Id_{Ph}}(\zeta_a, V_{1,a}) \quad (3)$$

This is the operation in Equation (3) where the system sends an encrypted  $\chi$  dataset where  $\zeta_a$  is a sample user health dataset taken from the HDS and  $V_{1,a}$  is a pair of user and his identity with an arbitrary selection process from the health care system configuration. The condition  $V(a) \neq 1$  is checked and if it is satisfied, the user system computes and submit the following:

$$\chi_{1,a} = Enc_{Id_{Sp}+Id_{Ph}}(1, V_{1,a}) \quad (4)$$

Equation (4) is a particular case where we specify the user identity  $\langle 1 \rangle$  which gives to the system a possibility to compute all submission rounds of his data set:

$$\chi_1 = \prod_{a=1}^N \chi_{1,a} \quad (5)$$

Equation (5) represents a computation of all datasets until the last round submission. The HSys then forward all  $\chi_1$  to the HTP. The system in the third party will compute the following expression and send back it the HSys for further steps:

$$\hat{\zeta}_1 = \chi_{T_{Id_{Sp}}}(\chi_1) \quad (6)$$

Equation (6) shows us that the system can identify the ID of the user who is, in this case, the patient and for now, the anonymization process is getting started. Moreover, it is remarkable that  $\{T\}$  value includes the expression to specify that this is not a replicated data as described in Algorithm 2.

Suppose that:  $\chi_1 = \{\chi'_1, \chi''_1\}$  in this assumption, the health care system in the IoT configuration will compute the following:

$$\tilde{\zeta} = \chi_{T_{Id_{Sp}}}(\hat{\zeta}, \chi''_1) \quad (7)$$

The result in Equation (7) shows that partial data  $\tilde{\zeta}$  is encrypted with the owner data  $Id$ ; in this case, it is  $\langle Sp \rangle$ . This expression leads us on the following theorem where all involved users with their data are assigned a random number.

**Theorem 1.** *The correctness of the anonymization function in the algorithm is true; that is, assuming that all involved parties follow the rule, then  $(\tilde{\zeta}_1, \tilde{\zeta}_2, \dots, \tilde{\zeta}_n)$  is a permutation of  $(\zeta_1, \zeta_2, \dots, \zeta_n)$*

**Proof.** The demonstration of the provability clarify it as follows:

$$\tilde{\zeta}_1 = \zeta_{T_{Id_{Sp}}}(\hat{\zeta}, \chi_1'') = \frac{\hat{\zeta}_1}{\hat{u}(\Phi_{Id_{Sp}}, \chi_1'')} = \frac{\chi_{T_{Id_{Dr}}}(\chi_1)}{\hat{u}(T_{ID_{Sp}}, \chi_1'')} = \frac{\chi_1}{\hat{u}(T_{Id_{Sp}}, \chi_1'')\hat{u}(T_{Id_{Ph}}, \chi_1'')} \quad (8)$$

In Equation (8), the system takes into consideration of all involved users (Sp and Ph) as we stated that the anonymization rule must be applied on each entity-playing role in the IoT system.

The last computation is based on the condition that user <a> and its id <1> satisfies the condition such as  $Va = 1$  for  $a(1)$  as its value, this will transform the Equation (8) into the following global Equation (9) and final result:

$$\begin{aligned} \hat{\zeta}_1 &= \frac{\chi_1}{\hat{u}(T_{Id_{Sp}}, \chi_1'')\hat{u}(T_{Id_{Ph}}, \chi_1'')} = \frac{\prod_{a=1}^N \chi_{a,1}}{\hat{u}(T_{Id_{Sp}}, \chi_1'')\hat{u}(T_{Id_{Ph}}, \chi_1'')} \\ &= \frac{Enc_{Id_{Sp}+Id_{Ph}}(\zeta_{a(1)}, V_{1,a}) \prod_{a \neq a(1)} Enc_{Id_{Sp}+Id_{Ph}}(1, V_{1,a})}{\hat{u}(T_{Id_{Sp}}, \chi_1'')\hat{u}(T_{Id_{Ph}}, \chi_1'')} = \zeta_{a(1)} \end{aligned} \quad (9)$$

With the permutation, operations of  $a(1)$  we deduct that the permutation function is applied on  $(1, 2 \dots N)$ , the result is then a permutation of the following expression:  $(\zeta_1, \zeta_2, \dots, \zeta_n)$ , which proves Theorem 1 of anonymization algorithm.

## 5. Conclusions

With the growth of the IoT-based healthcare system, extensive studies offering applicable solutions in the field have been developed and others are still going on. Considering such an environment, an immense volume of data is transmitted over the public network among the patients, physicians, nurses, and relevant health organizations. Therefore, it is highly important to assure the safety of the data owner to avoid an unwanted situation. This paper proposed the development of a theoretical approach that ensures the security and privacy of sensitive data for the considered IoT environment.

The proposed algorithm provided required security features such as privacy or confidentially for the user's data that is transmitted within the health care network. When the user sends his information to be used by the third party via a given health network, the encryption process is firstly executed using a key from the key pair and the system request a response to the third party in which the anonymization function generates a value to anonymize the encrypted data set.

In the work, we showed that our proposed scheme guarantees the anonymity function where the algorithm computes the conditions and then executes the anonymization procedure on the healthcare data. In addition, we demonstrated that the algorithm satisfies the computational complexity requirements of the execution of all steps. Lastly, a proof based on a mathematical analysis has been developed to demonstrate that the proposed algorithm ensures the veracity and can be a real application to secure the IoT technologies for the health care network using wireless communications. For future work, we intend to implement the proposed approach in a practical environment (using healthcare sensors). The experiment results can, therefore, be used for evaluation and comparison with other existing methods.

**Author Contributions:** Conceptualization, Writing the Original Draft, Project Administration, and Funding Acquisition, X.C.Y.; Methodology, Writing-Review & Editing, B.N.; Formal Analysis and Validation, Z.G.L.; Investigation and Data Curation, L.N.; Visualization, Resources, and Supervision, S.M.R.I.

**Funding:** This research was supported by the Scientific Fund Project of Facility Horticulture Laboratory of Universities in Shandong of China (Grant number: 2018YY016) and the Doctoral Scientific Fund Project of Weifang University of Science & Technology of China (Grant number: 2017BS17), it was also supported by the Innovation Fund of Ministry of Education, Science and Technology Development Center of China (Grant number: 2018A02013).

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

## References

1. Yao, L.; Sheng, Q.Z.; Benatallah, B.; Dustdar, S.; Wang, X.; Shemshadi, A.; Kanhere, S.S. WITS: An IoT-endowed computational framework for activity recognition in personalized smart homes. *Computing* **2018**, *100*, 369–385. [[CrossRef](#)]
2. Höller, J.; Tsiatsis, V.; Mulligan, C.; Karnouskos, S.; Avesand, S.; Boyle, D. *From Machine-to-Machine to the Internet of Things: Introduction to a New Age of Intelligence*; Elsevier: Amsterdam, The Netherlands, 2014.
3. Wang, G.; Gunasekaran, A.; Ngai, E.W.; Papadopoulos, T. Big data analytics in logistics and supply chain management: Certain investigations for research and applications. *Int. J. Prod. Econ.* **2016**, *176*, 98–110. [[CrossRef](#)]
4. Shahzad, A.A.; Kim, Y.G.; Elgamoundi, A. Security IoT Platform for Industrial Systems. In Proceedings of the 2017 International Conference on Platform Technology and Service (PlatCon), San Francisco, CA, USA, 8–12 June 2015. [[CrossRef](#)]
5. Ji, Z.; Ganchev, I.; O'Droma, M.; Zhao, L.; Zhang, X. A Cloud-Based Car Parking Middleware for IoT-Based Smart Cities: Design and Implementation. *Sensors* **2014**, *14*, 22372–22393. [[CrossRef](#)] [[PubMed](#)]
6. Bhatti, F.; Shah, M.A.; Maple, C.; Islam, S.U. A Novel Internet of Things-Enabled Accident Detection and Reporting System for Smart City Environments. *Sensors* **2019**, *19*, 2071. [[CrossRef](#)] [[PubMed](#)]
7. Arafat, A.D.; Muresan, R.; Mayhew, M.; Lieberman, M. IoT-Based Multifunctional Scalable Real-Time Enhanced Road Side Unit for Intelligent Transportation Systems. In Proceedings of the 2017 IEEE 30th Canadian Conference on Electrical and Computer Engineering (CCECE), Windsor, ON, Canada, 30 April–3 May 2017. [[CrossRef](#)]
8. Dziak, D.; Jachimczyk, B.; Kulesza, W.J. IoT-Based Information System for Healthcare Application: Design Methodology Approach. *Appl. Sci.* **2017**, *7*, 596. [[CrossRef](#)]
9. Dwivedi, A.D.; Srivastava, G.; Dhar, S.; Singh, R. A Decentralized Privacy-Preserving Healthcare Blockchain for IoT. *Sensors* **2019**, *19*, 326. [[CrossRef](#)] [[PubMed](#)]
10. Li, M.; Yu, S.; Zheng, Y.; Ren, K.; Lou, K. Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption. *IEEE Trans. Parallel Distrib. Syst.* **2013**, *24*, 131–143. [[CrossRef](#)]
11. Lee, J.Y.; Lin, W.C.; Huang, Y.H. A lightweight authentication protocol for Internet of Things. In Proceedings of the 3rd International Symposium on Next-Generation Electronics (ISNE 2014), Kwei-Shan, Taiwan, 7–10 May 2014.
12. Gong, T.; Huang, H.; Li, P.; Zhang, K.; Jiang, H. A Medical Healthcare System for Privacy Protection Based on IoT. In Proceedings of the 7th International Symposium on Parallel Architectures, Algorithms, and Programming (PAAP), Nanjing, China, 12–14 December 2015; pp. 217–222.
13. Seyed, F.A.; Mala, H.; Shojafar, M.; Peris-Lopez, P. LACO: Lightweight Three-Factor Authentication, Access Control and Ownership Transfer Scheme for E-Health Systems in IoT. *Future Gener. Comput. Syst.* **2019**, *96*, 410–424. [[CrossRef](#)]
14. Sliwa, J. A generalized framework for multi-party data exchange for IoT systems. In Proceedings of the 30th IEEE International Conference on Advanced Information Networking and Applications Workshops, (WAINA), Crans-Montana, Switzerland, 23–25 March 2016; pp. 193–198.
15. Berrehili, F.Z.; Belmekki, A. Privacy Preservation in the Internet of Things. In *Advances in Ubiquitous Networking 2*; Lecture Notes in Electrical Engineering; Springer: Singapore, 2017; Volume 397, pp. 163–175.
16. Shinzaki, T.; Morikawa, I.; Yamaoka, Y.; Sakemi, Y. IoT security for utilization of big data: Mutual authentication technology and anonymization technology for positional data. *Fujitsu Sci. Tech. J.* **2016**, *52*, 52–60.
17. Otgonbayar, A.; Pervez, Z.; Dahal, K. Toward Anonymizing IoT Data Streams via Partitioning. In Proceedings of the 13th IEEE International Conference on Mobile Ad Hoc and Sensor Systems (MASS 2016), Brasilia, Brazil, 10–13 October 2016; pp. 331–336.
18. Wang, J.; Amos, B.; Das, A.; Pillai, P.; Sadeh, N.; Satyanarayanan, M. A scalable and privacy-aware IoT service for live video analytics. In Proceedings of the 8th ACM Multimedia Systems Conference (MMSys 2017), Taipei, Taiwan, 20–23 June 2017; pp. 38–49.

19. Addo, I.D.; Madiraju, P.; Ahamed, S.I.; Chu, W.C. Privacy Preservation in Affect-Driven Personalization. In Proceedings of the 2016 IEEE 40th Annual Computer Software and Applications Conference (COMPSAC 2016), Atlanta, GA, USA, 10–14 June 2016; pp. 400–405.
20. Langheinrich, M. A Privacy Awareness System for Ubiquitous Computing Environments. In *UbiComp 2002: Ubiquitous Computing*; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2002; Volume 2498, pp. 237–245.
21. Langheinrich, M. Privacy by design—principles of privacy-aware ubiquitous systems. In *UbiComp 2001: Ubiquitous Computing*; Lecture Notes in Computer Science; Springer: Berlin, Germany, 2001; Volume 2201, pp. 273–291.
22. Kavenesh, T.; Jasapaljeet, S.D.; Saraswathy, S.G.; Lim, F.C. Developing a Privacy Compliance Scale for IoT Health Applications. *Comput. Sci. Inf. Technol.* **2018**, *6*, 54–62. [[CrossRef](#)]
23. Luo, E.; Bhuiyan, M.Z.A.; Wang, G.; Rahman, M.A.; Wu, J.; Atiquzzaman, M. PrivacyProtector: Privacy-Protected Patient Data Collection in IoT-Based Healthcare Systems. *IEEE Commun. Mag.* **2018**, *56*, 163–168. [[CrossRef](#)]
24. Trnka, M.; Cerny, T. On security level usage in context-aware role-based access control. In Proceedings of the 31st Annual ACM Symposium on Applied Computing, Pisa, Italy, 4–8 April 2016; pp. 1192–1195. [[CrossRef](#)]
25. Colombo, P.; Ferrari, E. Enhancing NoSQL datastores with fine-grained context-aware access control: A preliminary study on MongoDB. *Int. J. Cloud Comput.* **2017**, *6*, 292–305. [[CrossRef](#)]
26. Hosseinzadeh, S.; Virtanen, S.; Rodríguez, N.D.; Lilius, J. A semantic security framework and context-aware role-based access control ontology for smart spaces. In Proceedings of the International Workshop on Semantic Big Data, San Francisco, CA, USA, 26 June–1 July 2016. [[CrossRef](#)]
27. Kayes, A.S.M.; Jun, H.; Wenny, R.; Tharam, D.; Md, S.I.; Alan, C. A Policy Model and Framework for Context-Aware Access Control to Information resources. *Comput. J.* **2019**, *62*, 670–705. [[CrossRef](#)]
28. Kayes, A.S.M.; Wenny, R.; Tharam, D.; Elizabeth, C.; Jun, H. Context-Aware Access Control with Imprecise Context Characterization for Cloud-Based Data Resources. *Future Gener. Comput. Syst.* **2019**, *93*, 237–255. [[CrossRef](#)]
29. Prosanta, G.; Ruhul, A.; Islamc, S.K.H.; Neeraj, K.; Vinod, K.B. Lightweight, and privacy-preserving RFID authentication scheme for distributed IoT infrastructure with secure localization services for smart city environment. *Future Gener. Comput. Syst.* **2018**, *83*, 629–637. [[CrossRef](#)]
30. Atlam, H.F.; Walters, R.J.; Wills, G.B. Fog Computing and the Internet of Things: A Review. *Big Data Cogn. Comput.* **2018**, *2*, 10. [[CrossRef](#)]
31. Algorithm Analysis. Available online: [https://everythingcomputerscience.com/algorithms/Algorithm\\_Analysis.html](https://everythingcomputerscience.com/algorithms/Algorithm_Analysis.html) (accessed on 3 July 2019).
32. Ian, P. *Lecture Notes on Algorithm Analysis and Computational Complexity*, 4th ed.; Department of Computer Sciences University of North Texas: Denton, TX, USA, 2001.
33. Big-O Cheat Sheet. Available online: <http://www.bigocheatsheet.com/> (accessed on 3 July 2019).
34. Shamir, A. Identity-Based Cryptosystems and Signature Schemes. In *Cryptology*; Springer: Berlin/Heidelberg, Germany, 1985.
35. Philippe, G.; Adrien, H.; Duong, H.P.; Tillich, J.P. Identity-based Encryption from Codes with RankMetric. In *Cryptology—CRYPTO 2017*; Lecture Notes in Computer Science; Katz, J., Shacham, H., Eds.; Springer: Berlin/Heidelberg, Germany, 2017; Volume 10403. [[CrossRef](#)]
36. Francisco, J.V.P. Contributions to Design and Analysis of Fully Homomorphic Encryption Schemes. Ph.D. Thesis, Université Paris-Saclay préparée à l' Université de Versailles, Versailles, France, July 2018.

