informatics

Article

An Internet of Things Based Multi-Level Privacy-Preserving Access Control for Smart Living

Usama Salama *, Lina Yao and Hye-young Paik

School of Computer Science and Engineering, University of New South Wales, Sydney, NSW 2052, Australia; lina.yao@unsw.edu.au (L.Y.); h.paik@unsw.edu.au (H.-y.P.)

* Correspondence: u.salama@unsw.edu.au

Received: 25 January 2018; Accepted: 23 April 2018; Published: 3 May 2018

Abstract: The presence of the Internet of Things (IoT) in healthcare through the use of mobile medical applications and wearable devices allows patients to capture their healthcare data and enables healthcare professionals to be up-to-date with a patient's status. Ambient Assisted Living (AAL), which is considered as one of the major applications of IoT, is a home environment augmented with embedded ambient sensors to help improve an individual's quality of life. This domain faces major challenges in providing safety and security when accessing sensitive health data. This paper presents an access control framework for AAL which considers multi-level access and privacy preservation. We focus on two major points: (1) how to use the data collected from ambient sensors and biometric sensors to perform the high-level task of activity recognition; and (2) how to secure the collected private healthcare data via effective access control. We achieve multi-level access control by extending Public Key Infrastructure (PKI) for secure authentication and utilizing Attribute-Based Access Control (ABAC) for authorization. The proposed access control system regulates access to healthcare data by defining policy attributes over healthcare professional groups and data classes classifications. We provide guidelines to classify the data classes and healthcare professional groups and describe security policies to control access to the data classes.

Keywords: access control; ambient assisted living; authentication; Internet of Things; IoT

1. Introduction

Ambient Assisted Living (AAL) is the system that integrates healthcare devices implemented by wireless technologies, such as Radio Frequency Identification (RFID) and sensor [1], to monitor the patient's health status in healthcare applications. The emerging paradigm of Internet of Things (IoT) with AAL has been to put personal smart health systems into place. Such systems integrate ambient intelligence into our lives to create a smart environment by responding to people's locations and behaviours astutely. The most promising applications for AAL are aged care, patient care and independent living for the elderly.

Typical health monitoring applications for AAL and smart homes generate electronic health data, forming a rich database for further analytics. The sensor-collected data could be stored as part of the personal health data of patients to improve the service provided by healthcare organizations and to provide health updates to the patient's family members and friends. To demonstrate the benefits of collecting and storing health monitoring data and daily activity records of elderly patients, let us consider the following scenario which is illustrated in Figure 1.

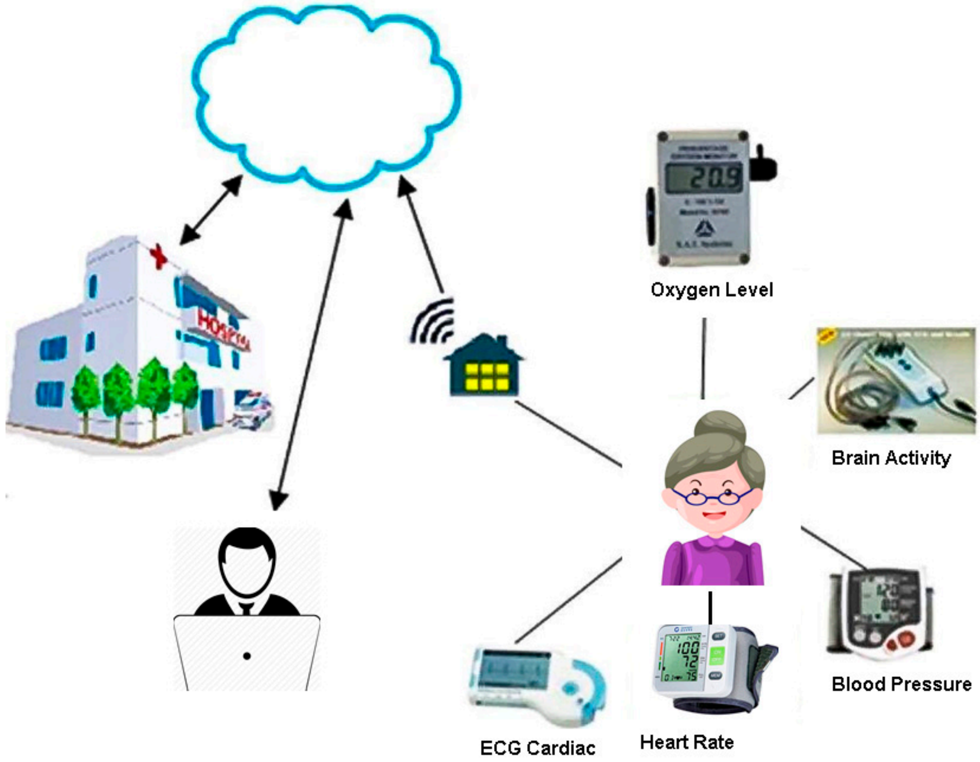

Figure 1. Motivation Scenario of Assisted Living in Internet of Things (IoT).

Mrs. Murphy had a heart attack last month and she is now at home. Her son Bob, who is working full time and lives in another city, wants to monitor/know his mother's health status and be aware of any developments that may occur. He also wants his mother's health records to be available to hospital doctors and staff members who are following his mother's case, so that he can be updated with expert analysis and feedback from medical practitioners. On the other hand, Bob also wants the hospital to have access to his mother's real-time health data, which will ensure that Mrs. Murphy receives the most efficient assistance from the medical staff in case of any health issues or developments. Bob has equipped his mother's house with wearable passive RFID tags and sensors to monitor her activities and movements. Biometric sensors are also in place to monitor cardiac activities, glucose levels, temperature, CO_2 levels, brain activity, blood pressure, GSR stress levels and oxygen blood levels. All the data will be collected and analysed in a real-time manner. The data will also be stored online with other healthcare data and will be available for authenticated and authorized users.

If an emergency situation arises, such as falling or another heart attack, the hospital will be alerted and so will her son Bob. Paramedics who rush to assist will have access to the necessary online healthcare data to save Mrs. Murphy's life, hospital staff will also have all the required health and medical information related to Mrs. Murphy and in a short time she will be getting the best possible treatment. Also, Mrs. Murphy's family doctor can use his access to the online healthcare data to follow up on the situation and update Bob when needed.

Bob usually accesses a secure website a few times a day to scan a check list and find out if his mother has eaten normally, taken her medication on time and if she was able to manage her daily activities. Due to the fact that Mrs. Murphy lives alone, Bob has also installed a smart lock so that he will be able to open the door to ambulance officers using the smart home application on his mobile.

Although utilizing aggregated healthcare data could help provide the best treatment, detect early signs of illness and discover new treatments, most of the current AAL platforms and solutions for personal health monitoring and telemedicine are difficult to use due to constant challenges in interoperability, usability, dependability, security and privacy [2]. Security is one of the main urgent needs in AAL, as the life of the patient will be at risk and the right to privacy will be violated if important and sensitive health data are accessible to irrelevant parties without the patient's consent.

To protect privacy, any access request to data should be justified by providing a clear purpose that necessitates a disclosure of the data. Access control is one of the promising solutions for protecting the sensitivity of health data from being compromised and leaked. Access control is about enforcing access rules to ensure that authorized users can access the resources they need to make the best decisions.

As the main contribution, in this paper we propose a novel Internet of Things endowed multi-level access control framework to regulate access to sensitive personal health data in order to protect privacy in AAL systems. This framework consists of two main components: the policy model that defines access control policies and the architecture model which defines the implementation of the policies to enforce access on data.

In this paper, we presented an IoT based system that provides a care management process to help older people live independently. The system monitors the daily activities of an elderly person and reports any abnormality in their daily routine, as well as, collects and reports any abnormality in their healthcare data which may indicate early signs of health issues. The proposed access control mechanism that was introduced is an attribute-based model which adheres to the dynamic nature of the healthcare organisation and has the flexibility to adapt to new access requirements.

Our proposed access control system makes contribution to the adaptable management of data access in AAL systems by addressing the need to have an adequate level of flexibility to regulate access to digital healthcare data stored in the cloud, while considering the dynamic nature of the users who may request access. The required flexibility is demonstrated in the policy model of the proposed system by implementing combinations of more than one rule to grant access in different situations. The system grants proper access levels based on the attributes of people (subject), data (object) and environments.

2. Related Work

Since personal health records are often a target for malicious attacks that lead to exposure of this sensitive information, some problems may arise if patients cannot trust that their personal heath record will be secured and only used for the indented purpose. Patients may intentionally hide information or not seek medical help to avoid embarrassment, loss of employment or denial of insurance [3]. A typical privacy protection framework for RFID services addresses the privacy issue during the collection stage by allowing patients to control the access to their personal health information transmitted from RFID tags [4]. The proposed system is based on the following:

1. A privacy protection system that ensures authorization, confidentially and integrity of the information.
2. An access control mechanism to manage the collected information, personal information and logs by user groups.
3. A provisioning system to secure communication paths, provide auditing capabilities and apply and negotiate privacy policy rules to prevent the collection of personal data without proper authorization.

There are many other solutions focusing on addressing privacy and access control of Electronic Health Records (EHR) using cryptographic and non-cryptographic approaches to preservice information privacy in the cloud [5,6]. The cryptographic techniques encrypt data in the cloud using digital signatures to authenticate users. It also enables patients to provide decryption keys to other users [7].

The security of personally controlled electronic health records (PCEHR) system was proposed by the Australian government to make the health system more agile. The system proposed a cloud-based framework that employs encryption techniques to control access to the cloud database. It also gives the patient control over their heath records by giving them the decryption key of their encrypted health data [8]. The new model still needs to address emergency access to patients' health records when a patient is not able to provide the decryption key and how the data could be accessed by different types of users such as physicians, insurers and researchers while protecting the patient's privacy.

Another system secures data on a semi-trusted cloud environment by distributing data across multiple clouds while using attribute-based encryption to protect the privacy of health data [9]. The proposed solution needs huge processing power and memory resources to minimize the processing time. Also, the use of Role Based Access Control model for authorization is not ideal for health data as users having a similar function will have the same access level and there is also a possibility for a user to have multiple roles. The use of a cloud-based healthcare system has been addressed in many papers. The security of health care data using cloud computing was mainly based on secure data collection, secure storage and the implementation of a strong access control system [10]. A security reference model consists of three core components:

1. Secure collection and integration of electronic health records produced by Care Delivery Organizations (CDOs) and a guarantee that EHR in different formats can be easily integrated.
2. Secure storage and access management by implementing data encryption and access control models based on role-based or attribute-based access control policies.
3. A secure usage model based on signature and verification.

In addition to these core components, authors also suggested using security protocols (e.g., SSL, TLS, IPSec) to encrypt communication between parties. Most of the previous approaches and studies in the cloud solution system for healthcare focus on storing the data securely and allow access to the patient's sensitive health data on demand. But for the healthcare system, there are different user groups, such as friends, caregivers, researchers and health practitioners. These user groups need to access the healthcare data based on their roles in order to perform their respective duties.

3. Framework Overview

In this section, we first overview the structure of the framework, followed by a description of the key components of our proposed solutions. The system is built on a network of sensors deployed in-house; smart devices, sensors fixed in walls and furniture and wearable devices which are all part of an intelligent home monitoring system that runs over the Internet of Things framework.

As illustrated in Figure 2, the system is a layered architecture for collecting, managing and sharing healthcare data produced by sensors, smart devices and healthcare professionals. The bottom layer, Data Collection, manages sensors associated with smart and wearable devices, collects healthcare data and sensor signals and processes data streams. As data collection is out of the scope of this paper, interested readers can refer to our previous work for more details [11,12].

The middle layer, Analytics and Data Management, generates and analyses contextual events such as localization and activity reorganization. This layer also processes and aggregates activities and objects used from smart devices' data feed and collects healthcare data from RFID health monitoring devices. The Contextual and Healthcare Data Processing unit has two main jobs; collecting all data and storing it with the patient's healthcare data in a secure cloud store and sending the data to the Triggering Engine which will create alerts, based on predefined rules if any of the collected information indicates health risks.

The top layer, Security & Access Control, presents our complete solution for the multilevel access control system that starts when the healthcare professional requests access to the patient's data from the user interface system. The user interface system sends the data request to the authentication server, authorization server, then to the cloud storage. This layer is the main point of this paper and we discuss our proposed solution in more details in Section 6.

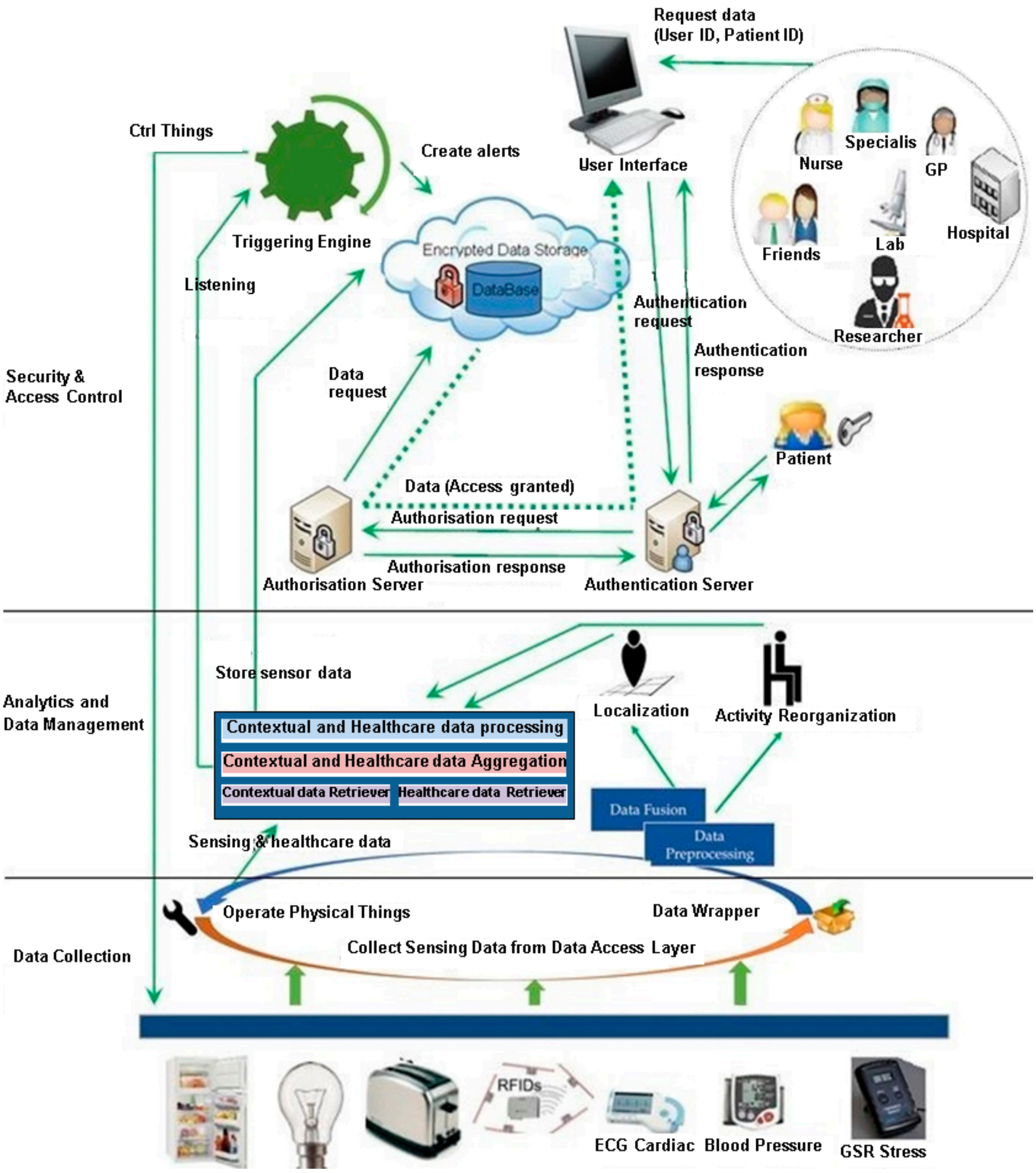

Figure 2. Framework of Proposed Architecture.

4. Data Collection Layer

The use of remote monitoring technology to monitor vital signs provides early indications of patients' health problems, thus allowing for more proactive and targeted care. It demands developing an IoT solution to electronically record vital signs, calculate warning scores and automatically escalate to raise an alarm with family members and physicians. The system can also use advanced analytics and combine collected data with the latest medical information to alert people to any early signs of risk such as acute organ failure, stroke or heart attack, based on the data collected and from previous situations.

Most of the related work uses analytics techniques applied to medical data to provide insights by representing the relationship between different health factors. We will briefly demonstrate in Section 5 how some movement disorder diseases could be detected by using the data collected by health sensors in an ambient assisted home. Data sources available to the system include;

1. Remote monitoring healthcare data collected by sensors.

2. Electronic healthcare data records, which includes patients' current health status, medical history and conditions collected from healthcare practitioners and organizations.
3. Background information such as authenticity, dietary and lifestyle habits collected from the patient or patient's family.
4. Medical information related to diseases such as early and alarming signs.

Although this is outside the scope of this paper, the use of different analytics techniques to utilize the collected data should be considered for further and more focused research. Our proposed multilevel access control system supports researchers as a group of users who could have access to the healthcare data. The use of an analytics technique such as predictive analytics using statistical modelling could be the best technique to implement a proactive and more targeted care solution to complex health issues. The new healthcare analytics system could use all available medical and clinical datasets as well as up-to-date research results to raise the alarm on patients who are deteriorating, allowing early intervention or giving a new lead to contain outbreaks and find best treatments.

On the other hand, using this huge volume of collected healthcare data and the patient's medical history data could be a time-consuming task for physicians. Using visual analysis to provide physicians with a graph or tabular view of some of these unstructured data sets will save time and save lives.

5. Activity and Data Management Layer

In this section, we briefly introduce how the semantic location and activities of daily lives are automatically extracted based on the data feeds from the ambient sensors. We develop a holistic view of smart home management, consolidating the resource and service management all in one place. In particular, we present a layered monitoring architecture based on IoT and cloud, which provides the infrastructure to transparently access sensors, processors and actuators using standardized protocols. The coordination module can automatically wrap up the real-time contextual events (e.g., activities and locations) and expose them as services in the form of RESTful APIs and further represent the APIs.

Recently, ambient intelligence in the smart home environment was able to respond to people's locations and behaviours using sensors and Radio Frequency Identification (RFID). This development introduces many applications in aged care, patient care and surveillance. The main prerequisite for these applications is the ability to locate and track people inside their homes.

Most of the RFID techniques that used to locate people require wearing a tag, which is not very convenient for many. A tag-free RFID localization application could be the optimum solution.

It is well known that received signal strength indicator (RSSI) is effected by ambient noise interference, physical antenna orientation and fluctuation of the power source. This leads to RSSI to be highly uncertain in a complex environment.

The approach presented in [11] for using a passive RFID tag array for posture recognition is based on two general intuitions; RSSI will change when a subject appears in the test area, and, if the subject appears at different locations, the tag's RSSI will show various fluctuation patterns.

The approach senses the environment using a passive tag array and uses machine learning to estimate the location. By using a training data set that contains the RSSI of these passive tags at specific locations along with their correct location label, the approach will estimate the subject's location for a given new RSSI.

The approach addresses localization as a classification problem and uses passive tag array to capture the RSSI changes which then feed to a series of probabilistic approaches. Multivariate Gaussian Mixture Model (GMM) and the expectation Maximization (EM) are used to model the RSSI grid distribution (locations) which was used to locate a single object based on the maximum posterior estimation.

To be able to confirm the subject's location l we need to find the maximum posterior distribution given the $Pr\ \left(l_j, o_i\right)$ sequence of observed sensory value o_i.

$$\dot{j} = \underset{j}{\operatorname{argmax}} Pr(l_j, o_i)$$

By using the Expectation-Maximization (EM) algorithm and training the model on the training set, the location of the subject is determined by the maximal probability of the subject being located at the location l.

To be able to recognize activities, we have developed a Hidden Markov Model (HMM) based model to determine the conditional probability of the captured new sensory streams and determine the activity (e.g., falling on the ground or sitting from standing) [12], giving sensor data observation vector $O = \{o_1, ..., o_T\}$ and a sequence of different postures $L = \{l_1, ..., l_T\}$, drawn from a predefined finite posture set. The joint probability sequence L and RSSI (Received Signal Strength Indication) sequence O is given by:

$$Pr(L, O) = Pr(o_{1:T}, l_{1:T})$$
$$= \prod_{t=1}^{T} Pr({}^{l_t}/_{l_{t-1}}) Pr({}^{o_t}/_{l_t})$$

Using the proposed solution for activity and posture recognition can help in detecting early signs of movement disorder related diseases. Movement disorders are usually detected by excess movements, by the lack of movements, or by rigidity and contraction of muscles.

An article by Dr. Mandal, in News Medical Net [13] stated that movement disorders may lead to severe disability and difficulty in having a normal life, which in turn causes a huge impact on society, as patients will not be able to keep gainful employment and may need constant supervision and care. Capturing the early signs of movement disorder offers an opportunity for early diagnosis and early treatment. There are different types of movement disorders; in this section we focus on the symptoms and signs that could be detected by our approach as discussed earlier.

- Rigidity, which is a resistance to movement. Most affected patients have their neck or leg muscles tense and contracted. When the patient attempts to move s/he may have short and jerky movements called "cog-wheeling".
- Akinesia which is slowness of movement, which is considered as one of the classic symptoms of Parkinson's disease. Patients also may develop a stooped posture, shuffling walk and becomes erratic and unsteady and this may lead to falls.
- Tremors, which are one of the most common symptoms. They appear in the head, face, or limbs. Tremors may occur during attempting tasks or even at rest.
- Postural instability which gives patients a stooped posture with bowed head and drooped shoulders. It also affects balance and coordination, which leads to repeated falls with serious injuries as a result.
- Dyskinesia, which is a series of abnormal movements which manifest as rhythmic or pendulous movements of the arms and legs. It also could be in the form of rapid jerky and purposeless movements of the limbs that appear suddenly.
- Restless leg syndrome, which is the feeling of bugs over the legs or arms at bedtime or at rest. The feeling is relieved temporarily by movement of the limbs.

The collected data used to recognize human activity can be applied to create a single dictionary for each activity for each person. Assuming we have N predefined types of activities that are stored with other health-related data in the healthcare database for each patient, a new signal strength vector will be matched to an existing movement type. By using data classification and defining a minimum confidence or error margin when matching the new vector against the predefined activities, we would be able to indicate the abnormality of movements and detect any new involuntary movements. The physician could be alerted for early treatment when the patient starts developing any of the movement disorder related diseases.

6. Access Control Layer

As mentioned earlier, the aggregation of medical, health and personal records has introduced new security risks for the patient's privacy by creating a single access point for all patients' personal health data.

Before discussing security issues for healthcare data, it is important to reference some of the reasons for choosing cloud storage as a solution to accommodate this type of data. The integration of the data feed from healthcare sensors and the patient medical records requires a flexible storage that is scalable enough to facilitate access for a large number of users and data volumes that continuously increase.

Cloud computing offers the optimum solution that meets the healthcare system's requirements for both on-demand storage and processing services. It offers the healthcare domain an affordable easy-to-manage infrastructure that is available anytime and anywhere, that is also highly scalable in order to facilitate the large number of stakeholders and millions of records. But, on the other hand, the issue of outsourcing this sensitive health information to the cloud providers leads to some serious privacy concerns.

There are different types of clouds that could be used for the healthcare system. The private cloud is the cloud infrastructure for a private organization that is owned and managed by this organization. In a healthcare scenario, the cloud infrastructure is typically managed by the healthcare organization or a designated third-party and may exist on premise or off premise. The healthcare data stored on the private cloud is considered to be more secure compared to other clouds. On the other hand, a hybrid infrastructure is more common in the healthcare system. Hybrid cloud infrastructure combines private and public clouds to support the healthcare organization with limited physical resources to store health data. But, on the other hand, a hybrid infrastructure requires more security measures to preserve privacy requirements [14].

The aggregation of medical, health and personal records has introduced new security risks for patient privacy by creating a single access point for all patients' personal health data.

Generally, a patient's health records may contain sensitive information in relation to sexual health, addictions, mental health, etc. All such digital information will last indefinitely and once released onto a cloud and accessed by remote users, can never recover its purely private status, which makes privacy of health data a big concern. Also, such a system must be available online when needed and must be only accessible by authorized personnel. Therefore, it is essential to have new access control policies and mechanisms that are suited for such systems.

Privacy risks can arise from health professionals who can unintentionally cause disclosure of health data. Also, this information could be leaked for revenge, profit, or other ill purposes by system operators or healthcare workers. Risks from the inadvertent or intentional release of information concerning infections, mental health, chronic disease diagnoses and genetic information are all well recognized both online and in the mass media. In this paper, we are proposing a multilevel access control system that manages access granted to different users such as physicians, nurses, family members and other health practitioners or researchers based on their need to know.

6.1. Privacy Requirements

In the healthcare environment, there are many different parties who need access to the healthcare data;

1. Healthcare organizations such as hospitals, laboratories and imaging centres.
2. Healthcare professionals such as family doctors.
3. Patients who should have full read access to the complete health records.

4. Any family member or a friend who the patients want to grant access to his/her data.

To ease illustration, we will use "owner" to denote the patient or patient's guardian in our system as in some circumstances the patient may not be capable of managing his/her own health records due to age or illness reasons. The following are the identified requirements for healthcare data online access:

1. Each healthcare unit should have the ability to determine the type/classification of the data it produces.
2. Owner should have the ability to grant or deny access to sensitive or private healthcare data to particular medical practitioners, healthcare unit or a family member.
3. Owner should identify a family doctor who will have access to all data classes.
4. Family doctor should be able to review healthcare data classification.
5. There must be an emergency attribute which allows the available healthcare practitioner to have access and to be able to provide assistance immediately.
6. Access could be granted to a team or a class of health professionals.
7. Owner should have the ability to delegate access to the healthcare data to someone else if required.
8. No-one should be able to overwrite old information but healthcare units and physicians should have the ability to add corrections to old information/reports.
9. Permission could be conditional to a given period of time or location. As an example, all access requests from a particular hospital are authenticated during the patient's admission time, bearing in mind the provided access level is determined by access policies.
10. Healthcare data should be available without obstruction to legitimate users and security policies should be easy to manage, maintain and modify once there is a need.

The core of the proposed access control system includes users' attributes that describe their association and roles and the classification of users' personal health data. The classification forms several data classes such as physical health, mental health and private health-related information.

The roles of users will be treated as the class of users. For example, GP is a class of all GPs, while a class specialist includes all different specialists who need to access the healthcare data. Besides health practitioners, owner can add a list of friends and family members as the "friend" class. The proposed system also considers the circumstances when this information is requested. Special access will be granted in emergencies and temporary access will be granted for a specific period of time if the patient is away from home. The access control policies simply regulate viewing access and addition of new data to healthcare records. Changing and deleting existing records is not allowed in order to preserve the healthcare and medical data history. Policies are not associated with individual records but with a collection of records that belong to a specific healthcare data class. There is no concept of a hierarchy of classes, so issues around policy inheritance are not relevant to the system described.

The healthcare professional requesting access to a patient's data must have a valid certificate. The process of getting access to patient healthcare data starts at the workstation which is connected to an authentication server. Authentication servers validate the healthcare professional's digital certificate, the patient's ID, then authenticate the healthcare professional and forward the access request to the authorization server. The authorization server checks access control policies for the patient and grants the proper access level to the healthcare professional. Policies are held by at the authorization server. This is not necessarily the same place the healthcare data itself is located but is similar to the authentication server. The actual evaluation of the policies is handled as an external service which is based on the rules and attributes supplied to evaluation.

FIDO (Fast IDentity Online) can be implemented to provide the authentication part of the proposed system. FIDO Alliance developed two protocols, the Universal Authentication Framework (UAF) and the Universal Second Factor (U2F). The authentication process uses public key cryptography and nonces to demonstrate possession of the private key. For the subject to be authenticated, the corresponding public key has to be registered with the server, which happens during an initial registration step [15].

In this paper we are going to focus on the authorization part of the access control for the healthcare system, as there are many successful implementations of the authentication process. Table 1 summarises some different healthcare data access control systems.

Table 1. Comparison of different healthcare data access control systems.

	Microsoft Vault	**PKB**	**NASH**	**Proposed System**
Default access	User chooses who has access to what information	Everyone in patient's health network	Any healthcare professional authorised by a healthcare organisation	Minimum set of data that is required in life threatening situations
Granularity	Patient can specify what data to share	Patient can share their own copy or give consent	Patient can choose which healthcare organisations have access to their data	Using subject and object classifications to grant access considering environment factors
Environment factors	Use time limited access	Nothing mentioned in relation to environment but consent engine can provide temporary access when required	Nothing mentioned in relation to environment factors when granting access to system users	Utilise environment factors such as date, time and location. Other factors could be added
Sharing	Co-manage health record of another user.	Patient can share their own copy of their health data or give consent	Using consent	Using policy model or adding someone to a group
Flexibility to add more control	No available information published in relation to the system design to indicate how the system handles new requirements	No available information published in relation to the system design to indicate how the system handles new requirements	No available information published in relation to the system design to indicate how the system handles new requirements	New classes can be added to subjects or objects. New environment factors can also be added.

There are attempts to use metadata to control access to medical records. In this particular case metadata associated with the patient, medical images and health professionals is considered as attributes that are used to control access in this medical imaging project grid. Semantic Access Control for Medical Application in Grid Environments [16] shows how metadata could be used to provide an efficient access control system to medical records using a set of connected computing elements and data storage on distant sites to provide a share of resources and storage capacity. The paper also introduced Semantic Access Certificates (SAC) as a way to authenticate users to medical data on the grid environments. Also, many systems have been developed to allow patients to bring together all their medical records from multiple providers including lab results, doctor's notes and health background. These systems regulate the health practitioner's access by providing patients with full control to authorize any person to access his/her own health record.

Patients Know Best (PKB) is a system that allows the patient to access healthcare data from all of connected professionals and organizations whenever they need it. It also allows patients to share with whoever they trust. The system has the ability to gain all of the medical data, connect wearable activity devices and communicate with health networks to track signs and symptoms in a safe and secure way that is approved by the US National Health Services NHS [17].

Privacy and security characteristics of Patients Know Best include:

- All healthcare data is consolidated in one record and controlled by the patient and available to everyone in patient's health network
- Patients can use privacy labels for each source of data and give privacy label permissions to different teams.
- Patients can see which teams have access to which privacy labels.
- Patients can share their own copy of healthcare data.

Another similar system is the Microsoft Health Vault, which provides a trusted place for people to gather, store, use and share health information online which is also approved by NHS.

Privacy and security characteristics of Microsoft Health Vault include:

- HealthVault user can share access with another healthVault user
- Patients can allow HealthVault programs to access and manage their data.
- Patients can share specific healthcare data with other people or programs that add data to health records
- HealthVault user can manage health records of a family member.

The Australian government, through the National Authentication Service for Health (NASH) project provides a nationwide secure and authenticated service for health organizations and personnel [18]. NASH provides healthcare professionals with access to electronic health data using a smartcard with a Public Key Infrastructure (PKI) certificate. Healthcare professionals can use their smart card and PIN to be authenticated from any workstation and to be able to send and receive digitally signed messages, prescriptions, hospital admission, hospital discharge and reports.

NASH grants health professionals access to healthcare data through the use of a PKI certificate located in the smart card they have been provided with after registering. The PKI certificate is an electronic document that includes information about the certificate's owner (subject) public key, the certificate's owner identity and a list of additional attributes (certificate extensions) and the digital signature of the Certification Authority (CA) that verified the information on the certificate.

Even though NASH is a national authentication service it easily can be used globally, by using cross certification to establish a trust relationship between the PKI certificates' issuers. Cross certifying health professionals will authenticate them and allow them to access patient's health records based on their attributes.

Privacy and security characteristics of NASH include:

- Logging login issues such as multiple failed logins and multiple login within a short period.
- Logging high transaction rates for a given Healthcare Provider
- Logging after-hours access and all instances of emergency access.
- Setting a Record Access Code (RAC) to allow and prevent access to patient's record unless in an emergency
- Flagging specific documents in patient's record as 'limited access,' and controlling who can view them.
- Removing documents from view and requesting healthcare providers to not upload information to the healthcare records.

6.2. Our Multi-Level Access Control Model

The proposed system is based on the Attribute-Based Access Control (ABAC) as it grants proper access level based on the attributes of people, data and environments. The system consists of two main components: the policy model that defines access control policies and the architecture model which defines the implementation of the policies to enforce access on data.

6.2.1. Attribute Definitions

Our model uses resource attributes, subject attributes and environmental attributes, as well as attributes extracted from the subject's PKI certificate. We also added attributes to resources that classify healthcare data to give more access control such as "physical health", "mental health" and "private".

- Resource Attributes

  A resource is an entity that is acted upon by the subject, such as the healthcare records. Resources have attributes that can help group them in records such as medications, medical history, or immunization. We defined six different classes that group healthcare data records.

  Public: The public class contains all healthcare data that is not sensitive such as;

  1. Health and activity data collected from sensors which may include; blood pressure, sugar levels, oxygen levels and any alarming information.
  2. Patient instructions, which is one of the most important fields that healthcare professionals need to view before dealing with the patient. It may contain warnings such as; the patient suffers from severe autism and could act out aggressively under pressure or wearing gloves and report any direct contact with the patient, as the patient could be vulnerable to infection or have an infectious disease.
  3. The public class could also contain allergies, medications, health maintenance schedules and lifestyle habits such as smoking, drinking and exercise.

  Physical: Physical classes contain all medical history related to diagnoses, laboratory and radiology results and all procedures that a patient has had or was scheduled for.

  Id_ info: ID info class contains all patients' identifying data such as name, address, emergency contact and ID.

  Mental: Mental health class contains the information related to mental diseases such as depression, bipolar, autism and personality disorders.

  Neuro: Neurological health class contains medical history of any nervous system related to issues that may cause some mental disorder symptoms such as Alzheimer's disease, stroke and injuries to the nervous system.

  Private: Private classes contain information that the patient does not want to share with anyone unless it is related to their treatment. Private healthcare data could include sexual orientation, history of drug use or social history.
- Subject Attributes: A subject is an entity requesting access, in our system s/he could be the healthcare professional, insurance agent, or a researcher. Each subject/user has associated attributes which define his identity such as; name, ID, job title and organization. Our system classifies users into the following groups:

  Owner: The owner of the healthcare data is the patient or patient's guardian. Owners should have access to all data classes.

  Family_doctor: A family doctor is the patient's primary doctor who is aware of the patient's health issues and history. Family doctors should have access to all data classes.

  Friend: A friend is a person who is nominated by the owner to have access to the patient's healthcare data. By default, the friend group should have access to all data classes except the Private class.

  GP: A GP is a doctor who temporarily treats patients due to the unavailability of the family doctor. GP should have access to Public, Physical, Id_info and Neuro data classes.

Researcher: A researcher uses the data to research new treatments, medicines or statistical purposes. We assume the research is on physical health and the researcher should have access to Public, Physical and Neuro data classes. A new rule should be added to the policy model for different research areas. The researcher must not have access to the identifying information (Id_info) which reveals the patient's identity.

Insurance: Insurance companies need access for claims or policy requirements. Insurance companies could have access to Public, Physical, Id_info and Neuro data classes.

Paramedics: Paramedics are trained to provide basic life support in short time frames. We assumed in our system that Public and Id_info should be sufficient for paramedic officers to perform their job.

Hospital: Hospitals should have access to all data classes except Private data class for each patient admitted. Hospital clinics should have the same access as GP groups.

Allied health: Allied health contains many professionals such as audiologists, dieticians, physiotherapists, occupational therapists, psychologists and social workers. The nature of these professions varies from providing purely physical treatments to purely mental treatments. On the other hand, occupational therapists assist people with illnesses and disabilities to develop and maintain daily living, or assist patients with mental health disorders such as autism. Based on these considerations, we decided to divide the allied health group into the following three subgroups:

1. *Allied_mental:* This group includes professionals such as psychologists and social workers. Professions of this group should have access to Public, Id_info, Mental, Neuro and Private data classes.
2. *Allied_physical:* This group includes professionals such as chiropractors, physiotherapists and podiatrists. Professions of this group should have access to Public, Id_info, Physical and Neurological data classes.
3. *Allied_both:* This group includes all allied health professionals who may deal with mental or physical disorders such as occupational therapists and speech pathologists. For this group, we set an environmental attribute "Require Social" to indicate if this patient has any mental disorder. The "Require Social" attribute allows the professionals of this group to have access to "Mental" data class in addition to the "Allied health physical" group access.

- Environment Attributes: Environmental attributes describe the operational and technical conditions that affect access, such as the date and time when hospital staff can have access to patients' records. Environmental attributes also include location; owner could allow all requests from hospital workstations while he is admitted to hospital. We include other environment attributes such as Emergency, location, date and Require_social.

6.2.2. Policy Model

Our policy model uses "u", "hd", "e" to denote authenticated user group, healthcare data class and environment respectively and functions to confirm user and healthcare data attributes. Our system assumes the owner of the healthcare data is the patient or the patient's guardian if the patient is not able to manage his/her own records for age or illness reasons.

The general form of the policy rule that decides whether a user u can access healthcare records hd in a particular environment e is the following Boolean function.

Rule: can_access (u, hd, e) ← f (Attr (u), Attr (hd), Attr (e))

According to this rule, user u will be granted access to healthcare records hd if the attributes of u, attribute of hd and attribute of e is evaluated by the function f and returned true.

- **R1:** can_access (u, hd, e) ← ((group (u) ϵ {Paramedics})∧ (data_class (hd) ϵ {Public, Id_info})) ∨((group (u) ϵ {Researcher})∧ (data_class (hd) ϵ {Public, Physical, Neuro})) ∨((group (u) ϵ {Owner, Family_doctor})) ∨((group (u) ϵ {Insurance})∧ (data_class (hd) ϵ {Public, Physical, Neuro, Id_info})) ∨((group (u) ϵ {Friend})∧ (data_class (hd) ϵ {Public, Physical, Neuro, Id_info, Mental}))

In R1, there are no environment constraints as they are irrelevant for this rule and there are five cases under which the authenticated user u will be granted access.

Case1: if u belongs to the "Paramedics" group and requests access to healthcare data from the "Public" or "Id_info" classes.
Case2: if u belongs to the "Researcher" group and requests access to healthcare data from the "Public", "Physical", or "Neuro" classes.
Case3: if u belongs to the "Owner" or "Family_doctor" groups, access is granted.
Case4: if u belongs to the "Insurance" groups and requests access to healthcare data from the "Public", "Physical", "Neuro", or "Id_info" classes.
Case5: if u belongs to the "Friend" group and s/he requests access to healthcare data from the "Public", "Physical", "Neuro", "Id_info", or "Mental" classes.

- **R2:** can_access (u, hd, e) ← ((group (u) ϵ {GP})∧ (data_class (hd) ϵ {Public, Physical, Neuro, Id_info})) ∨ ((group (u) ϵ {Hospital})∧(data_class (hd) ϵ (Public, Physical, Neuro, Id_info, Mental)))

In R2: there are also no environment constraints for this rule and there are two cases where the authenticated user u will be granted access.

Case1: if u belongs to the "GP" group and requests access to healthcare data from the "Public", "Physical", "Neuro" or "Id_info" classes.
Case2: if u belongs to the "Hospital" group and requests access to healthcare data from the "Public", "Physical", "Neuro", "Id_info" or "Mental" classes. We included "Mental" as the patient may be admitted to hospital for a period of time and the hospital staff should be aware of any mental care that patient may require.

- **R3:** can_access (u, hd, e) ← R2 ∧ ((environment(e) = Date) ∧ (Current date ≥ 01022017) ∧ (Current data < 01032017))

In R3, we just follow the access rule R2 and add an extra level of access control, that is, the date when a GP or hospital staff requests access. The date is an environment attribute that the healthcare data owner specifies to limit access to patients' records to a certain period of time. The specified dates could be hospital admission and discharge dates or the time where the family doctor is unavailable. The rule simply grants access as in rule R2 but only for the month of February 2017.

- **R4:** can_access (u, hd, e) ← ((group (u) ϵ {GP, Hospital})∧(environment (e) ϵ {Emergency}))

In R4, we have Emergency as an environment attribute. This rule gives access to all healthcare data classes to doctors or hospitals as a result of a preapproval from the owner in emergencies. Emergency situations should be defined by a physician or the family doctor, which may include poisoning, suicidal attempts, or unconsciousness.

- **R5:** can_access (u, hd, e) ← ((group (u) ϵ {Allied_physical, Allied_both})∧ (data_class (hd) ϵ {Public, Physical, Neuro, Id_info})) ∨ ((group (u) ϵ {Allied_mental})∧(data_class (hd) ϵ (Public, Mental, Neuro, Id_info, Private)))

In R5, there are also no environment constraints for this rule and there are two cases where the authenticated user u will be granted access.

Case1: if u belongs to the "Allied_physical" or "Allied_both" groups and requests access healthcare data from the "Public", "Physical," "Neuro," or "Id_info" classes.

Case2: if u belongs to the "Allied_mental" group and requests access to healthcare data from the "Public", "Physical", "Neuro", "Id_info" or "Mental" classes.

- **R6:** can_access (u, hd, e) ← R5∧ ((environment(e) = Location) ∧ (Location(u) ϵ {L}))

In R6, we just follow the access rule R5 and add an extra level of access control, that is, the location of the user. Healthcare data owner can specify a list of locations when the allied health professionals are granted access to the healthcare data. The same rule could be applied for the users of a GP and a Hospital group to limit access to GPs from L list of locations.

- **R7:** can_access (u, hd, e) ← ((group (u) ϵ {Allied_both})∧ (data_class (hd) ϵ {Public, Physical, Mental, Neuro, Id_info, Private})∧ (environment (e) = Require_social))

In R7, we added an environment attribute "Require_social", which controls the access of allied health professionals to the mental and private data under circumstances where professionals from the "Allied_both" group need to assist patients with both mental and physical issues.

6.2.3. Architecture of Multi-Level Access Control

The architecture model of the proposed attribute based access control system for the healthcare data is illustrated in Figure 3.

- Access Enforcement Engine (AEE): AEE is responsible for requesting the authorization decision and enforcing it. It is the only point of access for users who request access to healthcare data. Initially authenticated user "u" sends AEE an access request for a healthcare data class "hd". Then, AEE collects user and healthcare data class attributes and sends them for evaluation. Finally, AEE receives the access decision from the Access Decision Engine and either grants users access or denies their request.
- Healthcare Data Repository: a healthcare data repository is any server used to store the data online.
- Access Decision Engine (ADE): ADE is responsible for evaluating policies and making the access decision (grant or deny). ADE gets attributes of the user and healthcare data classes from AEE, retrieves environment attributes and then checks the policy for the appropriate policy rule and finally forwards the decision to AEE.
- Policy Repository: Policy repository stores all access rules. Policies are defined by the owners and healthcare professionals through a designated user interface.

Our model works as follows. Initially, AEE receives access requests for certain healthcare data from an authenticated user, extracts user attributes and healthcare data class and sends them to ADE. ADE retrieves environment attributes, validates all attributes against Access Policy rules and then returns "grant" or "deny" to AEE. AEE, in return, enforces the access decision on the user.

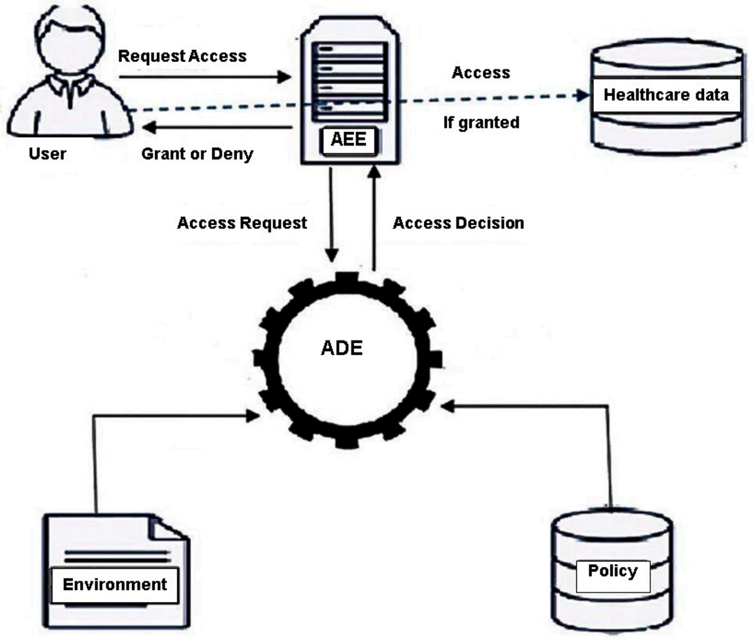

Figure 3. Architecture Model.

7. Discussion

Initially, we needed an access control model with a good level of flexibility to regulate access to digital healthcare data stored in the cloud. The nature of users requesting access to the stored data is a real challenge when it comes to defining an access control model. These groups of dynamic users who may request access occasionally was the main reason we chose ABAC model.

The assumption in the proposed model is that the patient or patient's guardian is the owner of the healthcare data. The system has predefined access policy rules similar to our policy model. These access rules should be discussed with different healthcare professionals to enable the best treatment and care for the patient. It is the owner's responsibility to define extended policy rules and to define and approve any extra environment attributes that grant access under certain circumstances.

The flexibility of our policy model is demonstrated by supporting multi-level access control and by easily implementing combinations of more than one rule. Our system could also be extended to address more complicated issues such as a default access rule for new data attributes, joint ownership, owner authority and any other related issues.

- **Default access rule:** in the case of uploaded healthcare data that have the minimum set of attributes and with no data class defined, there should be a generic access rule to allow or deny access, or to classify these data under certain classes. For example, if a decision was made to collect environmental data such as temperature or radiation levels and add this data to healthcare data, a default rule must be defined to grant access to all requests, assuming no category means public class, or to deny access, assuming these data are categorized as private.
- **Joint Ownership:** The owner could give (delegate) one or more ownerships over his data. For example, all children could be owners for their elderly parents. In the case of a joint ownership, we should have more than one access policy over the same data class, as owners can specify their own access rules. Our system grants access to some data when any one of the policies permits the access, which means the relation between the access policies is the logical "or" relationship. Assume both parents are owners of their child's healthcare data. The father grants Dr. John access to the healthcare data of his child while the mother denies the access. The Access Decision Engine (ADE) will check both access policies in a policy repository and the Access Enforcement Engine

(AEE) will return with permission to access the healthcare data of the child because one of the policies grants Dr. John access.

- **Owner authority:** in our system, healthcare data could have more than one owner, thus there may be conflicts when not all owners agree or disagree to grant access. This raises more concerns about authorization: do all owners have equal authority, does any owner have the ability to add more owners, or does a new owner have the authority to turn certain private data to public. Our system has only one primary owner who has full control over the data. The primary owner could be either the patient or one of his guardians, any other owners will be a secondary owner who can only grant and deny access requests but cannot add more owners or change data sensitivity.

8. Conclusions

In this paper, we have proposed a context-aware solution that helps older people to live independently in a safe environment with integrated multi-faceted authorization. Our IoT based system provides a care management process for elderly people who live alone by monitoring their daily activities and reporting any abnormality in their daily routine, based on analysing the signals collected from passive RFID. The system features a new multi-level access control mechanism that was introduced to secure access to healthcare data. The implemented mechanism is an attribute-based model which adheres to the dynamic nature of the healthcare organization and has the flexibility to adapt to new access requirements.

Author Contributions: U.S. and L.Y. conceived of the presented idea and developed the analytical method. U.S. analysed the data and carried out the experiments. U.S. wrote the manuscript with support from L.Y. and H.-y.P. All authors provided critical feedback and helped improve the manuscript.

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. Memon, M.; Wagne, S.R.; Hansen, F.O. Ambient assisted living ecosystems of personal healthcare systems, applications, and devices. In Proceedings of the Scandinavian Conference on Health Informatics, Copenhagen, Denmark, 20 August 2013.
3. 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]
4. Park, N. Customized healthcare infrastructure using privacy weight level based on smart device. In Proceedings of the International Conference on Hybrid Information Technology, Daejeon, Korea, 22–24 September 2011.
5. Premarathne, U.; Abuadbba, A.; Alabdulatif, A.; Khalil, I.; Tari, Z.; Zomaya, A.; Buyya, R. Hybrid cryptographic access control for cloud-based EHR systems. *IEEE Cloud Comput.* **2016**, *3*, 58–64. [CrossRef]
6. Gajanayake, R.; Iannella, R.; Sahama, T. Privacy oriented access control for electronic health records. *Electron. J. Health Inform.* **2014**, *8*, e15.
7. Abbas, A.; Khan, S.U. e-Health Cloud: Privacy Concerns and Mitigation Strategies. In *Medical Data Privacy Handbook*; Springer: Berlin, Germany, 2015; pp. 389–421.
8. Begum, M.; Mamun, Q.; Kaosar, M. A privacy-preserving framework for personally controlled electronic health record (PCEHR) system. In Proceedings of the 2nd Australian eHealth Informatics and Security Conference, Perth, Australia, 2–4 December 2013.
9. Fabian, B.; Ermakova, T.; Junghanns, P. Collaborative and secure sharing of healthcare data in multi-clouds. *Inf. Syst.* **2015**, *48*, 132–150. [CrossRef]
10. Zhang, R.; Liu, L. Security models and requirements for healthcare application clouds. In Proceedings of the 2010 IEEE 3rd International Conference on Cloud Computing (CLOUD), Miami, FL, USA, 5–10 July 2010.

11. Yao, L.; Ruan, W.; Sheng, Q.Z.; Li, X.; Falkner, N.J.G. Exploring tag-free RFID-based passive localization and tracking via learning-based probabilistic approaches. In Proceedings of the 23rd ACM International Conference on Information and Knowledge Management, Shanghai, China, 3–7 November 2014.
12. Yao, L.; Sheng, Q.Z.; Li, X.; Gu, T.; Tan, M.; Wang, X.; Wang, S.; Ruan, W. Compressive representation for device-free activity recognition with passive RFID signal strength. *IEEE Trans. Mob. Comput.* **2018**, *17*, 293–306. [CrossRef]
13. Mandal, A. Symptoms of Movement Disorders. News Medical 2012. Available online: http://www.news-medical.net/health/Symptoms-of-movement-disorders.aspx (accessed on 10 February 2018).
14. Zissis, D.; Lekkas, D. Addressing cloud computing security issues. *Future Gener. Comput. Syst.* **2012**, *28*, 583–592. [CrossRef]
15. Fido-Alliance. Simpler, Stronger Authentication. Available online: https://fidoalliance.org (accessed on 28 February 2018).
16. Seitz, L.; Pierson, J.M.; Brunie, L. Semantic access control for medical applications in grid environments. In Proceedings of the Euro-Par 2003 Parallel Processing, Berlin, Germany, 2–5 September 2003; pp. 374–383.
17. Strickland, M. Patients Know Best: A Changemaker Health Case Study. Available online: https://medium.com/change-maker/patients-know-best-a-changemaker-health-case-study-2f203b0971ae (accessed on 31 January 2018).
18. Australian Government. National Authentication Service for Health, D.H.S. Available online: https://www.humanservices.gov.au/organisations/health-professionals/services/medicare/national-authentication-service-health (accessed on 31 January 2018).