International Journal of Psychology , Social and Educational Sciences
Vol.4, NO.2 , P:182 - 203
Received: 20 December 2021
Accepted: 24 January 2022

Investigating security strategies in pervasive healthcare

Hamed Yarahmadi

Master of Computer Software Engineering

Abstract

The first step in examining security strategies in pervasive healthcare is cloud computing, because all of these strategies work based on these computations, so in the first step we need to complete our understanding of pervasive computing. In this article, we investigate all security strategies in pervasive healthcare, after identifying and then examine the security of these strategies in the science of pervasive healthcare against potential threats and dangers. We introduce all strategies in general and explain their advantages and disadvantages. Then we determine the advantages of each over the other and determine which strategy or suggestion can solve the shortcomings of the desired strategy.

Keywords: pervasive healthcare, physiological values, MPEG-21I PMP, RFID, EPR

1. Introduction

CLOUD COMPUTING is one of the fields that aims to create a world which the objects around us (which we deal daily) have the power to process and connect to the World Wide Web wirelessly or by cable. This model is called as the third wave of information processing. In the first wave (in the 1960s) many people had to share a computer, and in the second wave (1980s) each person had access to a personal computer. But in the third wave (the emergence of the idea of pervasive systems), each person automatically, without making any special adjustments, receives a personalized service from computers embedded in their environment (and hidden from their view). One of the sub-collections of cloud computing is pervasive healthcare, which works based on telemedicine and cloud computing technology (Kumar 2012). The main problem of this method is its security. In this regard, various strategies have been proposed and we identify the shortcomings of all strategies by examining and comparing them. We offer suggestions for each of them to solve their shortcomings.

2.CLOUD COMPUTING

Cloud computing is a model that process information of activities and objects that human beings deal with daily. Unlike the typical desktop model which a person consciously sits at a computer desk and does something, in the cloud computing model, a person uses many computing systems and devices to perform a normal activity without even knowing it. Some called this communication. The deepest technologies are the ones which the hardware is minimized. Cloud computing is taking a step in this direction. This Computation began in Mark Weiser's article, which described ubiquitous or invisible computing in 1988, which was later called Cloud computing. Perhaps the next vision of these computations is not just to create saturated environments with pervasive computations. Figure 1 shows the three existing generations in a combined form.

computing model as the third wave of computing (Mohamed Almorsy 2016). In the first wave, many people had to share a computer, in the second wave each person had access to a computer but in the third wave each person had access to many computers. Three key technical problems in this method are: UI power consumption and wireless communication. The information age was born over 60 years ago and has changed our lives a lot. Now, by entering the cloud computing age which have emerged 2 decades ago, we face with more peace and close

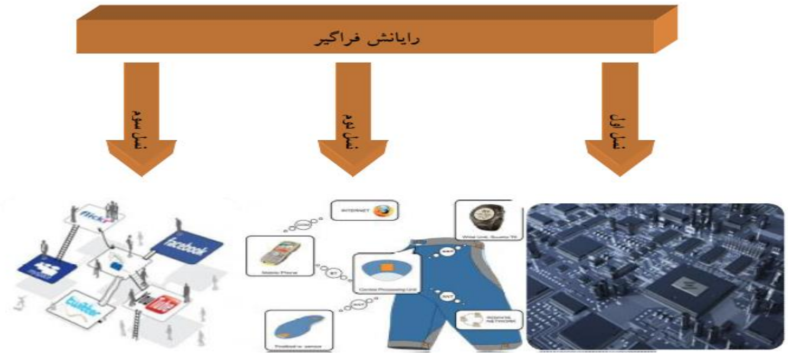

Figure (1) Generations of cloud computing

connecting "anything to something else". Some features of this generation include the manufacturing special all-purpose information and processing devices, activator sensor systems for (implicit) interactions between humans and machines, and the introduction of capabilities such as self-configuration and self-protection, self-optimization.

The second generation of cloud computing systems is called the generation of awareness which was formed between 2000 and 2007. This

As you can see in Figure 1, the first generation of cloud computing, known as connectable generation, covers the years 1991 to 2005. In this generation, new advances in technology (such as downsizing of electronic and telecommunication equipment, cheaper and more powerful processing, communication, and storage equipment, (Acharya 2010) and, new wireless communication standards) have been used to achieve the idea of freezers - door handles - lighting fixtures - shoes - hats - and even coffee cups and most importantly the human body use cloud computing by placing the chips needed in them for Connect to an unlimited network or connect to other devices or connect to a central server to provide the needed information, such as connecting a chip or wearable computer to the human body, which gives the hospital server data about human physical condition.

2.1-pervasive healthcare

Pervasive healthcare is a subset of cloud computing that works on the basis of chips, sensors, Internet networks, and wearable computers, that is, through special chips embedded in a patient's body or through putting on a special bracelets. The patient's condition is transferred to the hospital server at any time of his movement or life through the software fixed on the mobile phone and any other electrical device to better assess the patient's condition. Whenever he needs to take care, doctors help him or her. Figure 2 shows an example of a pervasive healthcare (Kumar 2012).

generation is based on sensor-based detection systems and new technologies for processing and presenting knowledge. In this generation, research issues such as context-aware and future-aware systems, self-aware or source-aware have been the focus of researchers. The most famous systems presented by Dey in 2001. In fact, every being or object in the environment is a part of the context, and any awareness or knowledge about any of these entities is a kind context awareness.

The third generation of cloud computing systems is called social cloud computing. The main purpose of social cloud computing is to take advantage of the features of the two fields of cloud processing systems and social networks. In social networks, the most important entity is the users. Given this issue, social context is often referred to individuals, groups, and associations. There are other definitions of social context in scientific articles. It should be noted that even information such as keywords that a user uses to search on Google or a person's online purchases can be implicitly considered as a social context. So ships - airplanes - cars - bridges - tunnels - machines - refrigerators -

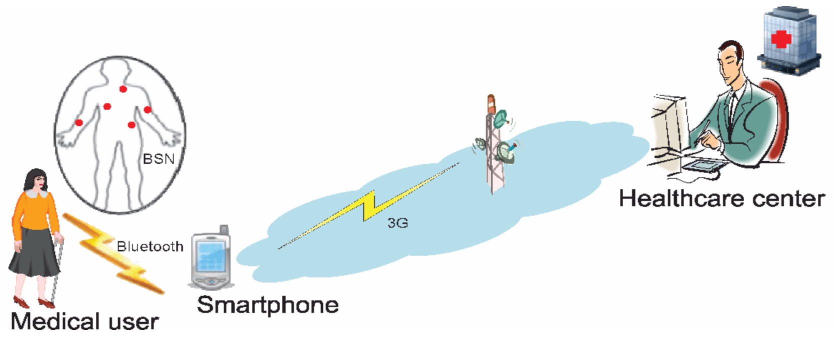

Figure (2) An example of a pervasive healthcare

compared in details in the following sections. And finally some suggestions are proposed to address their shortcomings. To better understand pervasive healthcare and the importance of its security, in figure 3,a three-level model is shown as an example.

But this technology is prone to all kinds of malicious and disruptive attacks, because it works based on NETWORKING systems, so based on maintaining security in these systems and protecting personal information, security strategies are provided for this technology that each of them will be explained and

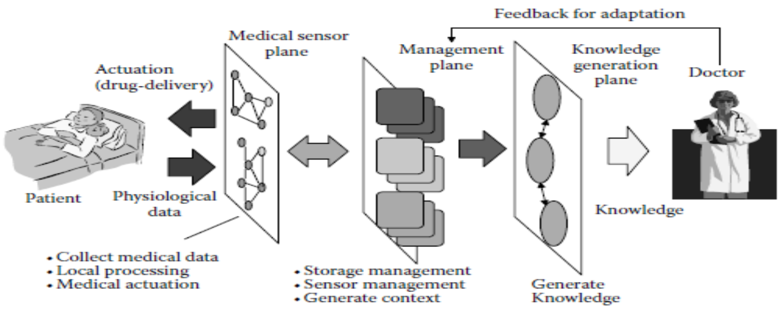

Figure (3) A general model for a pervasive healthcare system

knowledge (Krishna K 2006). But what do these levels provide? Medical sensor level: This level provides the basis for the inclusion of a large number of different types of medical sensors in the system. These sensors have the ability to continuously or intermittently monitor various physiological parameters such as ECG, blood

Conceptually, this model consists of three main levels. In order to better understand how pervasive health works, the three levels of the figure are explained to understand how it works. The first level is the level of medical sensor, the second level is the level of management, and finally the third level is the level of production (generation) of

Reasons for this vulnerability: health records (on paper) are highly centralized for data storage, and any copying of this information is a time-consuming process. But this problem is eliminated in this method because the information is on the network and it is easy to access and can be copied easily. So, it poses many threats (Kosch 2013) and unauthorized manipulation. Some potential threats to the pervasive healthcare system include:

1 .Unauthorized access to health data

2. Deliberate change of health information of certain patients, leading to incorrect diagnosis and treatment

3.Deliberate sounding of incorrect alarms or suppression of real alarms raised by the system in case of emergency

4. Economic and social discrimination of patients

The concept of security in the field of pervasive healthcare is different from traditional systems and relies on the maintenance of three features.

1. Data integrity: all information provided is correct and cannot be changed in any way (during transferring and storing)

2. Confidentiality of information: information should be given only to those who are authorized and only they should be able to disclose the information.

pressure, detect body temperature, galvanic resistance of the skin and various movements of body organs. The sensors may put on by the patient (wearable) or put inside the patient's body. Management level: This level provides the necessary infrastructure to manage the health of the data collected using the sensors. This raw information of the sensors is organized under a special format called the EPR record.

EPR: Collecting health data about a patient so that it can be stored and easily accessed. And computing devices such as Pocket PCs, cell phones, PCs, and servers are used to run the management level. (Krishna K 2006)

Knowledge Generation Level: it argues the collected data which is used in EPRS and stored by the last two levels (Krishna K 2006). It is at this level that features such as diagnosing the occurrence of a medical emergency, failure of a particular treatment method, incompatibility and contradiction between the proposed diagnosis and symptoms are identified.

Although pervasive healthcare uses the EPRS format to collect health data and goes beyond recording in a paper file method, it poses many security problems to healthcare (health). It may lead to unauthorized access and manipulation of sensitive health data of patients.

in the case of medical sensor (Krishna K 2006)

Securing sensors inside the body requires a device for symmetric encryption as a public key infrastructure that is too expensive. Proponents of using sensors in the human body have proposed a way to encrypt information to secure information between communication sensors within the body. As the human body is a highly dynamic environment, it can produce many specific physiological values rather than being easily predictable. (but it is random and from a wide range of values) and help the sensors to collect information, but this information must have the necessary security. Both transmitter and receiver sensors can measure physiological values and use them for security purposes.

Note: The main idea of this design is explained below in figure 4.

3. Confirmation: to ensure the correctness of the claimed identity when connecting with different entities

2.1.1 Security in sensor networks with physiological values (first strategy)

Security of public sensor networks is an important issue today because public sensor networks play an important role in pervasive healthcare. These sensors are used to collect health data from patients. One of the most important needs of medical sensors is that they should not interfere with the activities of the person wearing them. This requires small sensors that can fit inside the body. As the security of the overhead adds to the system, it should be ensured that this overhead is at least simultaneously. When the values are measured, the values of KS and Kr are for the sender and receiver, respectively. A random KsessiOn

Figure (4) Security in sensor networks

The main idea in this design is based on the previous measurements by the sender and receiver and their physiological verification (PV) individual, and any differences in these values in treatment show themselves as communication errors that the error correction code is used in these cases. Therefore, the receiver performs the error correction in Ḱsession K″ **session** ***(*** K″ **session =** ***f*** **(Ḱ*session*)**

Note: f is the error correction code. The receiver calculates its calculation's version using the MAC used in K″ **session.** Mac' **=**MAC (K″ **session** | C). If MAC and mac' values are the same, then the receiver decrypts C to obtain the information.

Figure 5 shows the securing of communications in the body's sensor networks, using physiological values encrypts the shipment with [C = EK session (Data)], and then hides KsessiOn using KS and one-time calculations on it (γ = K session $\oplus$ Ks). It also calculates (Krishna K 2006) the code of a message (MAC). The message here is encrypted using the C encrypted message used in K sessiOn (mac = MAC (K session | C)) and allows verification to maintain the integrity of the message. The sender then transmits the message [C, γ, mac] to the receiver, then uses Kr and γ to obtain Ḱsession (Ḱ session = γ $\oplus$ Kr). Due to the dynamic nature of the human body, the value of KS and Kr may be the same, resulting in Ksession ≠ Ḱsession, and most researchers claim that the measured value of PVSs is very close to the

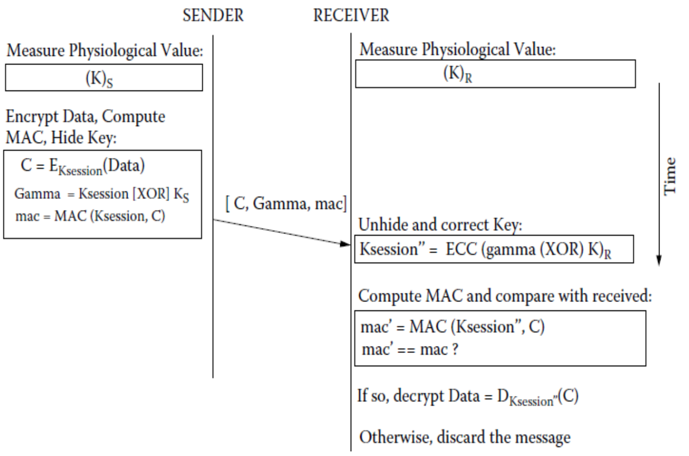
SENDER
RECEIVER
Measure Physiological Value:
$(K)_S$
Encrypt Data, Compute MAC, Hide Key:
$C = E_{Ksession}(Data)$
Gamma = Ksession [XOR] K_S
mac = MAC (Ksession, C)
[C, Gamma, mac]
Measure Physiological Value:
$(K)_R$
Time
Unhide and correct Key:
Ksession" = ECC (gamma (XOR) $K)_R$
Compute MAC and compare with received:
mac' = MAC (Ksession", C)
mac' == mac ?
If so, decrypt Data = $D_{Ksession"}(C)$
Otherwise, discard the message

Figure (5) Securing communications in the body's sensor networks, using physiological values

Privacy of information collected and protection of EPRs by distributed

2.1.2. Controlling access to EPRs (second strategy)

of roles to users provides an information identity of the privileges associated with them for a higher level of scalability and forms an access control list called ACL (Anagnostopoulos 2014) which maintains a list of information access privileges for each role, so the main advantage of an RBAC system or mechanism is based on the ability to reduce complexity and attempt to manage large-scale systems access.

RBAC format is for access control of medical information. And there is an argument that access control schemes used in healthcare settings support two types of silent policies.

1. (GC-ED): Eligible public consent by explicit denial
2. (GD-EC): Eligible public denial by explicit consent

These two policies can be discussed further to understand better, for example, the first example: all doctors allow to access except Dr. X. And for the second policy, as the second example: no doctor is allowed access except Dr. X. In the second type, access is severely restricted, but the second type is easier to prevent unauthorized access for all users because here all but one is unauthorized users.

on the other hand,)GC-ED) is useful for productivity. For example, using the GC-ED mechanism, a hospital can design by default a set of specific policies to prevent access to patient network and architecture is one of the pillars of security in pervasive healthcare. Privacy of EPRs when they can be seen by different people such as nurses and patients' families - pharmacies - insurance companies - drug manufacturers for economic services and health and medicine services that this sharing of medical information must be to the patient's informed consent. Pervasive healthcare needs controlling access schemes to fulfill the needs of pervasive healthcare in access control of EPRs in order to maintain the security of pervasive healthcare. This section describes how to authorize access to EPRs because different accesses by different people compromise the security of the information obtained and lead to misuse of the information.

RBAC (Role-Based Access Control): one of the techniques of access control in pervasive healthcare systems is role-based access control (RBAC). This is an access control mechanism that organizes users within the system into special groups based on the special role given to groups and their performance in groups. For example, all doctors in the hospital are in the role of doctor and the role given to them is doctor and all nurses in the hospital are assigned the role of nurse. RBAC assigns privileges to these roles to control access and maintain information security, this assignment implementation policy for the access of all doctors except Dr. X.

But a solution to this problem is provided, which is a simple format of RBAC in which an access control model is defined that records policies of access to patient information and is implemented through a pivotal role called Care Team Role(CTR).

A CTR consists of four main components

1. List of roles that allow access to patients' health information

2. List of roles that don’t allow access to patients' health information

3. Access privileges

4.Administrative information about CTR such as ID and its description

Figure 6 shows the structure of the CTR sub-structure and figure 7 shows the relationship between roles and permissions when using CTR

information, because in this policy we are dealing with a wide range of accesses, and it is not just for one person and it is more natural based on the health environments that a group of different people deal with this information, but this policy has a big problem that we mention.

In RBAC, a role can only execute the privileges assigned to it and no more, and based on the nature of that role, GD-EC scenarios can be expressed. Implementing GC-ED in RBAC is frustrating because then we need to list all the people who have access to the information and define a role for each of them, which can sometimes be very tedious and even impossible (Krishna K 2006). If access is restricted to a frustrating of users, this role can be very frustrating. For example, if the restriction defines for the role of a clinical specialist, the other role which is the child of that role, inherit this restriction from that role. So, we cannot easily do an

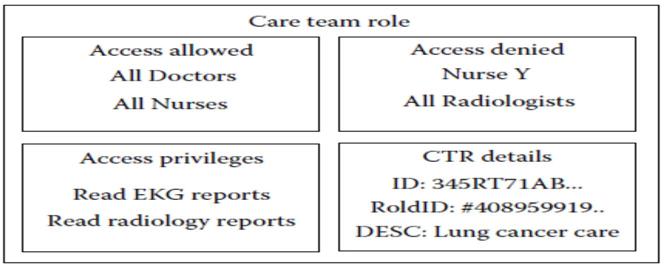

Figure (6) structure of CTR sub-structure

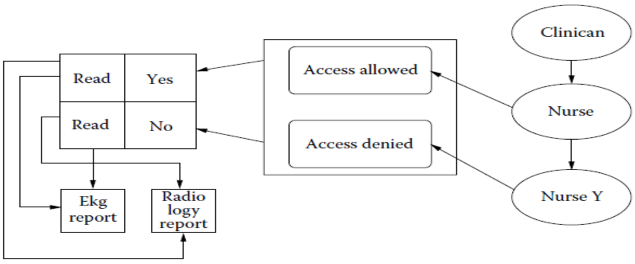

Figure (7) The relationship between roles and permissions when using CTR

which exchange medical information.

Although MPEG-21 is a standard used to share digital multimedia content, we argue that it can be used to protect data and user privacy in a comprehensive medical environment. It is assumed that digital content of medical information is provided by EMDs (embedded medical devices) (Fragopoulos 2009). Here the creator of the information content can be any supervised "user". supervisors or doctors can be the “end user" who have access to the server and to the information.

It is argued that a general security framework based on the mpeg-21 standard for wearable EMDs should be adopted to fill the gap that reduces the vulnerability of these devices against any kind of attack. As the medical measurements are taken from patients by EMDs, these measurements or information can include a variety of data in addition to raw data, such as a snapshot of the heartbeat data in a JPEG file or a video file of the heartbeat data. The

2.1.3. Using MPEG-21I PMP (Third Strategy)

MPEG-21 and IPMP (Intellectual Property Management and Protection) components can be used to protect and transmit medical information and enhance patient privacy. As we have said before, with the increasing reform of the pervasive healthcare system and the provision of its communication infrastructures such as wireless networks, Ad hoc and WiMAX-GSM-WCDMA-UMTS networks, etc., new security strategies will be provided such as the security framework that we have introduced.

MPEG-21: is a standard that includes mechanisms and tools for sharing digital rights, permissions and restrictions on digital content from the content creator to the content consumer. This standard is based on XML (Kosch 2013) to communicate easily and can be read by a variety of machines. And be unambiguous everywhere for communication among institutions

2.**Passive enemies**; are malicious users who create implicit interference in EMD through eavesdropping and communication links between EMD and other systems or through sid-channel attacks.

3. **Insiders** who include the most likely enemies. Theses attackers include healthcare personnel - nurses - doctors and IT specialists and even the patients themselves.

This architecture includes any kind of EMDs and their security and safety objectives. The identification of this architecture is in two directions; one is about security and operation objectives and another is security related objectives and privacy. Here are some of the security aspects that should be present in the pervasive healthcare system and are also considered in our architecture.

1.Access to medical data, i.e. ensuring that only the right people should have access to EMDs and medical information

2. Accuracy of data measurement that all data and measurements of EMD should be accurate

3. Tracing and identifying EMDs that in case of doubt, the accuracy of the information can be traced by tracking and seeing the person.

4. Modify and configure EMDs that authorized personnel can modify its configuration

MPEG-21 standard can help us deliver content. (Kosch 2013)

One of the main features of the approach we are introducing is that this approach has a direct impact on medical safety and the effectiveness of treatment and includes the MINIMALIZM standard, which ultimately affects the reduction of overall healthcare costs, thus leading to better use of limited resources in health care (Kosch 2013)

Medical data are obtained from different types of EMDs that are placed on the patient's body to identify the security mechanisms that should be implemented in the proposed architecture. These two measures should be taken in the direction of pervasive healthcare's security, and this architecture is no exception.

1.Potential attack and malicious users of the environment should be identified

2.Necessary security and privacy measures should be taken

To do the first step, the malicious users should be identified in an inclusive healthcare environment. There are three categories of users presented by Halperin et al. which are listed below.

1. **Active opponents**; are malicious users who have explicit involvement and physical access to an EMD

Figure 8 shows the digital item hierarchy

5.Exploit resources by increasing the battery life of EMDs by minimizing power consumption

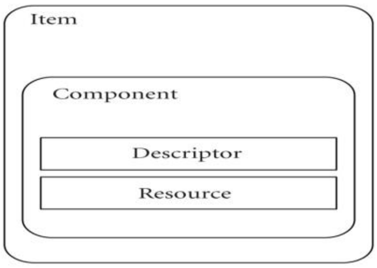

Figure (8) Digital item hierarchy

2019) The main concept in MPEG-21 IPMP is to use IPMP tools to protect digital items. These tools are not pre-defined for these standards, but any user, vendor, etc. may define and implement a set of tools that can perform basic security operations such as encryption algorithms, decryption, authentication, data integrity, cover-up, and fingerprinting mechanisms (Fragopoulos 2009). Using MPEG-21 IPMP components, we protect the entire DID or part of the DI through the main DIDL elements. We want to protect the main elements through adding IPMP information by referring to the tools and their mechanism. MPEG-21 IPMP is a new definition for the set of IPMP DIDL elements, which is the role and semantics of the element defined in DIDL. The structure of an IPMPDIDL element can be seen in Figure 9.

Security problems result from the reality of the digital items' description. The structure of these items includes content, features, and big data. It is clear that an xml document is easily visible and vulnerable to anyone for unauthorized use. According to this issue, MPEG-21 includes a section called Intellectual Property Management and Protection (IPMP), which provides a mechanism for protecting digital items.

MPEG-21 IMPMP, in conjunction with MPEG-REL, creates the Rights Expression Language (REL) for the user and creates a framework that enables all users to share a range of rights and benefits in digital content deliver in digital items and to ensure these rights and benefits, reliable management and protection is performed across a wide range of networks and devices (Pijush Kanti

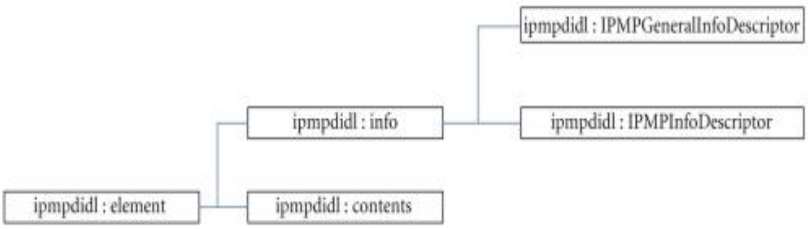
ipmpdidl : IPMPGeneralInfoDescriptor
ipmpdidl : info
ipmpdidl : IPMPInfoDescriptor
ipmpdidl : element
ipmpdidl : contents

Figure (9) The structure of an IPMPDIDL element

More specifically the ipmpdidl: IPMPInfoDescriptor element contains the child elements that you see in figure 10.

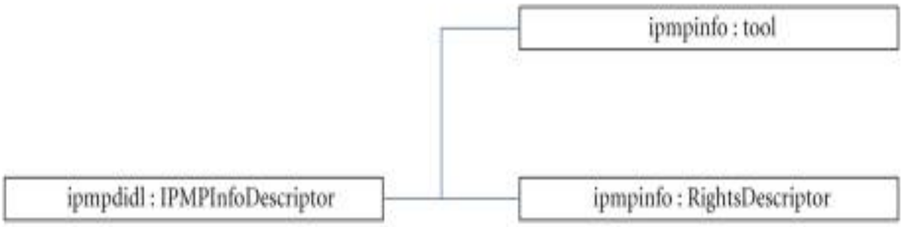

Figure (10) Children of the ipmpdidl: IPMPInfoDescriptor element

Using figure 11, we better explain the third strategy.

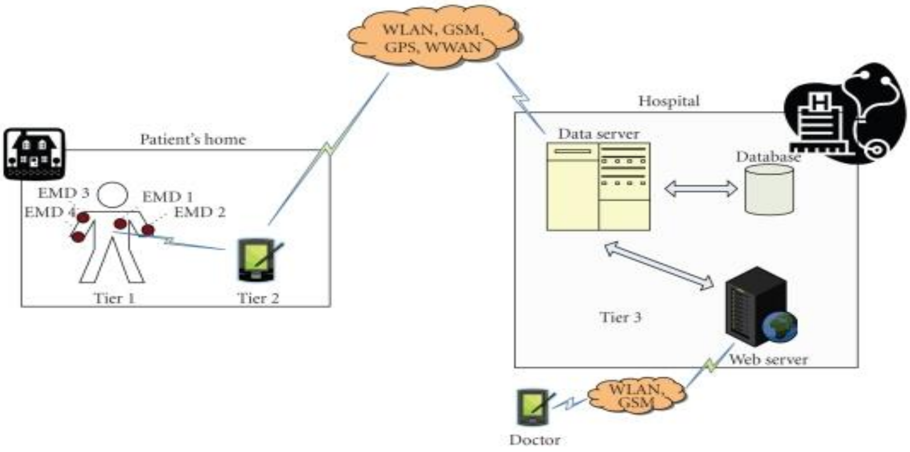

Figure (11) Proposed architecture for explaining the third strategy

communication networks. After configuring the network, the personal server application is started to manage the network, channel and time synchronization, data acquisition, data processing, data fusion and so on. In addition, to make a channel available, personal server connects a secure link to Tier3, and transfers reports or files that are further processed to be stored integrated in the patient's health record. The personal server stores the data locally so that the channel is available.

Tier3 includes a medical server that actually includes other servers such as an emergency server, a healthcare server, a medical records server, an email server, and a thin clint. The medical server application runs medical server for remote access using the secure link applet visualization that includes a wide variety of applications, such as communication channel to personal servers, integrating patient medical records data, and storing it in a database.

The medical server collects medical information by the EMDs and sends it to a pda, which is responsible for creating the mpeg-21 for protection, and includes permits and licenses shown in Figure 12.

Tier1 includes a number of portable EMDs equipped with related sensors that are responsible for processing and maintaining information and are called wwpan wireless wearable personal networks, (Kosch 2013). Each wwpan can obtain a sample of parameters and process one or more physiological parameters. More specifically, the small portable electrocardiogram device (ECG) can be used as an example which its size is 5cm* 5cm. It is used to monitor heart activity and provide complete signals in 12 derivatives and are used to collect signals through ten sensors and fixed-position electrodes. It has ten input channels (V1-V6, VRA, VRL, VLL, VLA) in the 500 Hz sample with 10-bit analog resolution and convertible to (A / D) digital.

Tier2 includes a personal server application running on a personal digital assistant, such as a mobile phone, laptop, or a personal computer. A personal server performs some of the tasks such as a transparent interface to wwpan, user and Tier3 (medical server & Thin clint). Interface to wwpan includes network configuration and task management. The task of configuring networks, among other functions is supporting of registration device and sensor, determining the initial values, customizing, and setting up

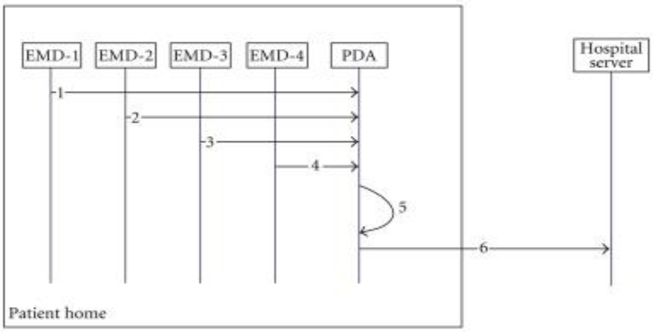

Figure (12) Transferring information to a medical server

Figure 13 shows an image of an MPEG-21 digital abstract item containing EMDs measurements.

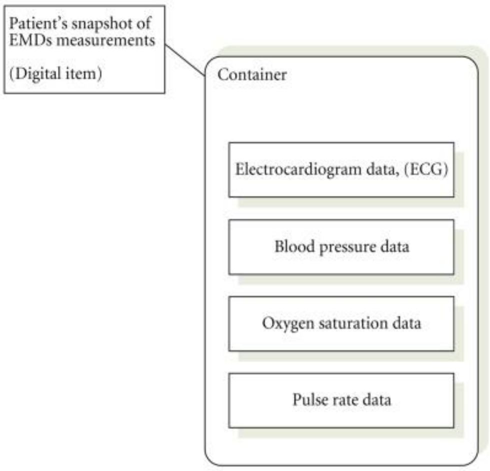

Figure 13. Image of an MPEG-21 digital abstract item

And in figure 14 you can see the schematic of the data in an ipmp container.

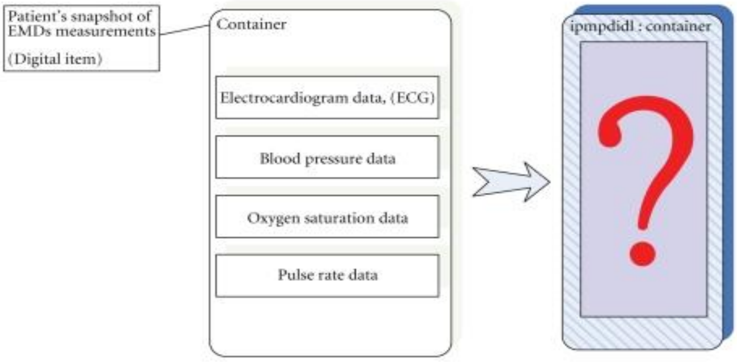

Figure (14) Schematic of the data in an ipmp container

file by identifying the number of patients is not protected and can be used to store the file in the database and some other information for the condition that the file was created in user’s pda. The other two items with MPEG-21 IPMP components are used by trained medical staff and physicians. Each of these items includes a license to use encrypted forms that gives the user access to the contents of the file. This license also contains the key to use patients' PDAs to encrypt medical data files. We assume that each patient and each physician and medically trained person has a set of public-specific keys (Fragopoulos 2009). This pair of keys is assigned by the main server in the hospital and can be canceled at any time because there is a continuous connection between the hospital server and the patient's server (home). Therefore, data usage license can be done by using public key encryption which is associated with the elements. In order to access the contents of protected items, the end user should decrypt with their private key, figure 15 illustrates a schematic view of MPEG-21 and the way that data files are transferred from the patient's home server to the hospital server.

In our view, the three groups should have the right to protected access to content

1. IT supervisors who are responsible for storing incoming files in databases

2. Medical personnel: such as: nurses

3.Physicians who are responsible for visiting the patients

Each of these groups should have different access rights to protected digital content. On the other hand, a nurse or trained medical staff should be able to see some details of the patient's information, for example part of the patient's personal data such as name, surname, and perhaps an initial diagnosis that may be made automatically after patient measurements at home. In order to inform the physician of the patient's condition, finally, the physician may have full access to the contents of the MPEG-21 packaged files, such as: patients' personal data, accurate measurements taken by EMDs, measurement time, and initial automatic diagnosis, so the production of the mpeg-21 container consists of three items (Kosch 2013). The first option, or the first item which contains the text of the data

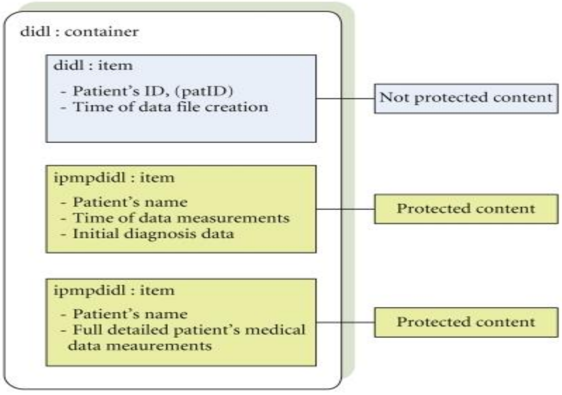

Figure (15) A schematic view of MPEG-21

2.1.4-Using RFID technology (fourth strategy)

RFID: or radio frequency identification device is one of the oldest and most widely used technologies. RFID automatically extracts data with its special tools and provides us with the appropriate data transfer tools at the expected time and place. RFID was used in July 2004 to identify patients in the hospital and give some staff access to patients' files (Tae Kim 2014). Since then, some US hospitals have begun implanting RFID systems in patients for better management.

Figure 16 shows RFID chips with RFID READER, which we will explain how it works in the next section.

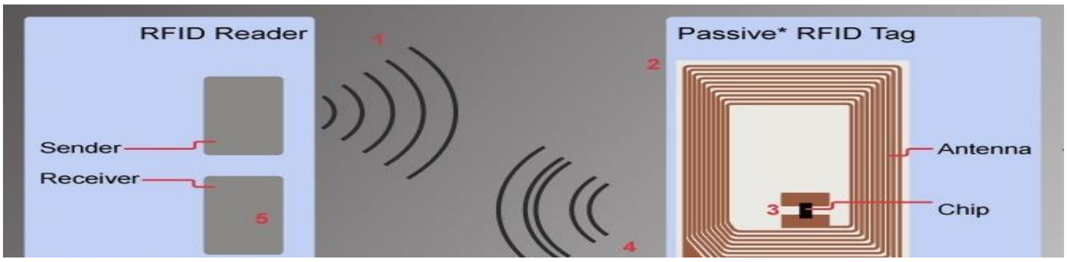

Figure (16) RFID chips with RFID READER

The method is that RFID technology, by identification through radio frequency, transmits data using the appropriate tools and by automatic devices or READERS, extracts information from a certain distance and provides us at the desired time and place. (Rahman Farzana 2017)

For many people, a radio frequency identification chip (RFID) is implanted. In this chip, patient information such as medical history and dose of medication (medical record) is read by a READER. When a doctor or a nurse who is in the emergency room and has a READER in pervasive healthcare. This method uses four factors for security.

1. Receiver and sender

2. Physiological agreement

3. Random Key session

4.The dynamic nature of the body

This method controls access to EPRs. The RBAC method creates security based on three factors

1.Role

2.The privileges of each role

3. Ability to create policies

- Compare the first and second strategies

1.The first strategy is a complex one that sometimes encodes commands between the sender and receiver, causing a lot of trouble for operations.

2.The first strategy is a symmetric encryption method and due to the decentralized structure of pervasive networks, there are no reliable centers for key management and authentication.

3. There are BRUTE FORCE attacks in the first strategy

4. The first strategy is a very complex method and most of the time its complexity is time consuming

5. The first strategy has many communication errors

- **The second strategy**

device (Wan 2013) reads a chip, receives a 16-digit word and can then access the information by visiting the site. It should be noted that the READER device should be located close to the chip to give the passcode to use the information. But in order to use this technology from far distances, we can turn the mobile phone into a READER device by installing application software on the mobile and this is better in terms of security for three reasons (Wan 2013).

1.Mobile software is activated with the frequency of the sender, who is a doctor or nurse

2.Even if malicious people get the 16-digit code, they don't access to the main site (database) of the hospital, it does not matter to them

3. This is an example of killing two birds with one stone, because both the current condition of the patient is measured by the sensor and the previous file can be accessed through the RFID chip.

Now we compare strategies with each other by referring to the positive and negative points

The first and second strategy: the first method or symmetric cryptography; although it is a method to maintain security in medical sensors, but it is still compared to other methods in the field of security

3.This framework is characterized by minimalism, which reduces the cost of health care, which is an important advantage over other strategies.

4.The architecture of this framework includes data measurement accuracy, which is more complete than other strategies because it supports all digital information.

5. Tracing and identifying information obtained from EMDs that is doubtful is possible through this framework and it is superior to other strategies in every way.

6. In this framework, in the protection of content by ipmp components and the core in this framework, full access control can be done, including quarantining information to its encryption or role-playing, so this framework has a wider evolutionary power than the other three strategies.

7. Utilizing resources by increasing the battery life of EMDs by minimizing power consumption is another feature of this framework. The framework includes a section called Intellectual Property Management and Protection (ipmp) that provides a mechanism for protecting digital items.

8. In line with MPEG-REL, this framework creates the language of rights expression for the user and creates a framework that enables all

1. This strategy has a list of privileges (ACL) which is a point in accessing information (Pijush Kanti 2019)

2. This strategy is based on the ability to reduce complexity and try to manage access

3 .Implementing all kinds of policies in this way is sometimes tedious like the first strategy

In general, the second strategy is a method with more positive steps than the first strategy, although the second strategy itself has many problems mentioned above.

- **The third strategy**

Security framework using MPEG-21 IPMP components of this framework is a secure multimedia framework. It is a new strategy that has certain advantages over other strategies. In the following, we mention some of its superior features compared to other strategies.

- Comparing the third strategy with the first and second strategies

1. Use a digital base that can include any kind of information in specific formats and support any kind of information while other strategies do not have this power.

2.The design of this framework is based on XML language, so it is easier to use it than other strategies and it is easier to create security tasks on it.

stage, it needs to be combined with another method that maintains access security against different people.

2. This strategy is far more secure than controlling access to information than solutions 1, 2, and 3, because all security is a 16-digit code that is used, so it should be combined with other methods to complete.

3.The question that arises about this method is, although it is possible to have medical records in databases, why we use this method along with measurement sensors.

4.The slowness of this strategy is one of its negative points. For example, if the mobile phone is far from the patient as a chip reader, this method does not work well.

In figure 17, you can see the percentage of desirability of each method from 100%, according to the positive and negative points of each in terms of security.

users to deliver a chain of rights and interests in digital content delivered in digital items.

9.This framework contains the element of ipmpdidl: contents. This element contains the contents of digital security which includes a set of protection tools (for example: cryptography, cryptography, hashing, digital signature) means that any method can be designed to control access in this framework.

10.The xml file in this strategy contains various items which all items contain some information that the user needs to identify the destination items, and it makes security in this method well maintained.

• Comparing the fourth strategy with the first, second and third strategies

1. Although this strategy has a simple structure, but its structure is more complex than the first strategy because in the 16-digit code access

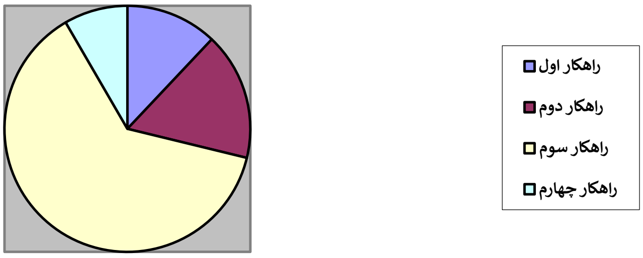

Figure (17) Percentage of desirability of methods

3. Conclusion

Comparison of security strategies in pervasive healthcare shows that the third strategy, or MPEG-21IPMP, is a more successful and popular strategy by maintaining a stable framework because it is based on XML and a special framework that is more difficult to penetrate. It exchanges information digitally in XML code. After that, the second strategy or controlling access to the EPR is successful, and then the first strategy. It should be noted that the first strategy is based on physiological agreement, so it is more complex than all other strategies. And finally, the fourth strategy or RFID is recommended. The future achievements can improve the situation of RFID strategy because it is developing and every year many researchers do different articles and theories about it.

References

[1] Tae Kim, Jung. (2014); "Authentication Process between RFID tag and Mobile Agent Under U-healthcare System", International Journal of Bio-Science and Bio-Technology, Volume 6, Pages 109-116

[2] Wan, Jiafu., Zou, Caifeng. ,…. (2013); "Cloud-Enabled Wireless Body Area Networks for Pervasive Healthcare", IEEE Network, Pages 1-7

[3] Fragopoulos, Anastasios., Gillis, John. Serpanos, Dimitrios. (2009);" Security Framework for Pervasive Healthcare Architectures Utilizing MPEG-21 IPMP Components", International Journal of Telemedicine and Applications, Volume 2009, Pages 1- 9

[4] Haque, Munirul., Iqbal Ahamed, Sheikh. (2006);" Security in Pervasive Computing: Current Status and Open Issues", International Journal of Network Security, Volume3, Pages 203- 214

[5] Venkatasubramanian, Krishna K., Gupta, Sandeep. (2006);" Security for Pervasive Health Monitoring Sensor Applications" Intelligent Sensing and Information Processing, Volume4, Pages 197-202

[6] Acharya, Debargh. (2010);" Security in Pervasive Health Care Networks: Current R&D and Future Challenges", Eleventh International Conference on Mobile Data Management, Volume11, Pages 305-306

[7] Kosch, Harald. (2013);" Distributed Multimedia Database Technologies Supported by MPEG-7 and MPEG- 21", GoogleBooks, Pages 1- 280

[8] Anagnostopoulos, Christos., Hadjiefthymiades, Stathes. (2014);" Autoregressive energy-efficient

context forwarding in wireless sensor networks for pervasive healthcare systems",Volume 18, Pages 101- 114

[9] Kumar, Pardeep., Jae Lee, Hoon. (2012);" Security Issues in Healthcare Applications Using Wireless

Medical Sensor Networks: A Survey, www.mdpi.org/sensors, Pages 55-91

[10] Rahman Farzana, Alam Bhuiyan.md, Iqbal Ahamed Sheikh. (2017) "A privacy preserving framework for RFID based healthcare systems "Future Generation Computer Systems, Volume 72, July 2017, Pages 339-352

[11] Pijush Kanti, DuttaPramanik, AnandNayyar (2019) "Chapter 14 - Security and Privacy in Remote Healthcare: Issues, Solutions, and Standards" Telemedicine Technologies, Pages 201-225

[12] Mohamed Almorsy, John Grundy, Ingo Müller(2016) "An Analysis of the Cloud Computing Security Problem", Published in in Proceedings of the APSEC 2010 Cloud Workshop, 6 pages