Data Privacy and Security for IoMWT (Internet of Medical Wearable Things) Cloud

Raluca Maria Aileni, George Suciu, Maheswar Rajagopal, Sever Pasca, and Carlos Alberto Valderrama Sukuyama

1 Introduction

The latest technology developments have produced a sudden release of intelligent and deeply associated computing devices that are in a Small Form Factor (SFF). Communication devices interact with people these days, in different domains, such as lifestyle, well-being, and entertainment [1]. Scaling down the hardware equipment carries out a crucial role in this improvement; the Internet was a less known part [1, 2]. The Internet performed by far the most critical role in the ascension of the technology, and it is fundamental because of the transformation it has gone through since the 1990s. During the time, the Internet was utilized mainly only for correspondence purposes, such as emails. Nonetheless, it has been observed an evolution during the years, when in the 2000s, the mobile phone was the revolution in the field of wireless technologies [2]. Nowadays, there are many numbers of customers associated with the Internet lead to the Internet

R. M. Aileni (✉) · S. Pasca
Politehnica University of Bucharest, Faculty of Electronics, Telecommunication and Information Technology, Bucharest, Romania

G. Suciu
Politehnica University of Bucharest, Faculty of Electronics, Telecommunication and Information Technology, Bucharest, Romania

Beia Consult International, Bucharest, Romania

M. Rajagopal
Sri Krishna College of Technology, Coimbatore, India

C. A. Valderrama Sukuyama
Mons University, Faculty of Engineering, Department of Electronics and Microelectronics, Mons, Belgium

N. Gupta, S. Paiva (eds.), *IoT and ICT for Healthcare Applications*, EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-030-42934-8_11

of Things (IoT). IoT comprises several items, for example, robots, sensors, and actuators to the Internet [2]. When these kinds of items, usually called wearable devices, are attached to humans' body, it can be monitored individual's health parameters and safety. Considering suitable specifications, IoT can be defined as a system of physical objects supported by sensors and introduced innovations for data communication that supplies interchange with the environment [3]. Wearable devices have the advantage that they can be worn without any difficulty and can monitor a person's physical activity easy [3, 4]. Such wearable devices, tri-axial accelerometers, magnetometers, altimeters, and gyroscopes shape an automatic virtual environment [3, 5].

Many essential benefits are encouraging healthcare organizations to embrace a connected future. Primary among them is the possibility to enhance patient outcomes when data are shared in real time. The IoT permits healthcare specialists to extract data from medical devices, mobile apps, and chips inserted in our bodies to help diagnose patient's health more quickly [6].

Wearable devices and Medical IoT Interoperability & Intelligence, empowered by the Internet of Medical Things (IoMT), is a fast-growing field. Numerous patients are wearing IoMT devices—from connected health and wellness devices to connected insulin pumps and embedded pacemakers. Leaders in the department estimate that a large number of health organizations—up to 87%—plan to utilize the Internet of Things (IoT) technology by 2019 [7].

Wearable devices and tracking devices have grown as part of standard healthcare methods, intertwined with an evolving healthcare transmission model. According to recent studies, the wearable technology market is assumed to rise from $20 billion in 2015 to $70 billion in 2025. Medical devices are implemented with Wi-Fi or Near-field communication technology in order to allow machine-to-machine (M2M) communication that is the base of IoMT [8].

Generally, the IoMWT construction relies on three layers: the perception layer, the network layer, and the application layer, as shown in Fig. 1. The primary responsibility of the perception layer is to gather healthcare data with a type of devices. The network layer is composed of the wired and wireless system and middleware and performs processing and transmission of the input collected by the perception layer. Well-designed transport protocols should improve transmission efficiency, reduce the energy consumption, and ensure the security and privacy [9].

This book chapter, structured on seven chapters, presents several aspects concerning sensitive data management, cloud security and patients' data anonymization using ARX application.

In this chapter, we present aspects concerning massive medical data processing (e.g., data collected using the electroencephalograph (EEG) for patients suffering with epilepsy, Parkinson, or Alzheimer) using Hadoop, health predictive modeling of the massive data, and an edge computing solution for patient data anonymization. Our proposed solutions for security and privacy in medical area address the security aspects on different levels of account type and data anonymization by differential privacy model using ARX application and simulating several reidentification attacks

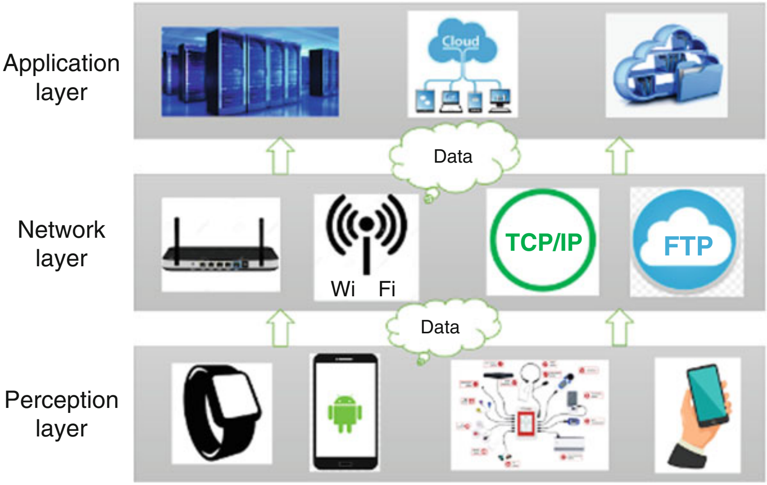


Fig. 1 Structure of medical internet of things

(persecutor, journalist, and marketer attack) analysis in order to provide the risks of data reidentification.

An essential application sector of the IoT is the healthcare sector. The IoT has acted a vital role in this area by intensifying service quality while decreasing costs. It is understandable to track health parameters, such as blood pressure, blood glucose, body temperature, and many more in real time by using wireless sensors. The evolution of sensors, better data processing technologies, and advanced technologies for wireless communication has driven to the expanding implementation of the IoT in the healthcare sector. The development of WBSNs (Wearable Body Sensor Networks) to frequently monitor patients' movements is an added milestone for the implementation of the IoT. Medical devices have endured severe changes, from the conventional unconnected devices to wireless modified devices. These improvements comprise the evolution of medical IoT systems that connect to cell phones. The medical IoT is a system involving mainly of health-monitoring devices. A back-end system remotely reads Patients' health parameters and eventually, investigates the collected data and presents suitable feedback to the clinical team [10, 11].

The medical technology business designs and manufactures a broad range of medical products that aid to diagnose, monitor, and treat diseases and health conditions.

The advancement of the IoMT is being serviced by an increase in the quantity of connected medical devices that can generate, collect, analyze, or transmit health data or images and connect to the healthcare provider networks, carrying data to either a cloud repository or internal servers [12].

2 Medical Wearable IoT Devices: Architecture, Evolution, and Methods in Remote Monitoring

In addition to the advancement in wearables for the wrist and eyewear, smart clothing ambitions are also on the rise. NanoSonic, Textronics (which manufactures NuMetrex), Weartech (GOW Trainer), and Sensoria are driving the application of those developing IoT in textiles. Specific items such as shirts can directly measure a person's temperature and heartbeat; therefore, socks can provide impact measurement [13].

2.1 Wearable Devices

Several research activities specific to the healthcare applicability domain currently performed worldwide have as primary interest sensor devices. Many projects were developing, and there are other projects already existing on the market. Several current projects have focused on wearable health devices [14]. The goal of this book chapter is to set the optimal safety for using wearable biosensors for patients according to the condition and physical state monitoring. The goal in IoMWT is to minimize the security risks by using the adequate methodology for working with personal sensitive data, anonymization, and data analytics in the cloud. The anonymization of the patients' data is crucial because it allows the legal use of data for predictive modeling, the study of the evolution of the disease, and correlations between the various symptoms.

The following are the most impressive indoor/outdoor health monitoring applications that operate on real-time and non-real-time modes.

(a) Health Gear – represents a wearable real-time system produced by Microsoft Research; it monitors and analyzes physiological signal from the sensors connected by Bluetooth to a mobile phone [15].

(b) MobiHealth – health project funded by the European Commission; enables patients to perform any kind of physical activity while continuously monitoring humans' parameters using UMTS and GPRS networks [16].

(c) Ubimon – developed by the Department of Computing from the Imperial College London, Ubimon has the purpose to identify, show, and express the most important problems when talking about the usage of wearable and implantable sensors for shared mobile monitoring [17].

(d) CodeBlue – represents a research working program developed by Harvard University, USA, and incorporates sensor node and wireless devices into a disaster response setting. It can work with a large number of wireless devices [18].

(e) eWatch – a wearable sensor device that makes available a platform for context-aware computing research. eWatch is developed as a wristwatch and has

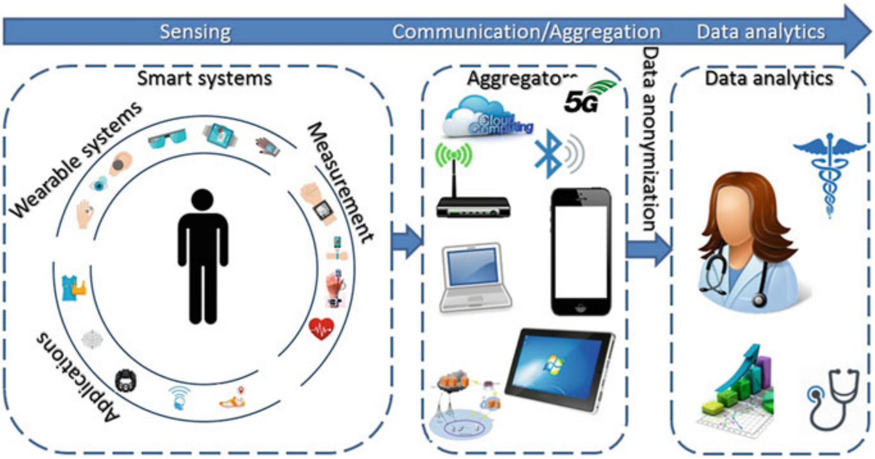


Fig. 2 Wearable internet of things application

different features: notifies when it is recorded light, motion, sound, abnormal temperatures, etc., and it is easy to use and view all the information [19].

(f) The vital jacket is based on mobile computing device that allow heart rate monitoring and can be used for medical monitoring, high performance sport and fitness application that transmit data via Bluetooth to PDA and store it in a memory card in a split second [20].

Figure 2 shows the phenomena of the transition of information from the patient to physicians.

The embedded sensors for a medical purpose will allow remote measurement for blood pressure, temperature, skin moisture, glycemia, or stress and will include actuators to turn on and off devices or adjust in real time. Patient vital sign data could be monitored for predictive analytics. Figure 3 describes the entire case scenario, why do we need to advance technologically in the field of medicine, when aged patients are suffering from diseases and medical care center are not enough as required. IoT wearable devices can monitor the patients 24/7 at home, and in case of an emergency, alerts are sent to the caretakers, as well as to the medical department to take the measures as it is described in Fig. 3. Readings are gathered through the biomedical sensors and sent to the wearable autonomous devices for monitoring, which generates the alerts according to the situation.

The process of using data is to filter the information in the private cloud and to anonymize data analyses in public cloud [20]. This process would help in keeping the privacy of the patient secure and authentic. The solution proposed in this chapter will use different security levels for different types of accounts (medical staff and patients) in order to provide security and privacy [21]. The second purpose of

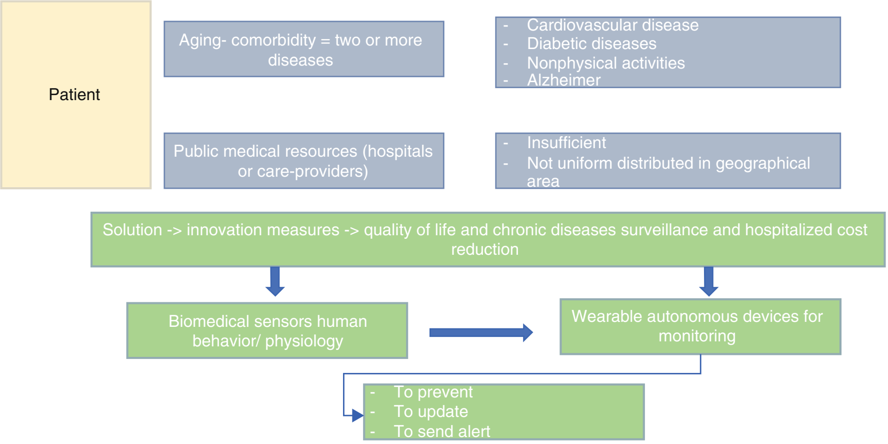

Patient
Aging- comorbidity = two or more diseases
- Cardiovascular disease
- Diabetic diseases
- Nonphysical activities
- Alzheimer
Public medical resources (hospitals or care-providers)
- Insufficient
- Not uniform distributed in geographical area
Solution -> innovation measures -> quality of life and chronic diseases surveillance and hospitalized cost reduction
Biomedical sensors human behavior/ physiology
Wearable autonomous devices for monitoring
- To prevent
- To update
- To send alert

Fig. 3 Information privacy for medical records

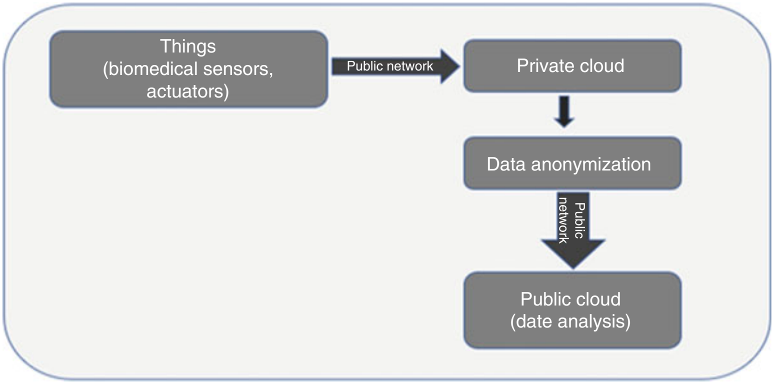


Fig. 4 Medical monitoring

this solution is to perform predictive analyses modeling for a better understanding and anticipation of patients' possible diseases or preventive actions. This is the reason for the need for anonymization of the patients' data performed in a cloud environment. Figure 4 illustrates the data privacy of the patient's data, as seen below.

For the process of anonymization [22, 23], several techniques can be used, such as the following:

- Kasking – protect X data by converting it in Y data (non-perturbative masking methods, perturbative masking methods, and synthetic data generation).
- Synthetic data – represented by protected data X, which consists of randomly generated records that do not directly derive from the records in Y (fully synthetic data; partially synthetic data, and hybrid data).

In this case, we choose to use the non-perturbative masking method and synthetic data method with partially artificial and hybrid data types. The steps for generating synthetic data are as follows:

- Set the model for the population
- Adjust the model to the original data set X
- Generate the synthetic data Y from the model

The challenges for IoT security for healthcare ecosystem, at the physical and logical level, are cryptographic algorithms development, authentication protocols, access control, and privacy.

3 Internet of Wearable Medical Things (IoMWT): Security Risks and Vulnerabilities

The massive amount of information that IoT and wearable technologies can gather, the privacy and security-related concerns become more and more critical as the number of these devices increases rapidly [24]. Users benefit from the personalization and customization that IoT and wearable technologies provide, yet those same capabilities have significant demand and exacerbate digital privacy and data security risks that are already in the market, taken in the category of traditional online services and technologies [25]. These privacy and security-related concerns can be observed in order to gain:

- Access to the device itself (i.e., if it is lost or stolen, makes a different kind of scenario)
- Access to the information that a device shares with nearby devices or systems (i.e., data transferred over Wi-Fi or other wireless networks)
- Access to data transmitted to the cloud or any remote storage system [26].

3.1 Related Work in Security and Privacy

A matter concerning security and privacy has been under discussion and hot topic of the modern era. There have been numerous authors [27] who illustrated the problems regarding the eHealth sector. The authors in [28] have taken into account some of the difficulties found in the private health sector for monitoring applications. This study assesses the security breaches for sensor network applications in wearable medical devices. The sensor devices must be foolproof since they are being used by nonexpert patients in case of medical application. The setup and control process of the data security mechanisms are node related, and they involve a little and intuitive human interaction. For the rest of the applications, to bootstrap initial secure communication between all the nodes in a BAN for secure data communication, device pairing techniques are approved, which is not easy for utilization. If we ignore the manual steps for usability increment, then it will sacrifice security [29, 30]. From all the above mentioned, the main conclusion is that between security issues and privacy issues, the first ones are the most important and most analyzed.

3.2 Security Risks and Vulnerabilities

Security represents one of the most significant aspects, which, in general terms, is seen as a concept for defining safety. According to the site of the US Department of Commerce [29], cautions against security breaches that might influence the personal data of wearable medical devices have to be taken care of. Healthcare systems mostly use sensor networks that face many downfalls in terms of security threats and cyberattacks. These can cause severe problems in the social life of people wearing wireless sensors devices because the gathered data can be utilized to harm the individual. As part of the active research, security issues regarding sensor networks, for example, eavesdropping on medical data, modification of medical data, forging of alarms on medical data, denial of service, and location tracking of users [31, 32]. Similarly, many people have specifically addressed security issues concerning healthcare applications [33]. In the following section, we will highlight and discuss some threats, attacks, and possible countermeasures.

Security breaches in healthcare applications within end devices networks are a significant concern which must be addressed. Applications in the healthcare sector based on sensor networks have a similarity to WSN application environments. Security problems can be categorized into two primary levels, one of them being the system security and the other one the information security. Threats and attacks [30] are divided into two major sections: active and passive. Passive attacks can take place during the routing phase of the data packages in a system. The hackers have the possibility to change the route of the packets or can cause the transmission to be unpredictable. The hackers can cheat medical data by snooping to the wireless network. Current attacks are more dangerous than passive ones. Attacks may find the location of the user by eavesdropping, which may lead to life-threatening scenarios [34]. The prevailing trend of sensor device designs is that they have little external security characteristics and hence are prone to physical tampering. This aspect enhances the vulnerability of the devices and implies difficult security challenges. Likewise, essential data transmission from WBAN networks through GPRS or any other similar network systems can also be stolen using eavesdropping.

Attacks in health monitoring are in detailed manners regarding the eavesdropping and modification of medical data, falsification of alarms on medical data, DoS (denial of service), location and users' activity tracking, physical tampering with devices, and jamming attacks. People with malicious purpose may use stolen information to conduct harmful activities. Attacks, which can take place in healthcare systems, performed using WSN are presented in Table 1.

Table 1 The security risk to WBAN and corresponding security requirements

Attack assumption	The risk to WBAN	Security requirements
Computation capabilities	Data modificationImplementation	Data integrityAuthentication
Listening capabilities	Eavesdropping	Encryption
Broadcast capabilities	Replaying	Freshness protection

1. Modification in medical data—when attackers can alter the personal medical data during the gathering, transmission, or storing of it, it can result in corrupted medical records of the patients. This can lead to fake alerts, e.g., resulting in futile rescue missions. Or in a worse case, the false negatives (i.e., changing alerting data into natural result) can disguise real alerts or emergencies. The hackers have the possibility of deleting or replacing a section of eavesdropped information or the complete data that were spoofed and can send the alerting data back to the original receiver for malicious purposes. Medical data are essential, and the modifications brought to it may lead to hazardous resulting, taking into account the well-being of a patient or a healthy person even.
2. Impersonation attack—If a hacker spies on the identity of any wireless sensor node can tamper the other nodes.
3. Eavesdropping—Regarding the open characteristics used by the sensor networks of the wireless channel, any enemy may capture radio transmissions among wireless nodes without any effort. Stolen information can be utilized for mischievous activities.
4. Replaying—A piece of the accessible data can be eavesdropped and resent to the first receiver to accomplish a similar reason in an alternate case.
5. Threats and attacker can be categorized in internal or external. Because of the fact that external attackers are not part of the system, their malicious intentions cannot be prevented. Because external attackers are not part of the system, their harmful activities cannot be stopped. The primary intention of these attacks is to abduct sensitive personal data. For the reason that wireless connections are more vulnerable than wired connections, the attackers can find them more comfortable. When they know the personal health data value, they may try to steal it by using both internal and external attacks.
6. Eavesdropping on medical data—during the gathering, transmission, and storing processes of the medical data, the attacker can take advantage and attempt to access that information illegally. An example is represented by unapproved spying radio transmissions between nodes. Medical data are highly sensitive to abuses and require to be protected against eventual attacks.
7. Forging of alarms on medical data—Attackers can generate fake messages instead of modifying the regular ones. This action performed by the attackers can lead to inaccurate data records or false system reactions.
8. Tracking users' location—A PEMS (Portable Emissions Measurements System) system user permits a constant track of the messages that are sent, and since the

system supports the localization of people, data can be obtained, reunited, and analyzed to result precise location profiles.

9. Tracking users' activity—This is a very common attack when it comes to eHealth systems. Considering the data records, patients' activities can be analyzed. For example, we can identify how much time a person spends during workouts and monitor the heart rate, oxygen saturation, etc.

4 Edge IoT Software- and Hardware-Level Security

IoT edge computing offers the possibility of gathering computational and analytics capabilities that are connected to the concept of data generation. IoT deployments became secure since some processes will occur in a specific location. Even though the IoT systems are based on different types of architectures, collaboration and edge intelligence are two characteristics that are common to all of them. One essential thing about this technology is that it uses the advantages of the fact that IoT devices are interconnected and of the gateways that will ensure data processing and device management.

IoT edge computing provides a particularly extensive protocol that will maintain data ingestion. Nowadays, enterprises need a platform that will be used to collect machine data and display them to other IoT systems. Moreover, there are a couple of accepted standards regarding enterprise applications that will be used. IoT platforms must support several devices that follow specific data ingestion protocols. The platform must be modular, and it should allow new forms of communication. Finally, several functionalities such as encryption or data protection will be provided to ensure essential security operations.

Moreover, IoT edge computing must provide the ability to work offline as this measurement will reduce the costs and will offer higher performance; currently, most companies will work with a large amount of data. First, this type of system must establish a secure connection between the cloud and the edge. An engine that will process the information gathered and analyzed by different learning tools that will allow the possibility of sending alerts in case of problems. Furthermore, the IoT edge platform must enhance operational processes that already exist. This facility will ensure that people have access to all types of data in real time.

When choosing the optimum IoT platform, each need must be taken into consideration. When building an application, its progress is strictly monitored. Although edge computing is still developing in terms of facilities, selecting the best IoT platform is something that needs to be considered in the long run as current and future needs are essential.

The hardware architecture of these systems needs to support deployments at multiple scales. Therefore, many gateways are used within the IoT platforms. Usually, ARM, x86, and MIPS are used along with containerization technologies that will facilitate the implementation of the same set of functionalities within the same IoT hardware without the need of making any further changes. It lowers the costs, and it reduces the number of employees hired to maintain different versions of production hardware and software. Frequently, platforms that can exchange resources with cloud are preferred, as they will anticipate unexpected requests coming from applications [35].

When talking about hardware layer in the context of edge computing, security needs to be taken into consideration while making the design of the device. Cryptographic keys are integrated within the chips and can be used to authenticate the user. However, this kind of system is still vulnerable as the keys are shared on a universal bus but can be solved if the keys are stocked at a different level and not through sharing keys.

For the communication layer, edge gateways are needed to ensure security by encrypting the data. If the network has a low bandwidth, MQTT (Messaging Queuing Telemetry Transport) can also be used. As for the cloud part, sensitive data need to be moved to the cloud. Furthermore, certificates will help within the authentication process. Moreover, the update devices need to be updated remotely so that attacks will be avoided [36].

There are a couple of IoT attacks that were taken into consideration in the last couple of years. The first category is related to the OSI (Open Systems Interconnection) physical layer that requires unauthorized access to physical systems. There is another category of attacks related to the software part, which includes viruses. DDoS (distributed denial of service) are can also be included in this section, although they can appear at lower levels within the OSI Model. The risk related to this section is that some warning might not be noticed.

Network attacks can also occur, and they represent one major vulnerability of IoT devices due to their wireless connectivity. A cryptanalysis attack occurs when someone tries to recover a message without having an encryption key. This situation also includes the case when the hacker tries all the possible combination for a password. The side-channel attack is related to the encryption that was used to gain access to the information [37].

5 Data Security in Private, Public, and Hybrid Cloud

Cloud's most significant advantage is that it makes the information more accessible when an Internet connection is available. However, there are many.

The public cloud is a free service such as Office 365, Dropbox, and Google apps that can be accessed via the web. On the other hand, the private cloud provides the same function but uses a firewall that will block the access of any unknown users. While giving this type of service, some problems such as the loss of resources or the vulnerability of the information might arise [38].

However, there are still some advantages regarding the use of a public cloud such as the inability of locating the exact information, the lack of hardware failures, and the use of degrees of physical security. On the other hand, the public cloud allows access to be granted from every location. Also, international issues might become a critical problem and can lead to criminal misconduct.

The private cloud aims to grant access to physical servers and to keep the information secured by a firewall. Moreover, the design of the architecture can be changed according to user's preferences, and this allows the data infrastructure to be isolated. Still, it can be an essential disadvantage if users have access to physical access. In addition, the owner is responsible for the security of the cloud [39]. A private cloud offers precise control over the security parameters, as all the measurements are taken inside the system and redistributed to the security provider [40]. Therefore, private cloud implementations provide multiple security advantages, although it still requires maximum attention from the organizations that will use it [41].

On the market, there is a third option called a hybrid cloud. This offers a mixture between the best elements of both public and private cloud. It gives the possibility of moving between the two of them, providing more flexibility and multiple options regarding the deployment of the data. It is essential to have a cloud team that will plan and organize the entire cloud strategy as they should decide whether an application should be moved to the cloud or not and keep track of the policies and costs. It is essential to have fluency during the process of handling data, as the speed is an essential key within this type of service [42].

Hybrid cloud has a couple of requirements such as the presence of public infrastructures like Microsoft Azure or a WAN (wide area network) established between the public and the private cloud. To use a hybrid cloud, servers, a LAN network (local area network), and a load balancer must be implemented. A private cloud software layer can be installed to create the virtualization layer or a hypervisor that will be used to sustain VMs (virtual machines) or containers.

The maximum interoperability between API (application programming interfaces) and services must be ensured. Therefore, cloud layers that are compatible with the targeted public cloud must be selected. Hybrid clouds will allow the enterprise to implement a local private cloud that contains critical data and resources [43].

6 Personal Data Management and Anonymization in the Cloud

The start of the last decade manifested that the speed and the volume of data generated are surpassing the current memory of institutions' data management [44]. Cloud-based data management is, indeed, stimulating to recognize the potential of large-scale data management solutions by providing adequate scaling of resources. In a cloud-based data management situation, institutions or organizations pay storage and computing power to execute the data management applications to work preferably. Data management is one of the most significant research domains in cloud computing. Many cloud-based data management systems are in service now, such as Bigtable in Google, Cassandra, and Hive in Facebook, HBase in Stream, PNUTS in Yahoo!, and several other systems. Cloud computing has grown into significant influence on data management research and performs as a critical role [45].

The Registration and Unique Identifier generation module is necessary for creating a PHR (Patient Health Record) tool. The module is used to provide information for all patients with a unique ID value. All hospital employees can fetch the data of the patient by using only the ID from the database. Additionally, this module can reduce consumption. To maintain or create one patient medical record, every hospital needs to have a unique identifier value for the patient in an organization. For generating an ID value for each user, the Md5 hash algorithm is used. That takes a password as input and 32-bit id as an output. MongoDB application preparation is used to store patients' records. Every data, along with this metadata, are to be stored in a single place; it will simplify the access time of data and minimize the use of joining the robust modules [46].

MD5 hash algorithm presents a processing 512-bit block as input and produces a 128-bit (16 bytes) blocks, often expressed as a 32-digit hexadecimal value. After getting all the medical records from the patients, it is needed to store in an encrypted format both rest and the transformation. All patients' sensitive medical information is changed into critical values by using an Md5 hash algorithm only for the limit. After hashing, the encrypted data are separately stored on a different cluster. Transferred medical records of the patients are encrypted, so whenever we want to transfer medical records for patient's treatment, we need to decrypt records in the opposite side. Hadoop MapReduce algorithm for anonymizing data is used to help to deal with the massive amount of the daily updatable patient's records. Hadoop MapReduce has several components, such as HDFS and MapReduce (Fig. 5). *HDFS (Hadoop Distributed File System)* was entirely used for data storage and contained the data node and the name of the node. MapReduce is used for operating by Mapper and Reducer [46].

Several records of the human body electrical activity produced by heart, brain, or muscles can be used in medical diagnosis.

These records must be anonymized when are used for statistics in order to protect the sensitive data of the patients.

- In case of medical bioheat transfer, MapReduce can be used to process data and to select only the appropriate data based on the default limits (by Reducer – Fig. 6):
- Set the temperature limits [47]:

```
INSERT INTO TABLE temperature
Select
*,
high_limit_temperature-actual_temperatureas
critical_temperature,
IF ((high_limit_temperature-actual_temperature)>1.2, 'Low',
IF ((actual_temperature-high_limit_temperature)>1, 'High'))
AS temperature_limit
```

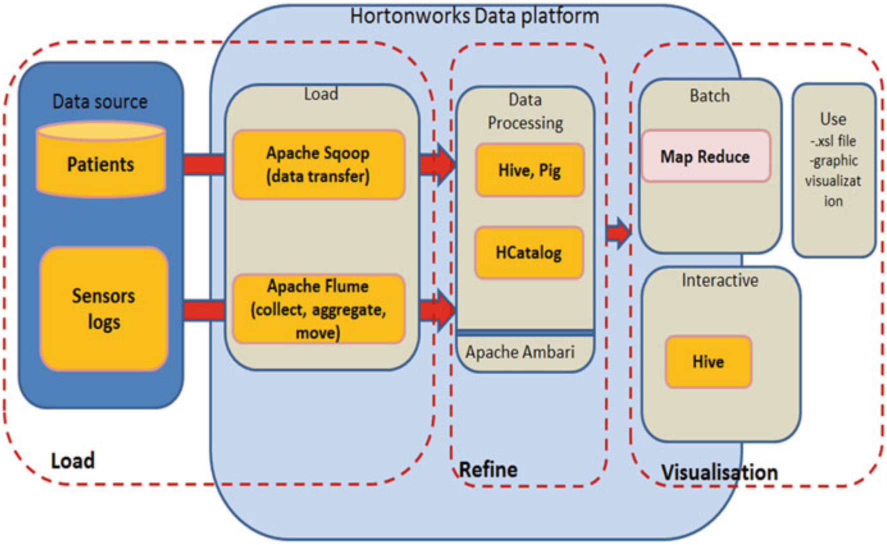


Fig. 5 Big data predictive analytics for bioheat transfer modeling [46, 47]

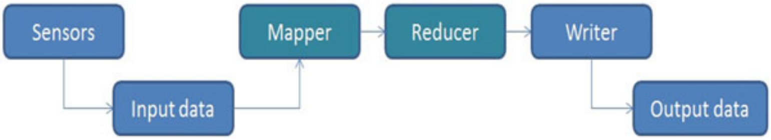


Fig. 6 Data processing by MapReduce [46, 47]

```
IF ((high_limit_temperature-actual_temperature)<1.2, 'Normal'
IF ((high_limit_temperature-actual_temperature)<1, 'Normal'))
AS temperature_normal from temperature_data;
```

- In case of the diagnosis or disease evolution studies that involve patients with epilepsy, Parkinson, or Alzheimer, the edge computing solution is necessary in order to process the massive volume of data collected by EEG (Figs. 7 and 8).

The EEG method based on electrodes is used for study neurological disorders such as the following:

- *Epilepsy* represents a chronic disease of the brain, demonstrated by the crises convulsive partial (focal lengths) or preferences, due to spontaneous electrical discharges that occur at the level of the brain.
- *Parkinson* represents a progressive neurological illness characterized by such trembling of the extremities, hardness of the muscles).
- *Alzheimer* involves progressive nerve degeneration due to the reduction of the number of neurons, brain atrophy, and the presence of the "caterpillar" plates, indicating the loss of memory and disorientation in time and space.

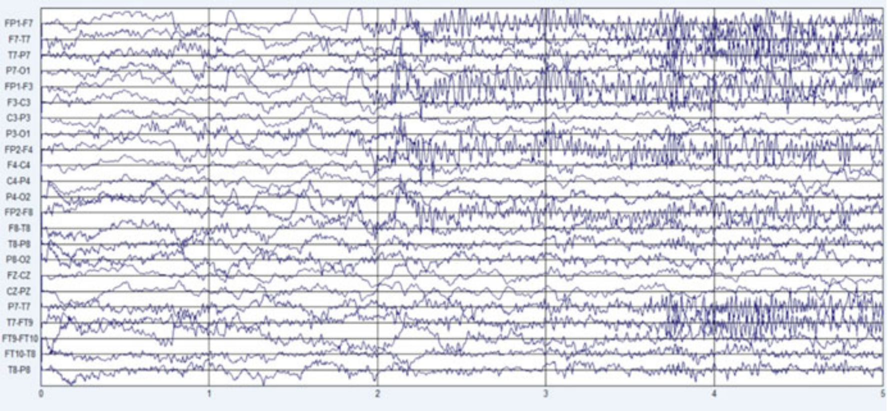


Fig. 7 EEG-23 channels, patient with epilepsy [48]

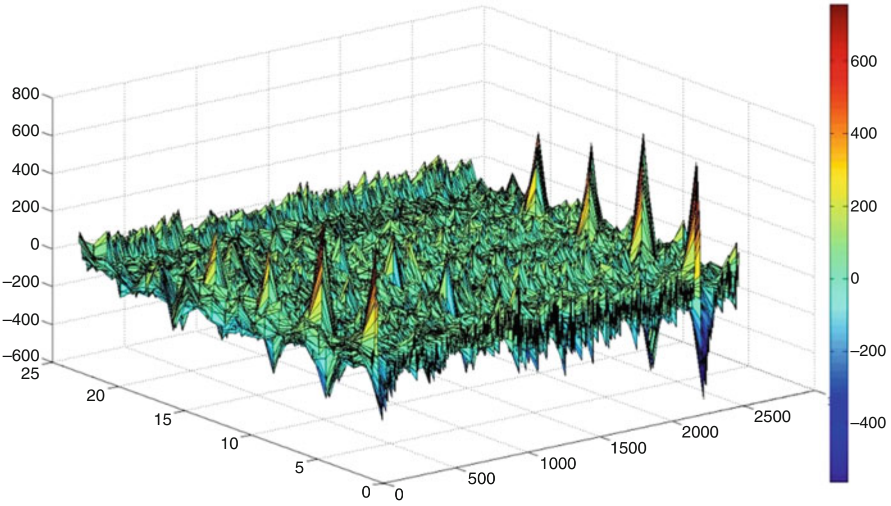


Fig. 8 EEG-3D view seizure, patient with epilepsy [48]

In an analysis of the EEG signals, we used discrete wavelet transform (DWT) and complementary filters in order to obtain the doubling of the data (Figs. 9 and 10) and reduction of the samples [48].

$$s = a_{12} + \sum\nolimits_{i=1}^{12} d_i \tag{1}$$

The proposed solution for wearable EEG and data analysis, in correlation with other body parameters such as ECG, PPG, temperature, and skin moisture, is presented in Fig. 11.

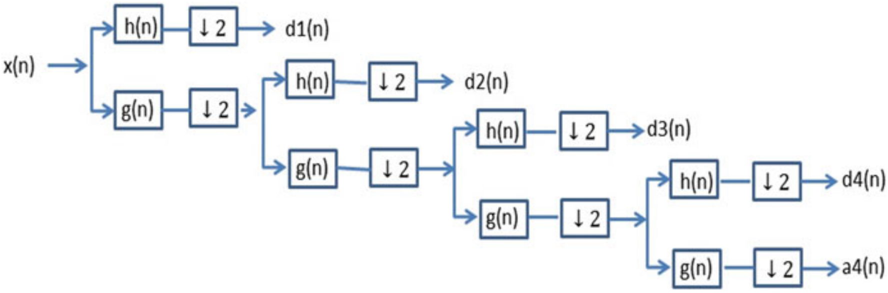


Fig. 9 Signal decomposition in details and approximations [48]

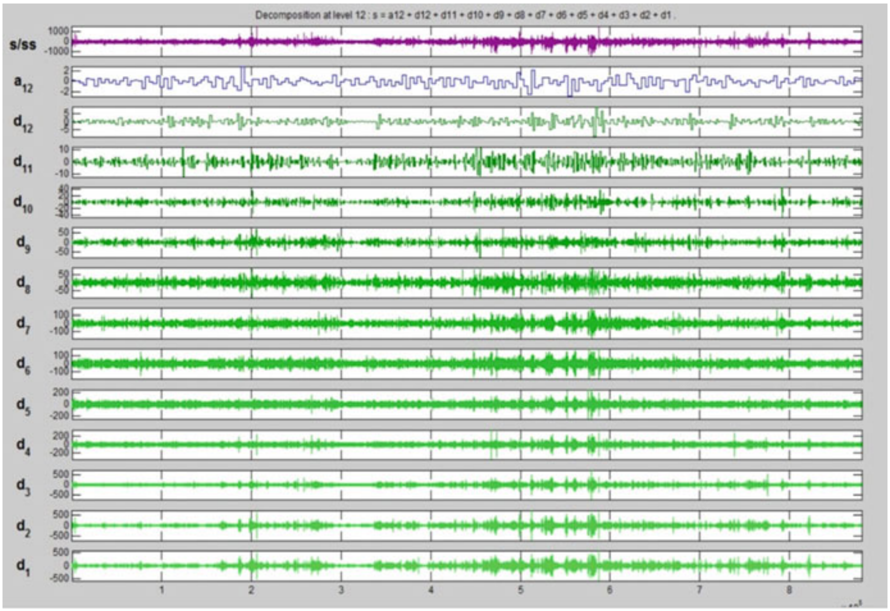


Fig. 10 Wavelet decomposition on 12 levels (1) [48]

The applications dedicated for data anonymization are open-source (ARX, Amnezia, μ-ARGUS, sdcMicro) or professional anonymization software (Aircloak Insights) GDPR-compliant. The Aircloak Insights application allows instant data anonymization, control, and the right balance between costs and efficiency. Also, this application can be created as a data-based business model by using anonymized data.

The anonymized patient records are generated by using the technique of generalizing and specification. In this technique, the critical attribute of quasi domains value is changed into a more general form. For example, if the native patient residency is Chennai, after the anonymization algorithm, the output will be India.

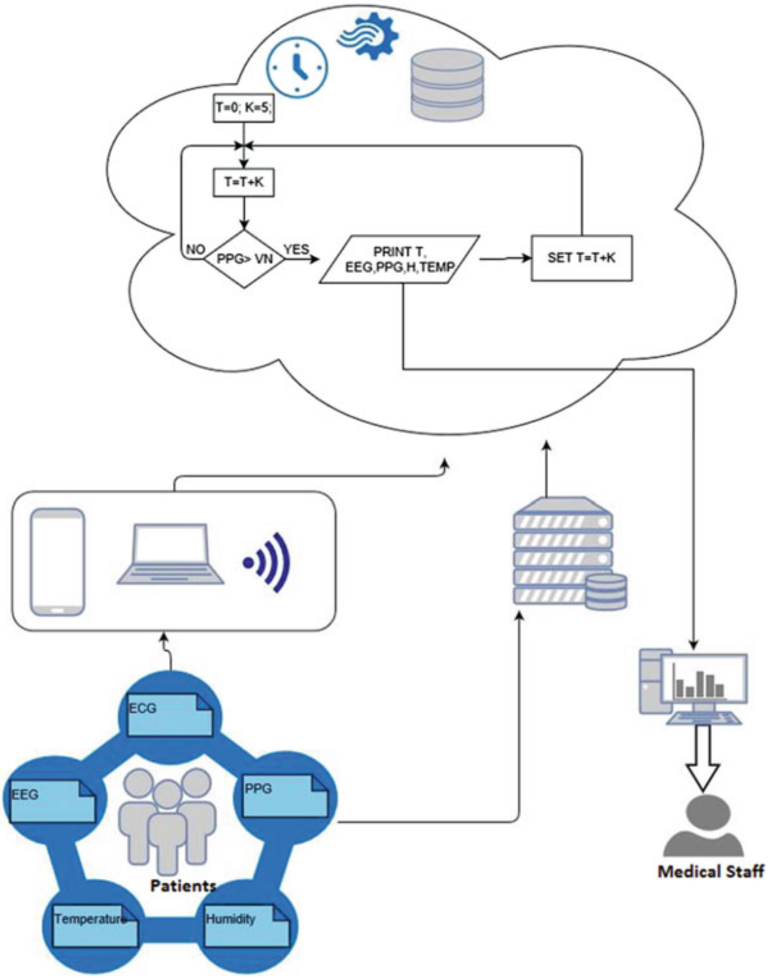


Fig. 11 WearEEG apps – block diagram [48]

This technique hides the values by symbols (for example, if the PIN code number has six digits, changing values of the number into symbols will be done only for the last three digits. By using a novel AAPM (Authorized Accessible Privacy Model), only the authorized personnel will be able to view and edit the patient's records. The authorized person has full rights over the data. The indirectly authorized person has only rights to insert data rather than edit or view.

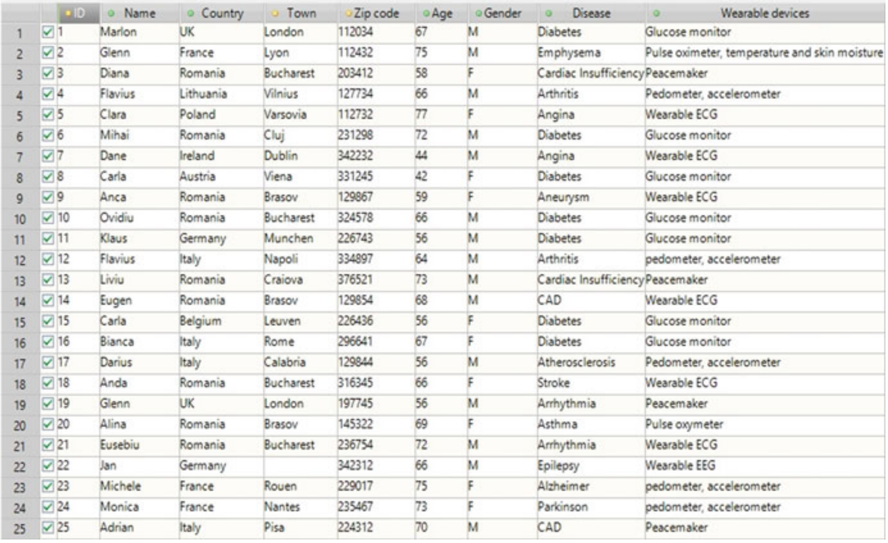
Anonymization is the best way to provide privacy over the microdata, which is released by the data publisher. Most of the existing systems are using several anonymization algorithms. A large number of top-down specification and bottom-up generalization techniques are developed separately for many organizations. Security and privacy over the patient's sensitive information must be provided. Specific attributes are also available in the data sets. For categorical attributes, the hybrid anonymization algorithm is used and includes both TDS (Top-Down Specialization) and BUG (bottom-up generalization).

The term [49] anonymization in cloud computing refers to anonymizing data while hiding any data which is public or sensitive to the original data. Data anonymization is widely used for securing sensitive data, and the techniques used in this field are focused on the public cloud. Mainly speaking, this feature enables the preservation of data to be private while just exposing a few critical data.

One of the algorithms used in anonymization is the k-Anonymity, an algorithm used for making each record alike from k-1 records. K-anonymity has three attributes, such as the following:

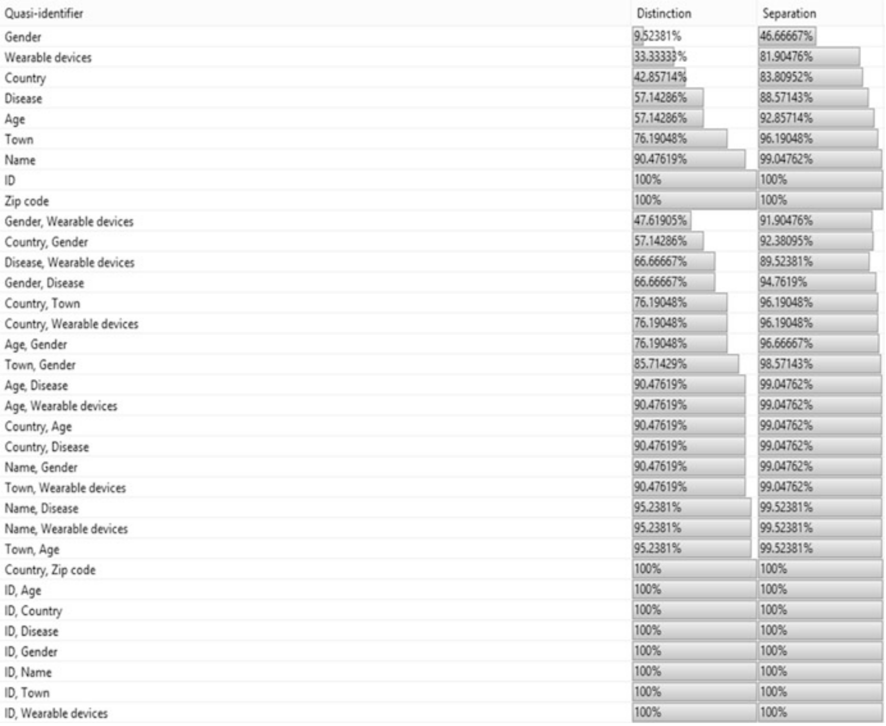
- Attributes having the propriety of recognizing an individual straight forwardly
- Quasi-identifier: linked attributes to external information that identifies each particular individual
- Sensitive attributes: attributes that should not be revealed to third parties.

We generated a model in ARX, we used as input data (Fig. 8) a set of sensitive (age, name, address), and insensitive data (disease, wearable devices), and we applied the models 2-Anonymity and differential privacy. The results are presented in Figs. 15 and 16 that represent the reidentification attack risks before and after data anonymization. In Figs. 12 and 13 the input microdata set, before the attack, and the output microdata after the attack are presented.



		ID	Name	Country	Town	Zip code	Age	Gender	Disease	Wearable devices
1	☑	1	Marlon	UK	London	112034	67	M	Diabetes	Glucose monitor
2	☑	2	Glenn	France	Lyon	112432	75	M	Emphysema	Pulse oximeter, temperature and skin moisture
3	☑	3	Diana	Romania	Bucharest	203412	58	F	Cardiac Insufficiency	Peacemaker
4	☑	4	Flavius	Lithuania	Vilnius	127734	66	M	Arthritis	Pedometer, accelerometer
5	☑	5	Clara	Poland	Varsovia	112732	77	F	Angina	Wearable ECG
6	☑	6	Mihai	Romania	Cluj	231298	72	M	Diabetes	Glucose monitor
7	☑	7	Dane	Ireland	Dublin	342232	44	M	Angina	Wearable ECG
8	☑	8	Carla	Austria	Viena	331245	42	F	Diabetes	Glucose monitor
9	☑	9	Anca	Romania	Brasov	129867	59	F	Aneurysm	Wearable ECG
10	☑	10	Ovidiu	Romania	Bucharest	324578	66	M	Diabetes	Glucose monitor
11	☑	11	Klaus	Germany	Munchen	226743	56	M	Diabetes	Glucose monitor
12	☑	12	Flavius	Italy	Napoli	334897	64	M	Arthritis	pedometer, accelerometer
13	☑	13	Liviu	Romania	Craiova	376521	73	M	Cardiac Insufficiency	Peacemaker
14	☑	14	Eugen	Romania	Brasov	129854	68	M	CAD	Wearable ECG
15	☑	15	Carla	Belgium	Leuven	226436	56	F	Diabetes	Glucose monitor
16	☑	16	Bianca	Italy	Rome	296641	67	F	Diabetes	Glucose monitor
17	☑	17	Darius	Italy	Calabria	129844	56	M	Atherosclerosis	Pedometer, accelerometer
18	☑	18	Anda	Romania	Bucharest	316345	66	F	Stroke	Wearable ECG
19	☑	19	Glenn	UK	London	197745	56	M	Arrhythmia	Peacemaker
20	☑	20	Alina	Romania	Brasov	145322	69	F	Asthma	Pulse oxymeter
21	☑	21	Eusebiu	Romania	Bucharest	236754	72	M	Arrhythmia	Wearable ECG
22	☑	22	Jan	Germany		342312	66	M	Epilepsy	Wearable EEG
23	☑	23	Michele	France	Rouen	229017	75	F	Alzheimer	pedometer, accelerometer
24	☑	24	Monica	France	Nantes	235467	73	F	Parkinson	pedometer, accelerometer
25	☑	25	Adrian	Italy	Pisa	224312	70	M	CAD	Peacemaker

Fig. 12 Input data –ARX



Quasi-identifier	Distinction	Separation
Gender	9.52381%	46.66667%
Wearable devices	33.33333%	81.90476%
Country	42.85714%	83.80952%
Disease	57.14286%	88.57143%
Age	57.14286%	92.85714%
Town	76.19048%	96.19048%
Name	90.47619%	99.04762%
ID	100%	100%
Zip code	100%	100%
Gender, Wearable devices	47.61905%	91.90476%
Country, Gender	57.14286%	92.38095%
Disease, Wearable devices	66.66667%	89.52381%
Gender, Disease	66.66667%	94.7619%
Country, Town	76.19048%	96.19048%
Country, Wearable devices	76.19048%	96.19048%
Age, Gender	76.19048%	96.66667%
Town, Gender	85.71429%	98.57143%
Age, Disease	90.47619%	99.04762%
Age, Wearable devices	90.47619%	99.04762%
Country, Age	90.47619%	99.04762%
Country, Disease	90.47619%	99.04762%
Name, Gender	90.47619%	99.04762%
Town, Wearable devices	90.47619%	99.04762%
Name, Disease	95.2381%	99.52381%
Name, Wearable devices	95.2381%	99.52381%
Town, Age	95.2381%	99.52381%
Country, Zip code	100%	100%
ID, Age	100%	100%
ID, Country	100%	100%
ID, Disease	100%	100%
ID, Gender	100%	100%
ID, Name	100%	100%
ID, Town	100%	100%
ID, Wearable devices	100%	100%

Fig. 13 Risk analysis based on quasi-identifiers

For quasi-identifier (Fig. 13), we used the zip code, and names which could be linked to external data to reidentify individual record owners, and that was removed from output data.

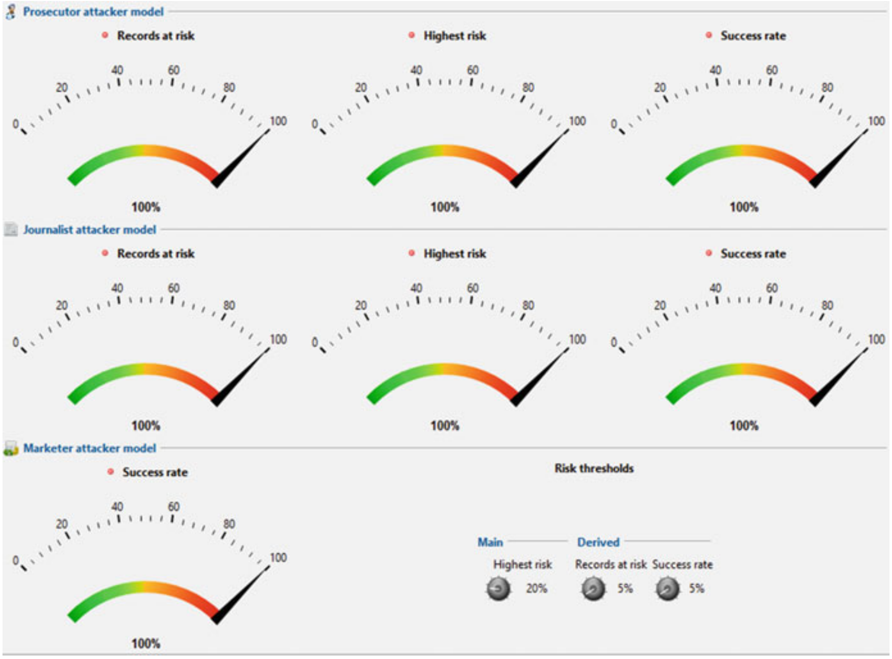
The models used for reidentification attacks are persecutor, journalist, and marketer attack.

Using the reidentification risk analysis implemented, we obtained the estimated risk provided for three different attacker models:

- The prosecutor scenario
- The journalist scenario
- The marketer scenario

In the prosecutor model, the attacker already knows that the data for an individual patient is contained in the data set. In the journalist model, the attacker does not know about data sets content. In the marketer model, the attacker is not interested in reidentifying a specific individual but in attacking a more significant number of individuals' records.

In Figs. 14 and 15 the risk analysis for prosecutor attacker model, journalist attacker model, and marketer attacker model, before and after anonymization by differential privacy model are presented.



Risk thresholds

Main: Highest risk 20%

Derived: Records at risk 5%, Success rate 5%

Fig. 14 Reidentification attack risks before data anonymization

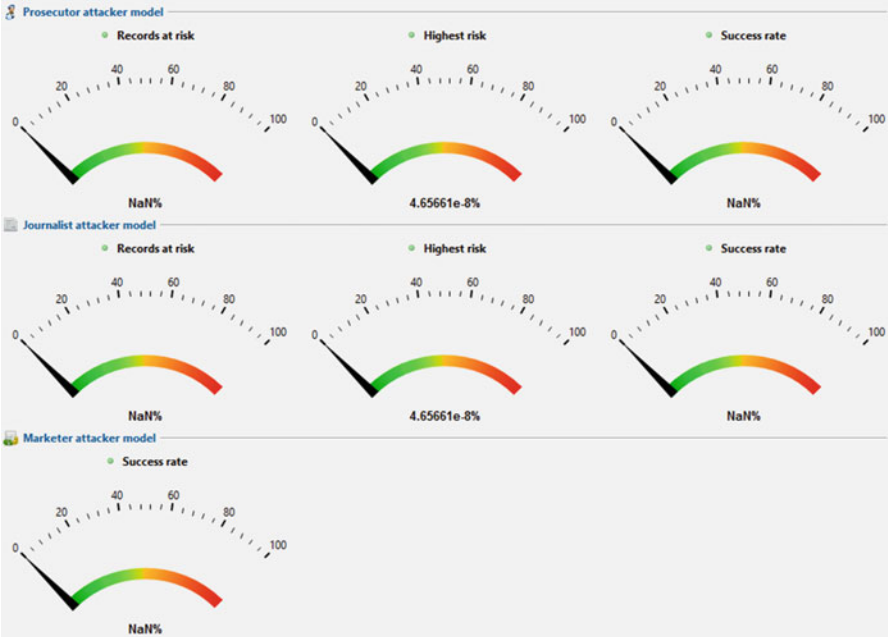


Fig. 15 Reidentification attack risks after data anonymization

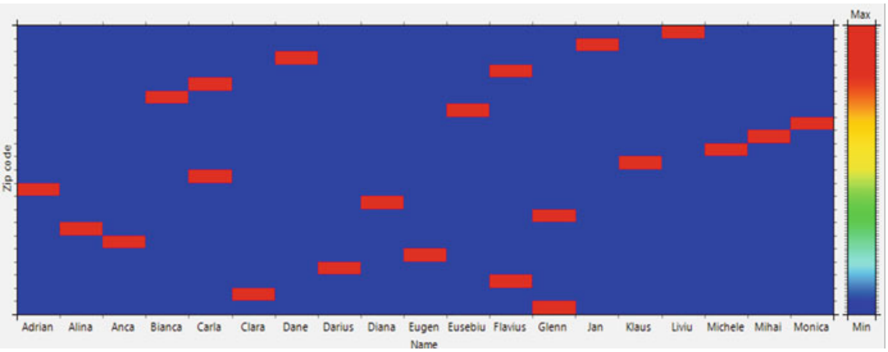


Fig. 16 Contingency before anonymization

Zip code
*
*
Name

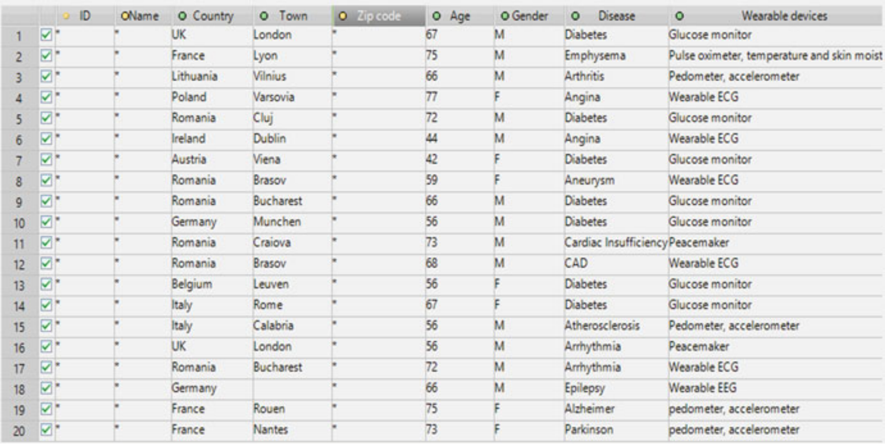
Fig. 17 Contingency after anonymization

In Figs. 16 and 17 the contingency before and after anonymization are presented. The contingency Name = f(zip code) represents the bivariate frequency distribution of the variables (zip code and name).

In Fig. 18, it can be observed that the patient cannot be identified by zip code or name after the anonymization.

7 Conclusions

Sensor network applications in health care are the hot topic of the modern age, which is being researched and deployed all over the world. With the advancement of these applications, effects will arise as well. In this chapter, we tried to highlight the concerns of significant social implications like privacy and security. In order to meet a set of specific security requirements, eHealth monitoring systems confidentiality



		ID	Name	Country	Town	Zip code	Age	Gender	Disease	Wearable devices
1	☑	*	*	UK	London	*	67	M	Diabetes	Glucose monitor
2	☑	*	*	France	Lyon	*	75	M	Emphysema	Pulse oximeter, temperature and skin moist
3	☑	*	*	Lithuania	Vilnius	*	66	M	Arthritis	Pedometer, accelerometer
4	☑	*	*	Poland	Varsovia	*	77	F	Angina	Wearable ECG
5	☑	*	*	Romania	Cluj	*	72	M	Diabetes	Glucose monitor
6	☑	*	*	Ireland	Dublin	*	44	M	Angina	Wearable ECG
7	☑	*	*	Austria	Viena	*	42	F	Diabetes	Glucose monitor
8	☑	*	*	Romania	Brasov	*	59	F	Aneurysm	Wearable ECG
9	☑	*	*	Romania	Bucharest	*	66	M	Diabetes	Glucose monitor
10	☑	*	*	Germany	Munchen	*	56	M	Diabetes	Glucose monitor
11	☑	*	*	Romania	Craiova	*	73	M	Cardiac Insufficiency	Peacemaker
12	☑	*	*	Romania	Brasov	*	68	M	CAD	Wearable ECG
13	☑	*	*	Belgium	Leuven	*	56	F	Diabetes	Glucose monitor
14	☑	*	*	Italy	Rome	*	67	F	Diabetes	Glucose monitor
15	☑	*	*	Italy	Calabria	*	56	M	Atherosclerosis	Pedometer, accelerometer
16	☑	*	*	UK	London	*	56	M	Arrhythmia	Peacemaker
17	☑	*	*	Romania	Bucharest	*	72	M	Arrhythmia	Wearable ECG
18	☑	*	*	Germany		*	66	M	Epilepsy	Wearable EEG
19	☑	*	*	France	Rouen	*	75	F	Alzheimer	pedometer, accelerometer
20	☑	*	*	France	Nantes	*	73	F	Parkinson	pedometer, accelerometer

Fig. 18 Output data: after anonymization

and security have to accomplish particular features. For healthcare data analytics, it is necessary to ensure the patients' data privacy by sensitive data modification by anonymization or removing. The anonymization also has the disadvantage that can lead to insufficient data content or data loss. Using a hybrid cloud presence of public infrastructures like Microsoft Azure or a WAN (wide area network) established between the public and the private cloud. To use the hybrid cloud, servers, a LAN (local area network), and a load balancer must be implemented. A private cloud software layer can be installed to create the virtualization layer or a hypervisor that will be used to sustain VMs (virtual machines) or containers. Besides, it should be mentioned and understood that there is not enough focus on the sensor network, but an overall discussion is needed on the whole system, including backends. Another critical aspect to consider is national security and data protection laws. It is essential to discuss legal and organizational questions, as well as to extend existing PEMS prototypes through security mechanisms. The general public needs to know the benefits and what this implies to be prepared at any time. Rules and regulations of cyber laws, as well as existing health regulations, need to be updated and formalized.

As future work, we envision implementing a cloud platform for managing data privacy for wearable medical devices.

Acknowledgments This work has been supported in part by UEFISCDI Romania and MCI through projects PARFAIT, ESTABLISH, and WINS@HI, funded in part by European Union's Horizon 2020 research and innovation program under grant agreement No. 787002 (SAFECARE) and No. 813278 (A-WEAR).

References

1. S. Ray, J. Park, S. Bhunia, Wearables, implants, and internet of things: the technology needs in the evolving landscape. IEEE Trans. Multi-Scale Comput. Syst. **2**(2), 123–128 (2016)
2. A. Ometov, S.V. Bezzateev, J. Kannisto, J. Harju, S. Andreev, Y. Koucheryavy, Facilitating the delegation of use for private devices in the era of the internet of wearable things. IEEE Internet Things J. **4**(4), 843–854 (2017)
3. M. Haghi, K. Thurow, R. Stoll, Wearable devices in medical internet of things: scientific research and commercially available devices. Healthc. Inform. Res. **23**, 4–15 (2017)
4. J. Wei, How wearables intersect with the cloud and the Internet of Things: considerations for the developers of wearables. IEEE Consum. Electron. Mag **3**, 53–56 (2014)
5. Y. Athavale, S. Krishnan, Biosignal monitoring using wearables: observations and opportunities. Biomed. Signal Process. Control **38**, 22–33 (2017)
6. https://www.carestream.com/blog/2019/01/08/the-iot-in-healthcare-in-2019/
7. Davis J., 87 percent of health organizations plan to adopt IoT technology by 2019, study shows, Healthcare IT News. (2017). https://www.healthcareitnews.com/news%20/87-percent-health-organizations-plan-adopt-iot-technology-2019-study-shows
8. Internet of Medical Things (IoMT) Connecting Healthcare for a Better Tomorrow, UST Global INc. (2017). https://www.ust-global.com/sites/default/files/internet_of_medical_things_iomt.pdf
9. W. Sun, Z. Cai, Y. Li, F. Liu, S. Fang, G. Wang, Security and privacy in the medical internet of things: A review. Security and Communication Networks, in Journal Security and Communication Networks **2018**, 1939–0114 (2018). https://doi.org/10.1155/2018/5978636
10. P.A. Williams, A.J. Woodward, Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem. Medical Devices (Auckland) **8**, 305–316 (2015)
11. D. Miorandi, S. Sicari, F. De Pellegrini, I. Chlamtac, Internet of things: vision, applications and research challenges. Ad Hoc Netw. **10**, 1497–1516 (2012)
12. Deloitte Center for Health Solutions, Medtech and the Internet of Medical Things – How connected medical devices are transforming healthcare (2018). https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Life-Sciences-Health-Care/gx-lshc-medtech-iomt-brochure.pdf
13. The Internet of Me: How Wearable Tech is Changing the Internet of Things, the Application Developers Alliance Emerging Technology Working Group, https://static1.squarespace.com/static/53864718e4b07a1635424cdd/t/54b6aacae4b0b6572f7175e5/1421257418695/ADA+-+IoT+Wearables_Final.pdf
14. L. Wolf, S. Saadaoui, Architecture concept of a wireless body area sensor network for health monitoring of elderly people. Consumer Communications and Networking Conference, 2007. CCNC 2007. 4th IEEE, (2007), pp. 722–726
15. N. Oliver, F. Flores-Mangas, HealthGear: a real-time wearable system for monitoring and analyzing physiological signals. *International Workshop on Wearable and Implantable Body Sensor Networks* (2006) 4
16. W. Yong, G. Attebury, B. Ramamurthy, A survey of security issues in wireless sensor networks. IEEE Commun. Surv. Tutor. **2**(8), 2–23 (2006)
17. T. Zia, A. Zomaya: Security issues in wireless sensor networks. *In Proceedings of International Conference on Systems and Networks Communications, 2006. ICSNC '06*, (2006), pp. 40–40
18. M. Welsh, D. Malan, B. Duncan, T. Fulford-Jones, S. Moulton: Wireless sensor networks for emergency medical care. GE Global Research Conference, Boston (2004)
19. U. Maurer, A. Rowe, A. Smailagic, D.P. Siewiorek, eWatch: a wearable sensor and notification platform. *International Workshop on BSN, Wearable and Implantable Body Sensor Networks*. (2006), pp. 4–145
20. http://fiji.eecs.harvard.edu/CodeBlue

21. S. Vaudenay, *A Classical Introduction to Cryptography: Applications for Communications Security, in Applications for Communications Security*., Springer US (2006). https://doi.org/10.1007/b136373
22. http://www.cms.hhs.gov/
23. W. Yong, G. Attebury, B. Ramamurthy, A survey of security issues in wireless sensor networks. IEEE Commun. Surv. Tutor. **2**(8), 2–23 (2006)
24. A. Milenkovic, C. Otto, E. Jovanov, Wireless sensor network for personal health monitoring: issues and an implementation. Comput. Commun. **29**, 2521–2533 (2006)
25. P. Thibodeau, The Internet of Things could encroach on personal privacy. *Computerworld* (2014)
26. J. Singh, J. Powles, The Internet of Things—the next big challenge to our privacy. *Guardian* (July 28, 2014
27. A. Sacco, Fitness trackers are changing online privacy—and it's time to pay attention, CIO (2014)
28. F. Kargl, E. Lawrence, M. Fischer, Y.Y. Lim, Security, privacy and legal issues in pervasive eHealth monitoring systems. 7th International Conference on Mobile Business ICMB, (2008), pp. 296–304
29. A. Ashraf, A. Rajput, M. Mussadiq, B.S. Chowdhry, M. Hashmani, SNR based digital estimation of security in wireless sensor networks. In *Communications Infrastructure. Systems and Applications in Europe*, vol. 16, (2009), pp. 35–45
30. D. Kouvatsos, G. Min, B. Qureshi: Performance issues in a secure health monitoring wireless sensor network. In *Proceedings of 4th Int. Conference on Performance Modelling and Evaluation of Heterogeneous Networks (HET-NETs'2006), British Computer Society (BCS)*, IEE, Ilkley, UK, September 11–13, (2006) WP01(1–6)
31. H.S. Ng, M.L. Sim, C.M. Tan, Security issues of wireless sensor networks in healthcare applications. BT Technol. J. **24**(2), 138–144 (2006)
32. http://www.its.bldrdoc.gov/
33. T. Zia, A. Zomaya, Security issues in wireless sensor networks. In *Proceedings of International Conference on Systems and Networks Communications, 2006. ICSNC '06*, (2006), pp. 40–40
34. M. Meingast, T. Roosta, S. Sastry, Security and privacy issues with healthcare information technology. 28th Annual International Conference of the IEEE Engineering in Medicine 100 J Med Syst (2012) 36:93–101 and Biology Society, EMBS '06, (2006), pp. 5453–5458
35. https://internetofthingsagenda.techtarget.com/blog/IoT-Agenda/Five-requirements-of-a-leading-IoT-edge-platform
36. https://www.networkcomputing.com/network-security/role-security-edge-computing
37. https://www.iotworldtoday.com/2017/09/23/iot-device-security-comprehensive-look-edge-cloud/
38. G. Suciu, E.G. Ularu, R. Craciunescu, Public versus private cloud adoption—A case study based on open source cloud platforms. In *IEEE 20th Telecommunications Forum (TELFOR)*, (2012) 494–497
39. https://www.networkworld.com/article/3158424/cloud-computing/public-vs-private-cloud-why-the-public-cloud-is-a-real-threat-to-security.html
40. Z. Xiao, X. Fu, R.S.M. Goh, Data privacy-preserving automation architecture for industrial data exchange in smart cities. IEEE Trans. Industr. Inform. **14**(6), 2780–2791 (2017)
41. https://searchcloudsecurity.techtarget.com/tip/Private-cloud-computing-security-issues
42. https://www.forbes.com/sites/forbestechcouncil/2018/06/29/four-major-considerations-for-hybrid-cloud-security/#2c7dad4544a5
43. https://searchsecurity.techtarget.com/magazineContent/Challenges-with-data-protection-in-the-cloud
44. G. Suciu, M. Anwar, I. Rogojanu, A. Pasat, A. Stanoiu, Big data technology for scientific applications. In *IEEE Conference Grid, Cloud & High Performance Computing in Science (ROLCG)*, (2018), pp. 1–4
45. A.A. Vandurke, Data management in the cloud computing IJSRD. Int. J. Sci. Res. Dev. **5**(12) (2018). ISSN (online): 2321–0613

46. R.M. Aileni, S. Pasca, R. Strungaru, Big data predictive analytics for bioheat transfer modeling, *ROLCG Conference*, (2016) ISBN 978-973-0-22868-7
47. R.M. Aileni, S. Pasca and C.A. Valderrama Sukuyama, Wearable health care: Technology evolution, algorithms and needs, in *Book Enhanced Living Environments: From Models to Technologies*, IET Digital Library, pp. 315–343, (2017), doi:https://doi.org/10.1049/PBHE010E_ch13
48. R.M. Aileni, B. Hurezeanu, S. Pasca, Wavelet transform for seizures detection in EEG Records. In *2018 10th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)*, IEEE (2018), pp. 1–6
49. A. Raj, R.G.L.D. Souza, Big data anonymization in cloud using k-anonymity algorithm using map reduce framework. Int. J. Sci. Res. Comput. Sci. Eng. Inform. Technol. **5**(1), 50–56 (2019)