Scientific Research Publishing

Communications and Network, 2017, 9, 249-274
http://www.scirp.org/journal/cn
ISSN Online: 1947-3826
ISSN Print: 1949-2421

Privacy-Preserving Healthcare System for Clinical Decision-Support and Emergency Call Systems

Alia Alabdulkarim[1,2], Mznah Al-Rodhaan[2], Yuan Tian[2]

[1]Information Technology Department, King Saud University, Riyadh, Kingdom of Saudi Arabia
[2]Computer Science Department, King Saud University, Riyadh, Kingdom of Saudi Arabia
Email: aalabdulkarim@ksu.edu.sa, rodhaan@ksu.edu.sa, ytian@ksu.edu.sa

How to cite this paper: Alabdulkarim, A., Al-Rodhaan, M. and Tian, Y. (2017) Privacy-Preserving Healthcare System for Clinical Decision-Support and Emergency Call Systems. *Communications and Network*, **9**, 249-274.
https://doi.org/10.4236/cn.2017.94018

Received: November 2, 2017
Accepted: November 25, 2017
Published: November 29, 2017

Abstract

Healthcare centers always aim to deliver the best quality healthcare services to patients and earn their satisfaction. Technology has played a major role in achieving these goals, such as clinical decision-support systems and mobile health social networks. These systems have improved the quality of care services by speeding-up the diagnosis process with accuracy, and allowing caregivers to monitor patients remotely through the use of WBS, respectively. However, these systems' accuracy and efficiency are dependent on patients' health information, which must be inevitably shared over the network, thus exposing them to cyber-attacks. Therefore, privacy-preserving services are ought to be employed to protect patients' privacy. In this work, we proposed a privacy-preserving healthcare system, which is composed of two subsystems. The first is a privacy-preserving clinical decision-support system. The second subsystem is a privacy-preserving Mobile Health Social Network (MHSN). The former was based on decision tree classifier that is used to diagnose patients with new symptoms without disclosing patients' records. Whereas the latter would allow physicians to monitor patients' current condition remotely through WBS; thus sending help immediately in case of a distress situation detected. The social network, which connects patients of similar symptoms together, would also provide the service of seeking help of near-by passing people while the patient is waiting for an ambulance to arrive. Our model is expected to improve healthcare services while protecting patients' privacy.

Keywords

Privacy-Preserving, CDSS, MHSN, Decision Tree, Random Forest, Random Decision Tree, Opportunistic Computing

1. Introduction

The PHR is the essential asset of any healthcare center (Hospitals, clinics, ... etc.). Physicians depend on it to record the patient's medical history, and to refer to it during diagnosis. Due to the fact that PHRs are computerized nowadays, they are subject to various attacks; and therefore, precautions must be taken to preserve their privacy. Furthermore, many applications such as CDSS and MHSN are used to improve healthcare services. CDSS is a system used by physicians to help them decide which disease class the diagnosed patient's symptoms belong to; it is based on a knowledge base that is extracted from experts and/or literature [1]. Moreover, MHSNs are social networks of patients and caregivers, where the latter observe the patients remotely through Wireless Body Sensors (WBS) attached to their bodies, and communicate the patient's current status to caregivers periodically. Therefore, distress situations could be detected at the moment, and help could be sent immediately. In addition to the emergency call service, there is the social feature that would connect patients together. However, all of these systems depend on the phi; hence, the improvement of care they provide could be on the expense of the privacy of the patients [2] [3] [4]. In this study, we explore different healthcare systems to design a model that would enhance the medical care services provided to patients while preserving the privacy of their PHR.

1.1. Problem Definition

Consider Bob is a patient, visiting Alice, a physician in a hospital. Alice uses the CDSS to decide Bob's illness. However, the CDSS is placed on a cloud; thus, Bob's information is required to be transmitted over the network, making it exposed to the cyber attacks. Moreover, the CDSS on the cloud needs historic medical records of different patients to build their decision-support system, which may also expose patients' private health information to an unauthorized person. Now suppose Alice wants to monitor Bob's condition remotely, which also requires health information to be transmitted over the network and risking it to be exposed. Consequently, privacy preserving measures are needed to protect the Patients' Health Information (PHI). Furthermore, what if the device used to remotely monitor Bob is low on energy and there are no means for recharging it. All of the above problems are considered major threats for the patients' information and the quality of the healthcare services they are receiving. Besides, there are various studies that tackled these problems and proposed different solutions such as [2] [3] [4]; however, each problem was addressed separately.

1.2. Motivation

Considering the problems related to healthcare services mentioned earlier, we are motivated to design a model which comprises a CDSS and an MHSN with privacy preserving solutions to keep PHI protected from unauthorized accesses,

and improve the quality of healthcare services provided by healthcare centers. Moreover, we intend to design the CDSS on a cloud, which its classification model will be trained and tested without accessing the original data. Furthermore, we plan to exploit the advantages of MHSN to provide a social network that would aid physicians in monitoring their patients from a distance, and also linking patients together for support and comfort. Finally, we aim to improve the solutions available in the existing studies, and propose them as one system.

1.3. Methodology

In order to go on with our research, we will need to conduct the following steps:

1) Design our two subsystem models for a **P**rivacy **P**reserving **C**linical **D**ecision-**S**upport **S**ystem (PPCDSS), and a **P**rivacy **P**reserving **E**mergency **C**all **S**ystem (PPECS).

• PPCDSS: This system consists of two parts, training and testing:

- Training include building a decision tree model without disclosing patients' PHI.

- Testing the classifier will be conducted by classifying new patients.

• PPECS: This system starts by each patient being hooked with a wbsn for sensing their vital signs and transmit them to the PDA for processing, and setting patient's preferences of whom they wish to come to the rescue (helper). The system requires the design of:

1) Access policy matrix which forms the patients' preferences of who to help.

2) The emergency call system.

3) The opportunistic computing framework.

4) The symptoms matching algorithm.

2) Insure the security of both subsystems through mathematical security proofs.

1.4. Contributions

Healthcare systems seek technology to enhance their performance while aiming to keep patients comfortable. Systems such as CDSS and MHSN provide the services to improve physicians' productivity and patients' satisfaction [2] [3] [4]. However, because these systems depend on transmitting patients' PHI through a network, that leaves the PHI vulnerable for attacks. Therefore, privacy-preserving systems are necessary to protect patients' privacy over these systems.

In our work, we propose a model consisted of two subsystems. The first subsystem, PPCDSS, will provide a CDSS with a privacy-preserving feature to protect patients' PHI. The second subsystem, PPECS, is an MHSN which allows physicians to monitor patients remotely without disclosing patients' PHI to unauthorized persons. Below, we list our contributions to the field:

1) We will merge the existing services in the literature in one model.

The existing systems in the literature, [2] [3] [4], either provide the emergency

call service, the opportunistic computing framework, or the classification feature.

2) We will use decision trees as the data mining technique for the CDSS.

Studies in section 2 have shown that decision trees are more accurate than NBC in medical diagnosis.

3) Our model allows to hide the votes of each hospital than each other; thus, no hospital can know which hospital objects to which tree(s).

The study in [5] protected each party's dataset by regenerating the ensemble and not revealing the objecting party objected to which tree(s) (**Figure 1(a)**). By using a cloud we eliminate the need of regenerating the ensemble (**Figure 1(b)**).

4) We will limit the access to the cloud's functions to health institutions, thus making the system be more secure (**Figure 2(b)**).

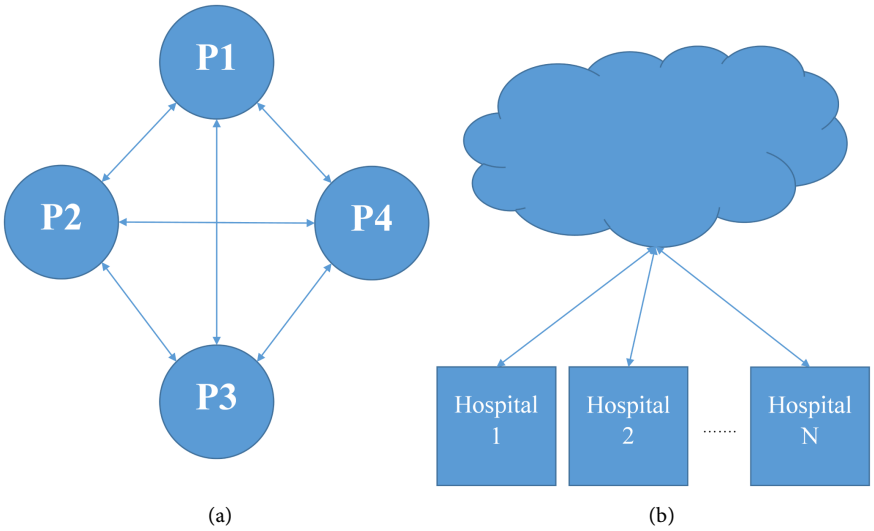

Figure 1. Hiding of Votes. (a) All parties exchange votes without a third party; (b) with a cloud, each party is oblivious of other parties' votes.

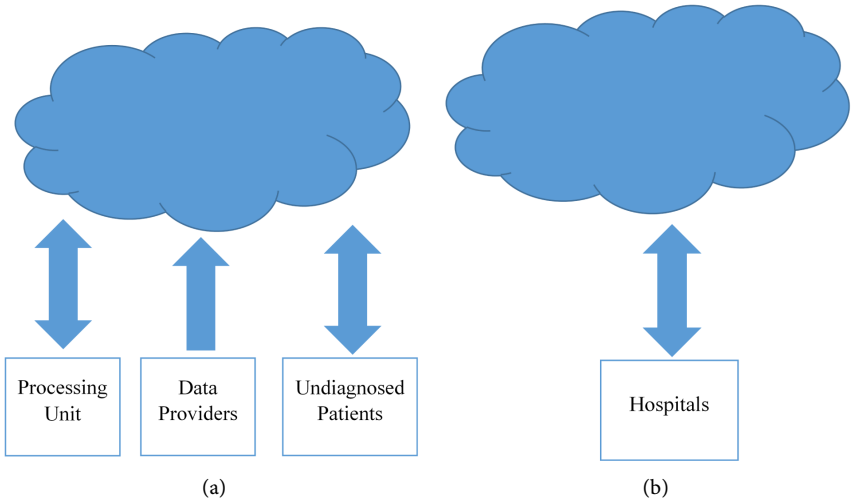

Figure 2. Participating Parties. (a) Three different parties are engaging with the cloud; (b) only hospitals are engaging with the cloud.

The PPCDSS in [3] gives access to the cloud to three different parties (**Figure 2(a)**).

1.5. Organization

The rest of the paper will be organized as follows. In Section 2, we provide a background on the current state of healthcare systems and followed by the related work in Section 2. The proposed model is listed in Section. In Section 9 we lay a motivational scenario for our proposed model. Finally, the conclusion in Section 17.

2. Background

Healthcare centers have taken advantage of technology to improve their services for a long time. For instance, they have turned to electronic health records instead of paper based for fast access and for environmental reasons. However, distributed patient information over different systems is still a problem. This problem has caused dissatisfaction of patients for being examined multiple times by different physicians and thus wasting the times of both [1]. Therefore, K. Leonard in [6] have stressed on the need to give patients the control of their health records, in addition to have one existing copy to give physicians fast access to the patient's medical history, and therefore enhance their health services. Below, we display examples of healthcare systems which helped in ceasing this problem.

2.1. Clinical Decision-Support System

The process of medical diagnosis is described as follows. The physician first start by collecting facts about the patient's medical history, physical examination, and laboratory tests. Then, the physician will begin to evaluate the symptoms and signs to make a list of all possible diseases. Finally, he will perform differential diagnosis by excluding one disease after another from the list until the diagnosis is fit into one category of diseases. As simple as it sounds, this process is considered complex [7]. Therefore, a solution to ease this process was needed to enhance physician's performance, and clinic's medical services.

Clinical Decision-Support Systems (CDSS) are defined to be any computer software developed to assist physicians in making clinical decisions using patient's medical history and clinical data [8] by providing them with patient-specific clinical information to enhance the quality of medical services [9]. Moreover, they were proven to improve patient's results, costs of care [1], and clinician's behavior by providing alerts, reminders, and treatment plans [10]. Hence, there was a growing interest in deploying CDSS in healthcare centers [1]. However, due to its nature of dealing with sensitive information, its evaluation is based on its accuracy, not physicians' performance improvement [10]. Therefore, the accuracy of these systems must be properly validated and tested to avoid patient morbidity. This is done by validating the system knowledge and

advice to assure they are accurate, consistent, and complete [11]. Furthermore, CDSS uses machine learning techniques, such as nave Bayes or decision trees, to build their systems. Moreover, the privacy preservation of patient's information in the system is another important concern [3].

2.2. Wireless Body Sensors Network

Patients with chronic diseases suffer from wasting their time at hospitals for monitoring their vital signs. Moreover, patients may undergo an emergency situation and cannot call for help. All these scenarios are possible and may happen at any time. One solution to this problem is to attach the wearable sensors to the patients for remote monitoring. This system is called mobile healthcare systems (m-healthcare) [4]. These wearable sensors form a wban, where the attached sensors will collect the vital signs of the patient and report them periodically to a device held by the patient; the latter will then forward the collected data to the healthcare centers [12]. They are considered as non-expensive solusions, which may provide a life log of sensed vital signs [13]. Furthermore, in case of an emergency, the carried device will detect the situation and alert the healthcare system to send an ambulance [4]. Therefore, m-healthacre systems will enhance the healthcare monitering systems [14].

2.3. Mobile Healthcare Social Network

M-healthcare systems were improved to add a social networking feature. In mobile healthcare social networks (MHSN), in addition to m-healthcare's monitoring and emergency services [2] [4], they may offer social networking between the patients themselves by connecting the ones with similar symptoms for experience exchange and support [15]. Due to these advances in healthcare technologies, nowadays, healhcare service centers are increasingly adapting MHSN into their systems for its convenience and efficiency [12]. However, the transmission of a patient's health information (PHI) raises a security issue. PHIs should be protected from attackers and eavesdropper in the network [2] [4].

2.4. Privacy-Preserving Healthcare Systems

To preserve the privacy of patients' PHI, encryption is used. For instance, homomorphic encryption can be used to hide the meaning of the patients' PHI before feeding them to the decision support system for training. Also, attribute-based encryption is useful because it helps patients in deciding who to access their PHI in the medical social networks. Moreover, secure techniques for matching patients with similar symptoms will allow patients of similar conditions to communicate safely without leaking PHI details.

3. Related Work

Our proposed model explores different fields of privacy-preserving such as healthcare systems, machine learning, opportunistic computing, and profile

matching. In this section, we briefly overview the studies related to our work to build an understanding of the current state of technology and their issues.

Privacy-preserving Healthcare Systems: Ledley and Lusted [7] are considered the pioneers in addressing the area of clinical decision-support systems (CDSS). They have explained the complicated process of diagnosing patients, and how computers can help physicians in excelling this process. They have proposed different models, using different mathematical disciplines, such as symbolic logic and probability (nave Bayes). Their work was the landmark of later studies in this field [8]. For example, [16] have presented the first Bayesian classifier for congenital heart disease patients. The model was based on the patient's symptoms, electrocardiograph results, and physical exam. Furtherly, the work in [17] described the challenges faced by intensive care unit physicians in diagnosing and treating infectious diseases; and therefore, discussed more than a few models, including nave Bayes, which could be deployed in the future of clinical practice. The early studies of clinical decision-support systems focused on the goal of improving the healthcare services by providing timely patient-specific information without turning the attention to the importance of preserving the patient's privacy. However, the work in [3] proposes a Privacy-preserving Patient-centric Clinical Decision support system (PPCD), which is based on Nave Bayesian classifier, to aid physicians and care givers in diagnosing patients while preserving their privacy. The system collects and aggregates patients' symptoms and diseases to train the Nave Bayesian classifier. The classifier is then used by physicians and patients to diagnose and retrieve results respectively.

Privacy-Preserving Decision Tree: is the task of generating decision trees from multiple party datasets without revealing private datasets to other parties [18]. The privacy-preserving techniques used varied between encryption and secret sharing schemes. The study in [18] used homomorphic encryption and digital envelope to construct a collaborative decision tree classification model without disclosing private datasets to other participating parties. Another model proposed by [19] used a semi-trusted commodity server. In their model, the data is vertically split among parties. Furthermore, the authors in [20] proposed a privacy preserving model using polynomials and fully homomorphic encryption; where decision trees are expressed in polynomials. Using oblivious transfer, the study in [21] [22] designed a privacy preserving decision tree model for constructing a classification model out a dataset divided between two parties, without revealing one's dataset to the other. Moreover, a study in [23] proposed a privacy preserving decision tree model over multiple parties using ID3; they have constructed the model to exchange the proportions needed to calculate the information gain through Secret Sharing Scheme (SSS). Another study in [5] proposed an RDT model for constructing a classifier between two parties; homomorphic encryption was used to encrypt leaf vectors.

Ciphertext Policy Attribute Based Encryption. The first CPABE was proposed by [24]. In their construction, the secret key is associated with a set of de-

scriptive attributes, and the ciphertext is associated with an access policy describing who has the privilege to decrypt the ciphertext. When a user receives a ciphertext, he can decrypt it if his descriptive attributes satisfy the access policy. The access policies in their work are based on access tree structures. Moreover, their scheme thwarts collusion attack by randomizing users' keys in a way to prevent them from combining the keys. Because decryption process is recursive, which is expensive, they have also proposed an optimization solution. Later studies, [25] [26] [27], came to improve [24]. In [27] the authors presented a scheme for CPABE that is expressive, efficient, and provably secure. It allows access control to be specified in terms of any access formula over the system attributes. While the works in [25] [26] have improved the efficiency or achieved higher level of security. Another comparative study in [28] have proposed a simple and effective scheme of CPABE using a single AND gates on positive and negative attributes. Their results show that they have achieved shorter decryption time than [24], and shorter secret key and ciphertext. Although their scheme show better performance results at a certain range of attribute numbers than [24], it imposes a limitation on the system for not being able to handle more expressive types of access policy structures.

Fully Homomorphic Encryption. Gentry's profound work has laid the foundations for FHE [29]. He solved the accumulated noise problem through *bootstrapping*. Bootstrapping involved blind partial decryption of the ciphertext to remove the noise. In other words, after performing a number of homomorphic operations on the ciphertext, decrypting and re-encrypting will produce a fresh-noise-free ciphertext [30]. Until today, there are plenty of attempts to present a practical FHE in literature [29] [31] [32] [33] [34]. Those papers covered many applications. However, Cloud computing is considered the main application of HE. Other applications included electronic-voting, multiparty computation, information retrieval, and database encryption delegations [35].

Opportunistic Computing. It is a framework which uses opportunistic communication between two devices for resources and services sharing. It became an interesting field for research and development [36]. The study in [37] addresses the problem of storing and executing an application that surpasses the memory resources available on a single node. Their work was based on dividing the code into a number of modules that are cooperating opportunistically. The original application is executed by running its subset of tasks at the corresponding node, which in turn provides services to neighboring node. The study in [4] has presented and exemplary work in opportunistic mobile social networks in the field of healthcare systems. Realizing the importance of real-time monitoring of patients of chronic diseases outside the hospital, they have proposed a system which takes advantage of nearby person's (helper) smartphone when the patient's smartphone is running low on power. Furthermore, a user-centric two-phase access control policy was designed to ensure patient's privacy; hence, a helper should be a medical user with similar symptoms according to a user-

predefined threshold. An implementation of this work was illustrated in [38]. The literature in this area remains scarce.

4. Proposed Model

In this section, we describe our proposed model through a descriptive scenario (4.1) and overall detailed description (4.2).

4.1. Descriptive Scenario

Consider Alice who is a cardiologist in Hospital C. Bob, who is a cardiology patient, is visiting Alice for the first time. Normally, Alice will have to collect Bob's Symptoms then apply her knowledge base to determine Bob's disease or condition. However, this task may vary in duration, and Alice has many patients to see and examine. To avoid wrong diagnoses, Alice would need assistance in making faster decisions. A CDSS would come in handy in such situation. These systems build a decision model based on a wide knowledge base of symptoms and their corresponding disease(s) collected from different hospitals. Using such systems will help Alice to speed up the diagnosis process with fewer errors.

Alice also would like to keep a constant monitoring of her chronic disease patients. So imagine Bob being diagnosed with a chronic condition. At first, Alice needs to monitor his condition without being hospitalized because Bob's condition does not require hospital admission, beside he has a family and a career that needs his presence. Therefore, Alice will equip Bob with Wireless Body Sensors (WBS) and a PDA. The WBS will periodically read Bob's vital signs and communicate them to the PDA, which in return will process them and transmit the processed results to Alice in Hospital C. This way, Alice can keep a close eye on Bob while he is moving along in his life.

Now let us imagine Bob being home alone and had a sudden heart attack. The PDA will immediately detect this urgent condition and will send a call for an ambulance to Hospital C, and notify Alice. Until the ambulance arrives, Bob will remain on the floor waiting for help that may take time due to long distance and/or traffic. To accelerate the first aid, a mobile health social network (MHSN) will be used to look for a nearby person for help. Normally, Bob would have been signed up with his customized PDA. Moreover, the nearby person may act as a relay to rebroadcast the call for help to broaden the search area, or he may be another patient using the same MHSN, a physician, or a paramedic. The latter two, physician or paramedic, will rush to the location upon receiving the call, and if the predefined settings in the PDA approve them as helpers. Bob will receive proper first aid while waiting for the ambulance.

The above scenario will require Bob to have a sufficient power on his PDA. However, since this can not be guaranteed, a solution is needed for such case. Opportunistic Computing may overcome this problem. Bob's PDA in this situation will first look for a nearby agent/proxy before searching for help. The agent/proxy's role is to act on behalf of Bob in searching for helpers. Therefore, the

consequences of having low energy on Bob's PDA could be avoided using opportunistic computing.

4.2. System Description

In our model, we aim to provide a system that enhances the medical services in hospitals and health institutions. We focus on two primary aspects in health services, diagnosis and emergency calls. In the former, it is widely known that it's not a straight forward process, which requires multiple steps to go through in order to reach the most proper diagnosis [7]. Moreover, in case of patients of chronic diseases, physicians wish to monitor their vital signs around the clock, however, it is hard to keep the patients in hospitals just for reading their vital signs periodically to detect abnormal conditions the moment they occur. Therefore, we propose a system that addresses the above problems with privacy preserving.

Before we start with the system description, we will identify the main parties involved in the system as shown in **Figure 3**:

1) Trusted Authority (TA): which is responsible for key management during setup.

2) Cloud: consists of three units:

a) Single Decision Tree (SDT) unit: responsible for calculating the entropy and information gain and decide where to split the dataset.

b) Random Forest (RF) unit: responsible for securely aggregating the local ensembles received from all hospitals, and then run the electronic voting manager to form the final global ensemble.

c) Random Decision Tree (RDT) unit: responsible for securely aggregating the local ensembles received from all hospitals, and then run the electronic voting manager to form the initial global ensemble. Finally, it prompts each hospital to complete filling the leaf nodes of each tree in the ensemble and then securely aggregates the ensembles again to sum up the values in leaf node to form the final global ensemble.

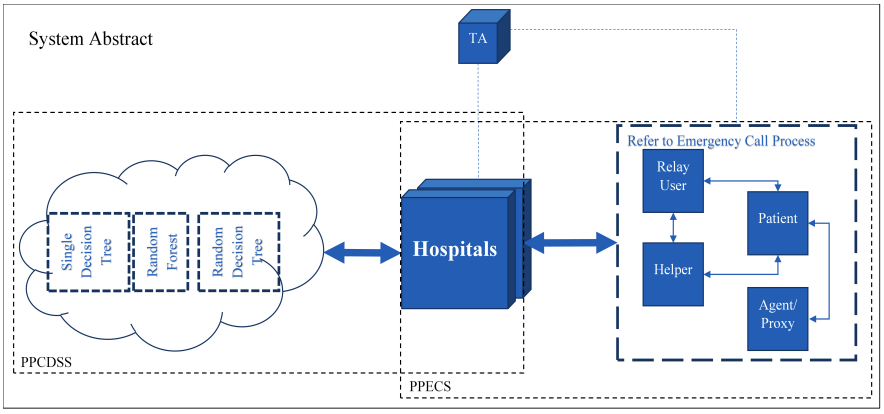

Figure 3. System Abstract. Showing the two subsystems, PPCDSS and PPECS, and their components.

3) Hospitals (healthcare centers): provides the system with the historical medical data (HMD). And, it uses the diagnosis unit inside the cloud to classify new symptoms.

4) Patients: are system users who has symptoms and disease class, and are being remotely monitored.

5) Relay user: is a passing-by system user who doesn't meet the patient's criteria of a helper, and can only receive the encrypted patient's health information (PHI) and re-broadcast them to other passing-by users.

6) Helpers: are system users who could be a patient, physician, or paramedic.

7) Proxies or Agents: other system users who are patients with similar symptoms.

Since our focus is on diagnosis and emergency calls, we divide our model into two subsystems, the ppcdss, and the ppecs. The overall system model is depicted in Figure 4.

4.2.1. Privacy-Preserving Clinical Decision-Support System (PPCDSS)

First, we start with the diagnosis part of the system. In practice, physicians collect patient's vital signs and symptoms to decide on their diagnosis. This symptom-disease matching process could be accomplished through different sets of processes. However, they all require numerous and time consuming steps [7]. In our model, we propose a design for a CDSS (Clinical Decision-Support Sys-

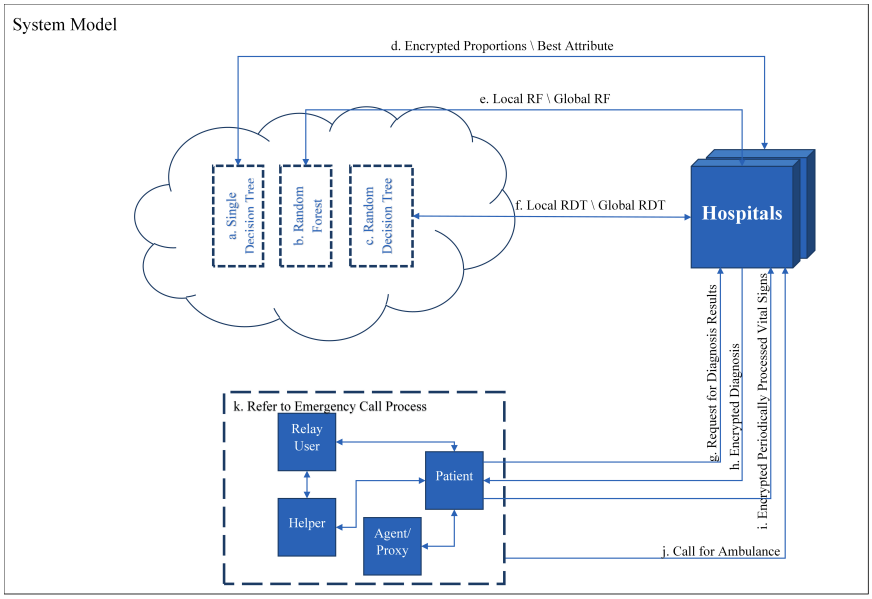

Figure 4. System Model. (a) The SDT unit; (b) the RF unit; (c) the RDT unit; (d) the encrypted proportions needed to build the SDT and the best attribute to split the dataset returned by the cloud; (e) the hospital's local RF ensemble, and the global RF ensemble returned by the cloud; (f) the hospital's local RDT ensemble, and the global RDT ensemble returned by the cloud; (g) the patient requesting for the diagnosis results after visiting the hospital; (h) the hospital response for the patient's request in (g); (i) transmitting the patient's periodically processed vital signs; (j) the call for an ambulance that could be transmitted from any user within (k); (k) the users of PPECS.

tem) to enhance physicians' productivity. The design is based on three variations on decision trees, Single Decision Tree (SDT), Random Forest (RF), and Random Decision Tree (RDT) (**Figures 4(a)-4(c)**). As the name implies, SDT is composed of one decision tree that is built from the whole dataset. On the other hand, RF and RDT are ensembles of decision trees. Each RF tree is built from a random subset of the whole dataset; whereas, each RDT tree is randomly built from the whole dataset. In our model, each hospital will locally build its own RF/RDT ensemble, and send it to the cloud; there, the final ensemble will be formed and sent back (**Figure 4(e)**, **Figure 4(f)**). Hospitals now can perform diagnosis locally using their decision model. Finally, the classification results will be securely forwarded to the patient's PDA upon request (**Figure 4(g)**, **Figure 4(h)**). Below we describe each decision model in details.

Single Decision Tree (SDT) Model: In this model, the goal is to build an SDT from the datasets of all hospitals put together (whole dataset). However, to maintain the privacy of each hospital's dataset, we use the cloud to act like a coach and direct each dataset owner (hospitals) where to split their data (**Figure 4(d)**). the process starts by having each hospital evaluate the proportions for each attribute that are needed to calculate the Entropy (E) and Information Gain (IG). Then, the evaluated proportions will be fully homomorphically encrypted and transmitted to the cloud (**Figure 5(a)**). there, the proportions aggregator (**Figure 5(b)**) will securely sum the proportions of the same attributes ; thus, obtain the attribute proportions of the whole dataset. The entropy calculator (**Figure 5(c)**) will use the former values to calculate the entropy of the dataset and each attribute; then hand them over to the IG calculator (**Figure 5(d)**) to calculate the IG of each attribute. Finally, the attribute with maximum IG value

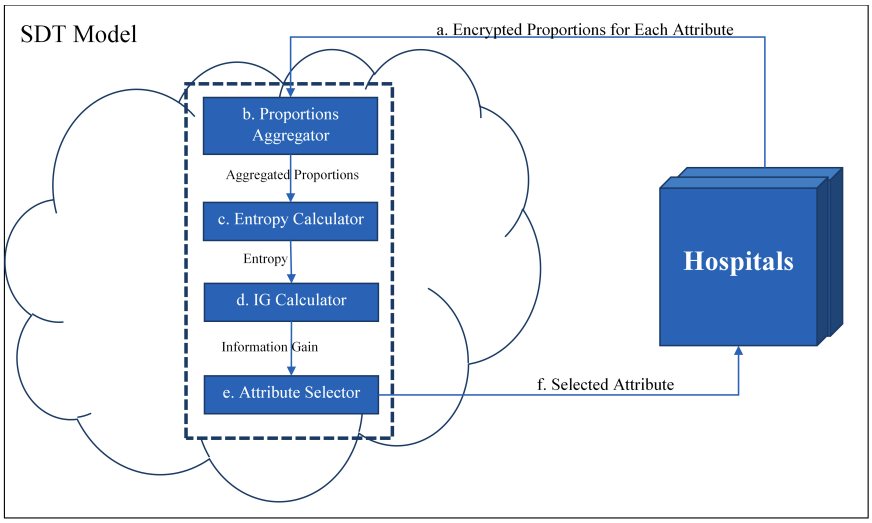

Figure 5. SDT Model. (a) The encrypted proportions for each attribute needed to calculate E and IG; (b) received proportions will be aggregated and summed for same attributes; (c) calculates entropy from aggregated proportions; (d) calculates information gain from entropy; (e) selects the attribute with maximum gain; (f) the best attribute is sent back to the hospitals.

will be selected by the Attribute Selector (Figure 5(e)), and then transmitted back to the hospitals (Figure 5(f)) to direct them where to split their datasets. This iterative process will continue until the complete decision tree is built at each hospital site.

Random Forest (RF) Model: A random forest is an ensemble of SDTs, where each one is built out of a random subset of the whole dataset. Since our whole dataset is considered as the aggregated datasets of all hospitals, we can think of each single dataset is a random horizontal subset. Therefore, each hospital can generate its own random forest and transmit it to the cloud (Figure 6(a)). There, the ensemble aggregator (Figure 6(b)) will form the initial global ensemble by removing any redundant trees. The output of the previous step will be handed over to the Electronic Vote Manager (EVM) (Figure 6(c)); in which it will send it to all hospitals to review and vote (Figure 6(d)). Each hospital will review the initial ensemble and vote out any tree that it considers revealing knowledge of its own dataset, then it will send its vote back to the cloud (Figure 6(e)). Each vote can only be seen by the cloud, thus, hiding the identity of the objecting hospital from the others. Finally, the EVM will remove the voted out trees from the ensemble, and then transmits the final global ensemble to all hospitals (Figure 6(f)). Although no security, nor privacy techniques were used in this model, the privacy was achieved through hiding the original datasets.

Random decision tree (RDT) Model: RDTs are an ensemble of randomly generated decision trees based on the whole dataset attributes. This variation of decision trees doesn't use the example in the dataset; however, it predefined a random tree height value, then it will randomly pick an attribute name to build the tree until the predefined height is reached. Finally, the last level of each tree will be of empty leaves. the process will continue until a certain number of trees are built. At this stage, the trees are only made-up of attributes but no classes. The next step is to assign to each leaf node a vector; the length of the vector is

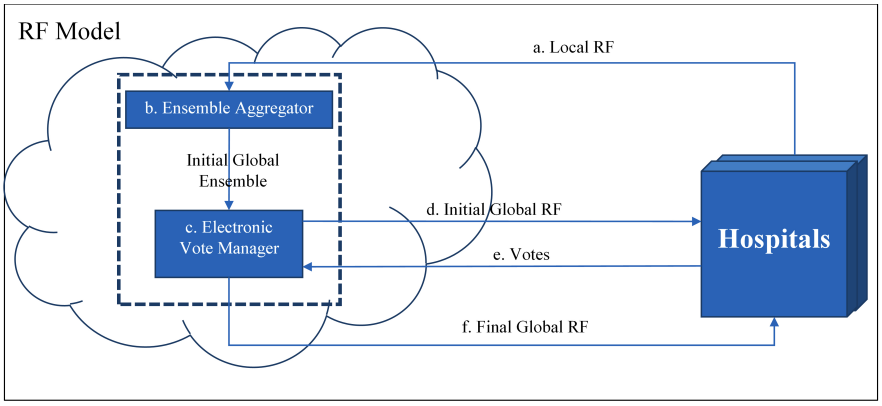

Figure 6. RF Model. (a) The locally generated RF ensemble at each hospital; (b) the received ensembles will be aggregated in one initial global ensemble; (c) the EVM will run and manage the voting on ensemble trees; (d) the initial global ensemble is sent to the hospitals to cast their votes; (e) each hospital will return their votes to the cloud; (f) the final global ensemble after removing voted out trees is sent to each hospital.

the number of the total classes, and each element value denotes the count of the examples of each class down the path of each leaf. In our model, each hospital will generate its own RDT of previously agreed upon number of trees and height. But before the vectors' elements are filled, each hospital will send its ensemble with empty leaves to the cloud (**Figure 7(a)**). There, the ensemble aggregator (**Figure 7(b)**) will form the initial global ensemble by removing any redundant trees. Then the EVM will run a vote on the ensemble (**Figures 7(c)-7(e)**). After forming the final ensemble with empty leaves, the Leaf Vector Calculator (LVC) (**Figure 7(f)**) will send it totall hospitals to fill in their count of examples (**Figure 7(g)**). Then, each hospital will encrypt the leaf vectors homomorphically to keep them private, and send it back to the cloud (**Figure 7(h)**). There, the cloud will homomorphically sum up the vectors of same trees to form the final global ensemble. Finally, the latter will be sent back to the hospitals (**Figure 7(i)**).

All of the above models will go through periodic updates for improving their performance. As for diagnosing new patients, it will always be done locally; thus, keeping their symptoms private.

4.2.2. Privacy-Preserving Emergency Call System (PPECS)

In the second part of the system model, the focus is directed towards the chronic patients who require constant monitoring. Instead of keeping them inside the hospital, they will be equipped with wireless body sensors which are connected with the patient's PDA via Bluetooth to form a wireless body sensor network (WBS). These sensors will periodically read the patient's vital signs and transmit them to the PDA, which in return, will process and transmit the data securely to the healthcare center (**Figure 4(i)**), therefore, allowing physicians to monitor

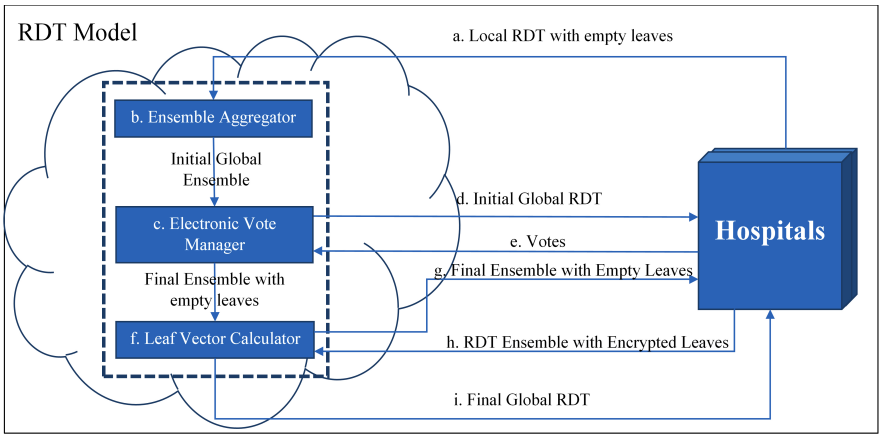

Figure 7. RDT Model. (a) The locally generated RDT ensemble at each hospital with empty leaves; (b) the received ensembles will be aggregated in one initial global ensemble with empty leaves; (c) EVM will run and manage the voting on ensemble trees; (d) the initial global ensemble is sent to the hospitals to cast their votes; (e) each hospital will return their votes to the cloud; (f) the LVC will manage the collection and summation of leaf nodes; (g) the initial global ensemble with empty leaves will be sent to the hospitals to fill in their counts; (h) each hospital will return the ensemble back to the cloud after evaluating the leaf nodes values; (i) the final global ensemble is sent to each hospital.

their patients from distance. Furthermore, in case the patient was going through a distress situation, such as a heart attack, the PDA will detect the current condition, and will send a call for ambulance to the healthcare center (**Figure 4(j)**). Meanwhile, the PDA will continue sending its periodic readings in a higher frequency. Besides, the PDA will start looking for any potential helper in the area to provide first aid until the ambulance arrives (**Figure 4(k)**). However, to preserve the patient's privacy, the potential helpers are carefully picked (**Figure 8**). First, they have to be members of the system; either patients, physicians, or paramedics. Then, depending on the searching patient's preferences on the type of the helpers, only the preferred users will be able to respond to the call (**Figure 8(a)**). Such scheme is achieved by using attribute based encryption. In addition, even if the potential helper doesn't meet or satisfy the patient's preferences, they will act as relay users who will re-broadcast the emergency call for a broader area coverage (**Figure 8(b)**).

The patient's distress situation may occur while their PDA is low in energy. In such case, the patient's PDA will start searching for a near-by system user with

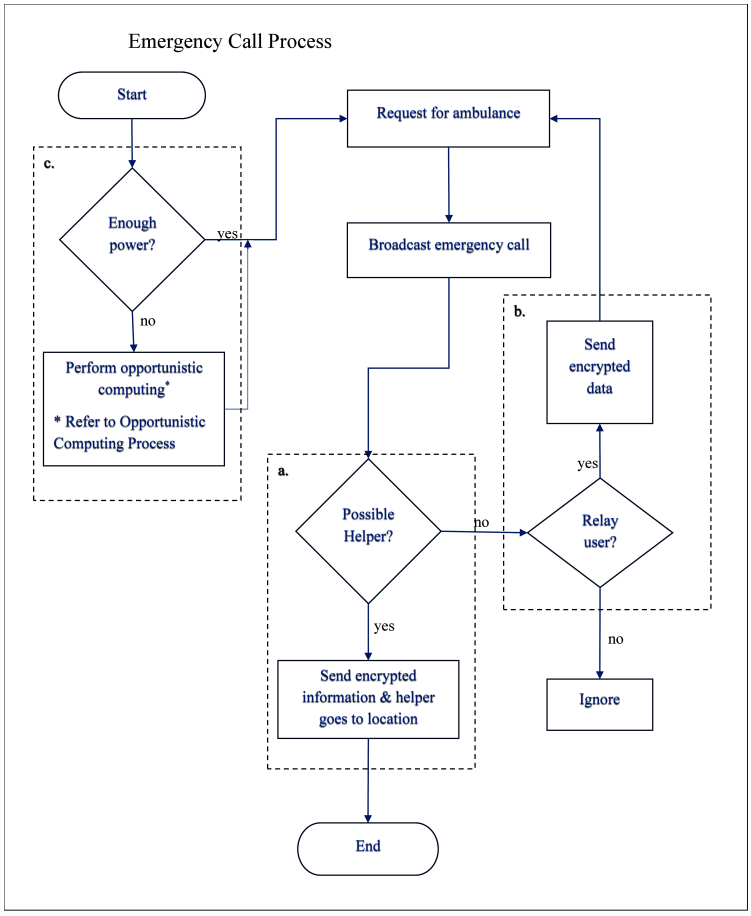

Figure 8. Emergency Call Process. (a) Testing the validity of near-by person by testing them against the patient's access control matrix; (b) when a near-by person doesn't pass the test in (a) he is tested for whether being a relay user or not; (c) in case the patient's PDA has low energy, the process in (c) is launched.

sufficient energy on their PDA to act as a Proxy or agent and carry on the above tasks on behalf of the original patient (**Figure 8(c)**). However, those users who happens to be another patients using the same system, must have certain similarity with the original patient's symptoms. The threshold of similarity is decided during setup by the patient (**Figure 9**). The algorithm in [39] will be used to measure the similarity in symptoms between two patients.

The symptom matching algorithm works by prompting for the near-by user's symptoms vector, which is for security purposes will be transmitted as a ciphertext using homomorphic encryption. Upon receiving, the prompting party will apply homomorphic encryption on their symptoms as well, then a series of calculations and message exchanging will result in a value (λ) that would decide whether the symptoms are similar or not. Such decision is made by comparing λ to a threshold value set by the prompting party. If λ is greater than the threshold then the symptoms are considered similar, otherwise not.

With the described model, a high degree of enhancement in medical care services is expected by allowing physicians to monitor their patients from distance, and detect distress situations as they happen to offer immediate help. The proposed system also provides a diagnosing tool which aids in speeding up the diagnosis process with accuracy.

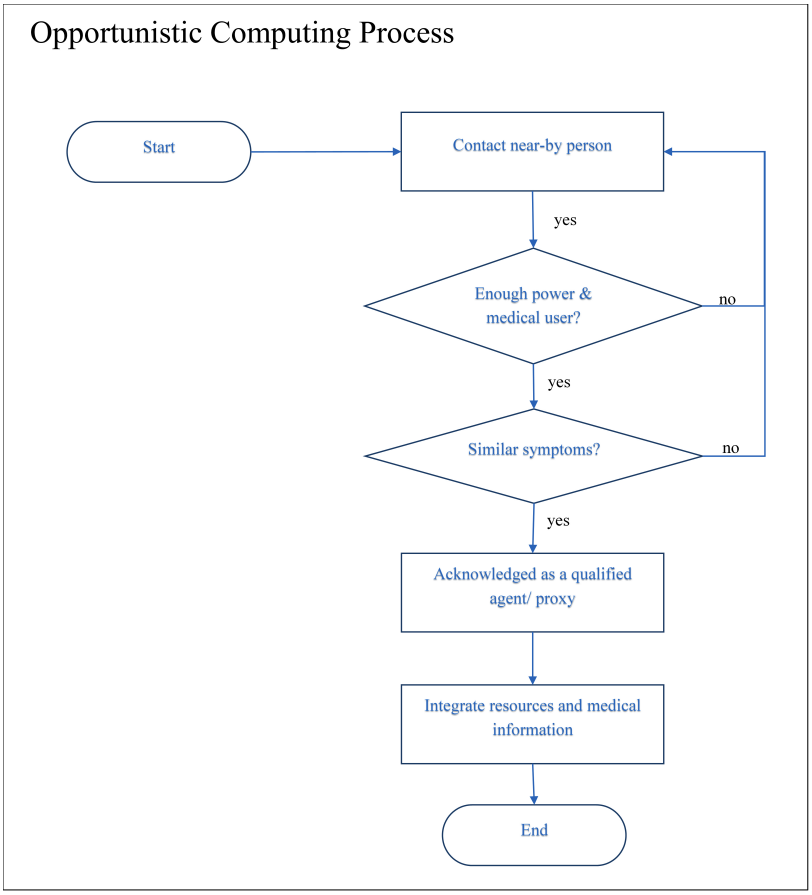

Figure 9. Opportunistic computing process.

5. Motivational Example

This section describes the motivating case study that will be used throughout the paper. Consider Dr. Alice who is a doctor in Hospital H, and Bob who is a patient in Dr. Alice's clinic. Every time Bob visits Dr. Alice, his vital signs are taken, and he is prompted to describe how he feels. Dr. Alice then is going to apply her knowledge to determine Bob's condition. Suppose on one visit, Bob's complained about continuous need for urination, micturition pain, and burning of urethra; he also denied nausea, and lumber pain. Consecutively, Dr. Alice will employ her knowledge base to diagnose Bob's condition; in which it would lead her to inflammation of urinary bladder disease. However, these symptoms could be shared by other diseases.

5.1. Motivating Scenario of the Single Decision Tree (SDT) Model

In Section 9, we have described a scenario where Dr. Alice would diagnose Bob based on her knowledge base. In this section, we describe the case study of the single decision tree model; where we show how three hospitals will collaborate to built the SDT model. Consider the three datasets in **Figure 10** for Hospital 1, Hospital 2, and Hospital 3 respectively. The datasets have five attributes, Nausea, Lumber pain, Urine pushing, Micturition pains, and Burning of urethra; and

Hospital 1:

#	Nausea	Lumbar pain	Urine pushing	Micturition pains	Burning of urethra	Class
1.	0	1	0	0	0	0
2.	0	1	0	0	0	0
3.	0	1	1	0	1	1
4.	0	0	0	0	0	0
5.	0	0	1	1	1	2
6.	1	1	1	1	0	3

Hospital 2:

#	Nausea	Lumbar pain	Urine pushing	Micturition pains	Burning of urethra	Class
1.	0	0	1	1	1	2
2.	0	0	1	0	0	2
3.	0	1	0	0	0	0
4.	0	0	1	0	0	2
5.	0	0	0	0	0	0
6.	0	1	0	0	0	0
7.	1	1	1	1	0	3
8.	0	1	1	0	1	1
9.	1	1	0	1	0	1

Hospital 3:

#	Nausea	Lumbar pain	Urine pushing	Micturition pains	Burning of urethra	Class
1.	0	1	0	0	0	0
2.	0	0	1	1	0	2
3.	1	1	1	1	1	3
4.	1	1	1	1	0	3
5.	0	0	0	0	0	0
6.	0	1	1	0	1	1
7.	1	1	0	1	0	1

Figure 10. Hospitals datasets.

each example can be one of four classes, 0, 1, 2, and 3 (where 0 = no disease, 1 = Nephritis of renal pelvis origin, 2 = Inflammation of urinary bladder, 3 = Both diseases). To build a decision tree out of the concatenation of the former datasets without revealing to each other will require a third party. In this case a cloud will mediate and manage the process. First, Each hospital will count the required proportions needed to calculate the entropy and information gain at the cloud. Those proportions will be stored in a two-dimensional array for each attribute. The number of columns will be equal to the number of possible decision classes (in our case they are 4), and the number of rows is equal to the number of possible values for each attribute (in our case they are 2 for all attributes). Each cell value will represent the number of occurrences for each class with each attribute value. For example, consider the arrays in **Figure 11** for attribute Nausea at each hospital, they show that Hospital 1's dataset has three rows where Nausea = 0 and Class = 0. Furthermore, by summing the cell values of each array, the total size of the dataset is retrieved; and by summing the cell values for each column, the total number of occurrences for each class is retrieved. Therefore, these arrays hold different and valuable information useful for entropy and information gain calculations. Before each hospital sends out its array to the cloud, they will homomorphically encrypt them. There, the cloud will sum the values of the corresponding array cells; see **Figure 12** for an example. Because the array values are encrypted homomorphically, the cloud is able to perform calculations but cannot know the real values. Having an array for each attribute, the cloud can calculate the values it need to evaluate the entropy and information gain. Following the example of attribute Nausea we show below how the entropy and information gain are calculated. Equation (1) shows Quinlan's [40] general for mula for calculating the entropy, and Equation (2) shows the value of entropy in our example.

	Hospital 1			
	0	1	2	3
0	3	1	1	0
1	0	0	0	1

	Hospital 2			
	0	1	2	3
0	3	1	3	0
1	0	1	0	1

	Hospital 3			
	0	1	2	3
0	2	1	1	0
1	0	1	0	2

Figure 11. The 2-D array for attribute Nausea at each hospital.

	At the cloud			
	0	1	2	3
0	8	3	5	0
1	0	2	0	4

Figure 12. The 2-D array for attribute Nausea at the cloud after summing the values of corresponding array cells.

$$\text{Entropy}(D)=\sum_{i=1}^{n}\left(\frac{-\text{freq}(c_i,D)}{|D|}\cdot\log_2\frac{\text{freq}(c_i,D)}{|D|}\right) \tag{1}$$

where:

n = number of columns

$\text{freq}(c_i,D)$ = number of occurences of class i = sum of column i cell values

$|D|$ = dataset size = the sum of all array cell values therefore:

$$\begin{aligned}\text{Entropy}(D)&=\left(\frac{8}{22}\cdot\log_2\frac{8}{22}\right)-\left(\frac{5}{22}\cdot\log_2\frac{5}{22}\right)\\&\quad-\left(\frac{5}{22}\cdot\log_2\frac{5}{22}\right)-\left(\frac{4}{22}\cdot\log_2\frac{4}{22}\right)\\&=1.949\end{aligned} \tag{2}$$

It should be noted here, that all calculations are performed homomorphically; therefore, the cloud doesn't know the real values calculated. Afterwards, it will calculate the information gain using Equations (5) and (6).

$$\text{Entropy}_A(D)=\sum_{j=1}^{p}\frac{|a_j|}{|D|}\cdot\text{Entopy}(a_j) \tag{3}$$

$$IG(A)=\text{Entropy}(D)-\text{Entropy}_A(D) \tag{4}$$

where:

A : attribute name

p = number of attribute values = number of array rows

$|a_j|$ = number of occurences of value a_j of attribute A = sum of row j cell values therefore:

$$\begin{aligned}\text{Entropy}_{Nausea}(D)&=\frac{16}{22}\cdot\left[\left(\frac{-8}{16}\cdot\log_2\frac{8}{16}\right)-\left(\frac{3}{16}\cdot\log_2\frac{3}{16}\right)-\left(\frac{5}{16}\cdot\log_2\frac{5}{16}\right)\right]\\&\quad+\frac{6}{22}\cdot\left[\left(\frac{-2}{6}\cdot\log_2\frac{2}{6}\right)-\left(\frac{4}{6}\cdot\log_2\frac{4}{6}\right)\right]=1.3252\end{aligned} \tag{5}$$

$$IG(A)=\text{Entropy}(D)-\text{Entropy}_A(D)=1.949-1.3252=0.6238 \tag{6}$$

Repeating the same steps for each attribute we find that attribute "Urine pushing" has the maximum information gain value, and thus, the cloud will inform each hospital to split their data at that attribute and repeat the above steps for each subset of the dataset. The final result will be the generation of one SDT at each hospital site. **Figure 13** shows the final decision tree.

Now going back to Dr. Alice and Bob, and tracing the tree with Bob's symptoms (Nausea = 0, Lumber pain = 0, Urine pushing = 1, micturition pain = 1, Burning of Urethra = 1), Dr. Alice can confirm the inflammation of urinary bladder disease.

5.2. Motivating Scenario of the Privacy-Preserving Emergency Call System (PPECS)

Continuing with the example in Section 9, we assume Dr. Alice wants to keep an eye on Bob to monitor his heart condition, but without checking him in the hos-

pital. Therefore, Bob will be equipped with WBS to monitor his vital signs, such as his pulse rate and blood tension (**Figure 14(a)**). Then, his PDA will be equipped with an application that will receive the transmitted vital signs via Bluetooth (**Figure 14(b)**). The PDA will periodically process the received data and transmit the results to the care giver via WiFi and GSM (**Figure 14(c)**). Furthermore, the vital signs will be encrypted to keep them safe from adversaries (**Figures 14(d)**, **Figure 14(e)**). Finally, the package containing the vital signs will be decrypted by the physician at the hospital (**Figure 14(f)**). Now, Dr. Alice can detect when Bob is going through a distress situation, and can send an ambulance to his location.

Suppose Bob was living far away from the hospital, or he went through an episode in location not near the hospital. To insure he receives the needed first aid

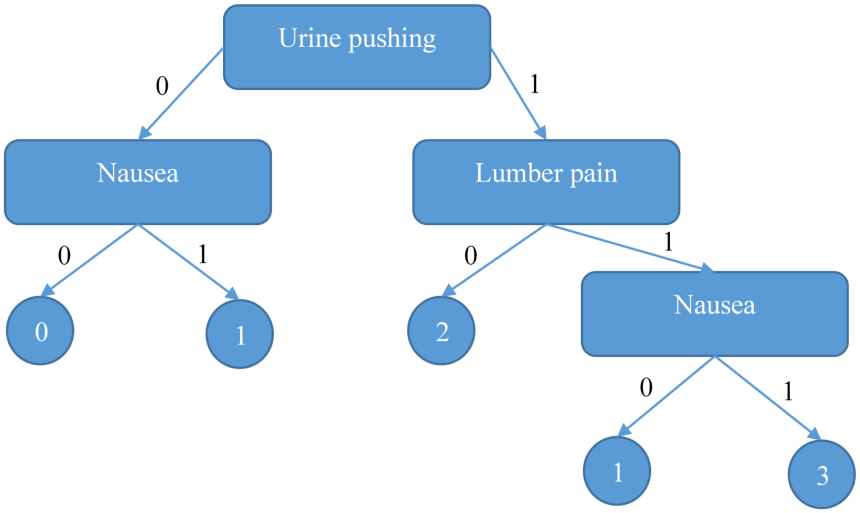

Figure 13. The decision tree generated by collaborating hospitals.

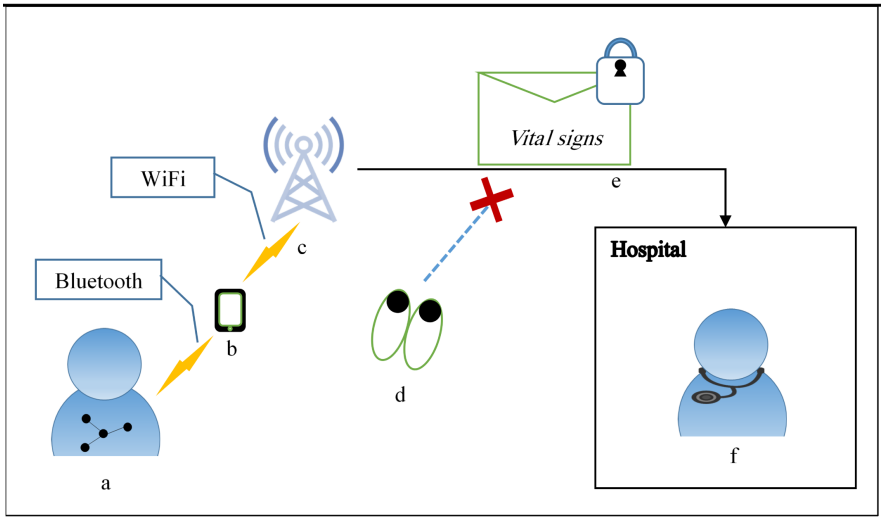

Figure 14. Remote Patient Monitor System. (a) Patient equipped with WBS; (b) patient's PDA; (c) GSM tower; (d) adversary; (e) encrypted vital signs; (f) hospital's physician.

as quickly as possible, the PDA application will feature a mobile health social network. This social network will exclusively include physicians, paramedics, and patients. Beside the social aspect of this network where patients may connect together and support each other; in a distress situation, a call for help could be broadcast to all users in the area. Because Bob's health record will be sent along with the call for help, he may have a preference on who should come for help, a physician, a paramedic, and/or another patient. Furthermore, he may decide how much can a receiver read from his health information. Therefore, at setup time, Bob will set the order of who he prefers to come fore help, and what information can he see. In **Figure 15** we can see that Bob have set the order to physician, paramedic, then patient. Where a physician can see his Health Record (HR) and the Physical Condition (PC), a paramedic can only read the PC, and a patient isn't allowed to see either.

Now we consider the case where Bob has a heart attack in his house (**Figure 16(a)**). His PDA will immediately send a call for the ambulance to the hospital,

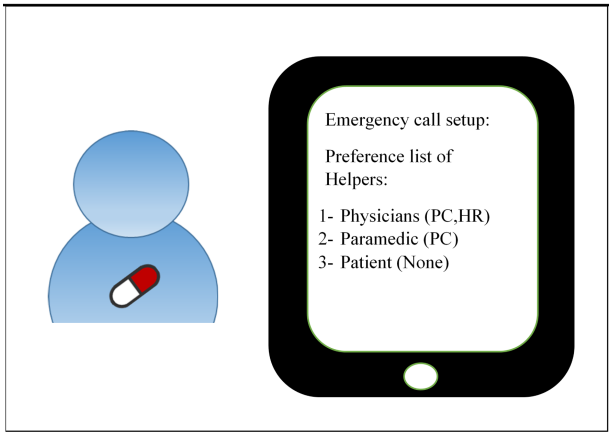

Figure 15. PDA setup for Bob's preference list of helpers.

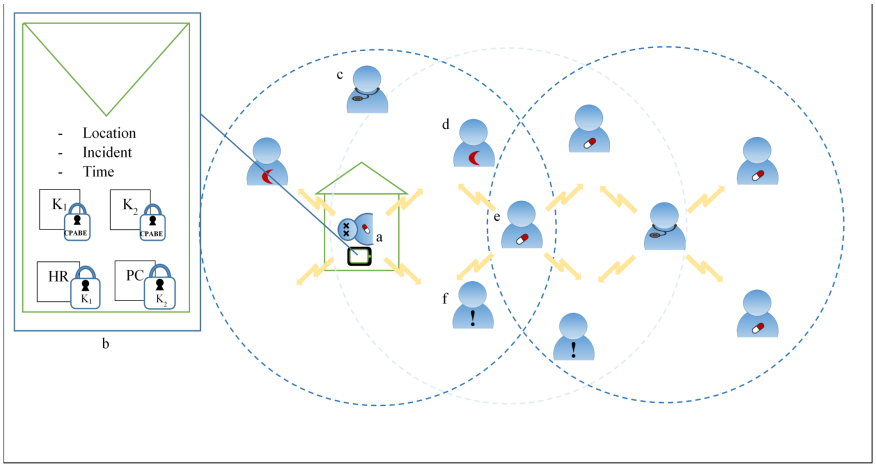

Figure 16. Emergency Call System. (a) Bob having a heart attack at home; (b) the call for help package prepared by Bob's PDA; (c) a physician; (d) a paramedic; (e) another patient; (f) not a user of the social network.

and then prepare the package in Figure 16(b). The package contains information on Bob's location, incident, and time. It also contains the HR and PC encrypted with two different keys, K_1 and K_2 respectively. And each key is encrypted using CPABE, where each is attached with the attributes of the subjects who are allowed to see the encrypted information. for example, in this case, K_1 will be attached with attribute physician, and K_2 will be attached with attributes physician, paramedic, according to Bob's Preference list (Figures 17(d)-(f)). The package will be broadcast in the area around Bob, and every social network user who receives this package will re-broadcast it to widen the area of search (Figure 16). Depending on the type of the receiver a certain action will be taken:

1) Physician: because Bob during setup have chosen for physicians to be allowed to view the HR and PC, any physician will be able to decrypt K_1 and K_2, and use them to decrypt HR and PC respectively (Figure 17(a)).

2) Paramedic: According to Bob's preference list, a paramedic can only view the PC; and therefore, they would only be able to decrypt K_2, and with it they will decrypt the PC (Figure 17(b)).

3) Patient: Bob didn't wish to have other patients as helpers, that's why, no patient in the area will be able to decrypt any of the keys (Figure 17(c)).

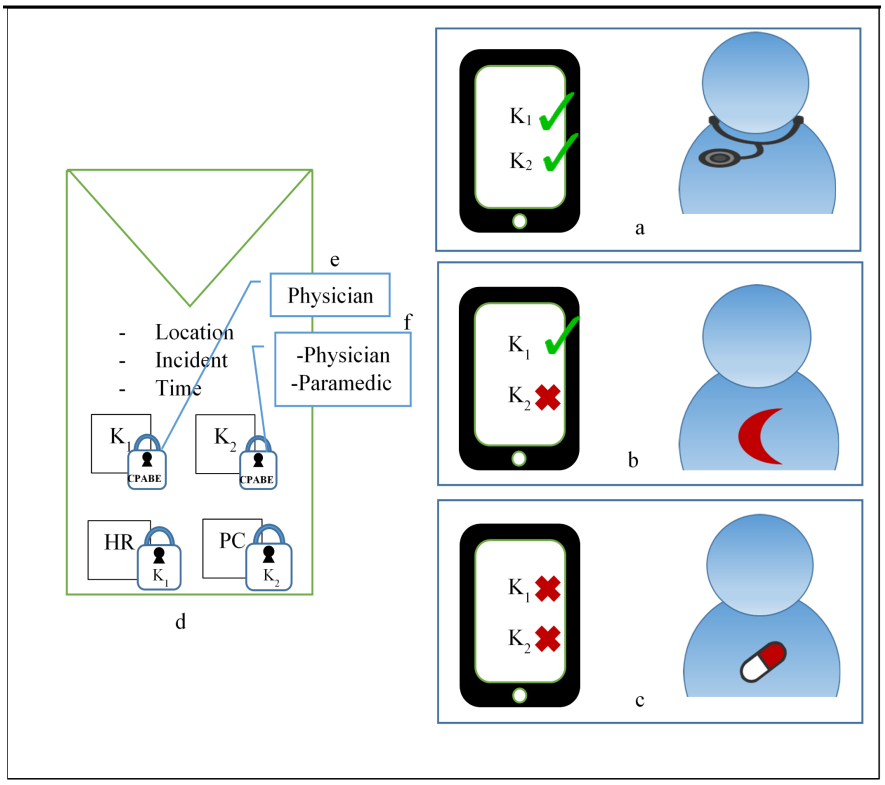

Figure 17. Different Actions of Receivers. (a) Physician's access privileges; (b) paramedic's access privileges; (c) patient's access privileges; (d) package generated by Bob's PDA; (e) attributes attached to the encrypted key K_1; (f) attributes attached to the encrypted key K_2.

Assuming the physician and paramedic in **Figure 16(c)** and **Figure 16(d)** have received the package. Both will immediately send a request for an ambulance. After decrypting the keys their attributes are attached to, they will use them to decrypt the corresponding ciphertext (HR, PC). On their way to the patient's location, they will review his information to deliver the proper first aid upon their arrival.

6. Conclusion

Due to the efficiency technology have added to healthcare services, caregivers tend to use systems such as CDSS and MHSN to enhance their performance and patients' experience. Furthermore, PHI are transmitted through the network as part of these systems' features. However, this imposes a threat on PHI for being exposed to different attacks. In this work, we have proposed a privacy preserving healthcare system, which is consisted of two subsystems, PPCDSS and PPECS. The former provides a privacy-preserving CDSS with decision trees, and the latter provides a privacy-preserving MHSN for monitoring patients' current condition from a distance. We will simulate our model using simulation tools, then analyze and discuss the results. Moreover, we expect our model to provide a privacy-preserving environment for transmitting PHI over the network, and for building a decision tree model and randomized versions of it without disclosing patients' information. Furthermore, Implementing and testing our system's performance and efficiency will allow us to compare it to other related work in terms of secrecy, and verify it through security analysis.

References

[1] Berner, E.S. and La Lande, T.J. (2007) Overview of Clinical Decision Support Systems. In: *Clinical Decision Support Systems*, Springer, Berlin, 3-22.

[2] Liang, X., Lu, R., Chen, L., Lin, X. and Shen, X. (2011) PEC: A Privacy-Preserving Emergency Call Scheme for Mobile Healthcare Social Networks. *Journal of Communications and Networks*, **13**, 102-112.

[3] Liu, X., Lu, R., Ma, J., Chen, L. and Qin, B. (2015) Privacy-Preserving Patient-Centric Clinical Decision Support System on Nave Bayesian Classification. *IEEE Journal of Biomedical and Health Informatics*, 1.

[4] Lu, R., Lin, X. and Shen, X. (2013) SPOC: A Secure and Privacy-Preserving Opportunistic Computing Framework for Mobile-Healthcare Emergency. *IEEE Transactions on Parallel and Distributed Systems*, **24**, 614-624.

[5] Vaidya, J., Shafiq, B., Fan, W., Mehmood, D. and Lorenzi, D. (2014) A Random Decision Tree Framework for Privacy-Preserving Data Mining. *IEEE Transactions on Dependable and Secure Computing*, **11**, 399-411. https://doi.org/10.1109/TDSC.2013.43

[6] Kevin, L. (2010) One Patient, One Record: Report on One-Day Symposium to Promote Patient e-Health. Technical Report, Ottawa.

[7] Ledley, R.S. and Lusted, L.B. (1959) Reasoning Foundations of Medical Diagnosis; Symbolic Logic, Probability, and Value Theory Aid Our Understanding of How Physicians Reason. *Science*, **130**, 9-21. https://doi.org/10.1126/science.130.3366.9

[8] Musen, M.A., Middleton, B. and Greenes, R.A. (2014) Clinical Decision-Support Systems. In: Shortliffe, E.H. and Cimino, J.J., Eds., *Biomedical Informatics*, Springer, London, 643-674.

[9] Berner, E.S. (2009) Clinical Decision Support Systems: State of the Art. AHRQ Publication, 4-26.

[10] Kaplan, B. (2001) Evaluating Informatics Applications Ome Alternative Approaches: Theory, Social Interactionism, and Call for Methodological Pluralism. *International Journal of Medical Informatics*, **64**, 39-56.

[11] Miller, P.L. and Sittig, D.F. (1990) The Evaluation of Clinical Decision Support Systems: What Is Necessary versus What Is Interesting. *Informatics for Health and Social Care*, **15**, 185-190.

[12] Zhou, J., Cao, Z., Dong, X., Xiong, N. and Vasilakos, A.V. (2015) 4S: A Secure and Privacy-Preserving Key Management Scheme for Cloud-Assisted Wireless Body Area Network in M-Healthcare Social Networks. *Information Sciences*, **314**, 255-276. https://doi.org/10.1016/j.ins.2014.09.003

[13] Kim, J., Beresford, A.R. and Stajano, F. (2007) Towards a Security Policy for Ubiquitous Healthcare Systems (Position Paper). In: *Ubiquitous Convergence Technology*, Springer, Berlin, 263-272.

[14] Rajeswari, A. and Shanmugapriya, S. An Efficient Mobile Health Care Emergency Services.

[15] Lu, R., Lin, X., Liang, X. and Shen, X.S. (2010) Secure Handshake with Symptoms-Matching: The Essential to the Success of M-Healthcare Social Network. In: *Proceedings of the 5th International Conference on Body Area Networks*, ACM, New York, 8-15. https://doi.org/10.1145/2221924.2221927

[16] Warner, H.R. (1961) A Mathematical Approach to Medical Diagnosis: Application to Congenital Heart Disease. *JAMA*, **177**, 177. https://doi.org/10.1001/jama.1961.03040290005002

[17] Schurink, C., Lucas, P., Hoepelman, I. and Bonten, M. (2005) Computer-Assisted Decision Support for the Diagnosis and Treatment of Infectious Diseases in Intensive Care Units. *The Lancet Infectious Diseases*, **5**, 305-312. https://doi.org/10.1016/S1473-3099(05)70115-8

[18] Zhan, J. (2007) Using Homomorphic Encryption for Privacy-Preserving Collaborative Decision Tree Classification. *IEEE Symposium on Computational Intelligence and Data Mining*, 637-645. https://doi.org/10.1109/CIDM.2007.368936

[19] Du, W. and Zhan, Z. (2002) Building Decision Tree Classifier on Private Data. In: *Proceedings of the IEEE International Conference on Privacy, Security and Data Mining*, Australian Computer Society, Inc., Vol. 14, 1-8.

[20] Bost, R., Popa, R.A., Tu, S. and Goldwasser, S. (2015) Machine Learning Classification over Encrypted Data. NDSS.

[21] Lindell, Y. and Pinkas, B. (2000) Privacy Preserving Data Mining. In: *Advances in Cryptology*, Springer, Berlin, 36-54. https://doi.org/10.1007/3-540-44598-6_3

[22] Lindell, Y. and Pinkas, B. (2002) Privacy Preserving Data Mining. *Journal of Cryptology*, **15**, 177-206. https://doi.org/10.1007/s00145-001-0019-2

[23] Emekçi, F., Sahin, O.D., Agrawal, D. and El Abbadi, A. (2007) Privacy Preserving Decision Tree Learning over Multiple Parties. *Data & Knowledge Engineering*, **63**, 348-361. https://doi.org/10.1016/j.datak.2007.02.004

[24] Bethencourt, J., Sahai, A. and Waters, B. (2007) Ciphertext-Policy Attribute-Based Encryption. *IEEE Symposium on Security and Privacy*, 321-334.

https://doi.org/10.1109/SP.2007.11

[25] Cheung, L. and Newport, C. (2007) Provably Secure Ciphertext Policy ABE. In: *Proceedings of the* 14*th ACM Conference on Computer and Communications Security*, ACM, New York, 456-465. https://doi.org/10.1145/1315245.1315302

[26] Goyal, V., Jain, A., Pandey, O. and Sahai, A. (2008) Bounded Ciphertext Policy Attribute Based Encryption. In: *Automata*, *Languages and Programming*, Springer, Berlin, 579-591.

[27] Waters, B. (2011) Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization. In: *Public Key Cryptography-PKC* 2011, Springer, Berlin, 53-70.

[28] Yu, M. and Xu, Q. (2012) A Simple and Effective Scheme of Ciphertext-Policy ABE. 8*th International Conference on Computational Intelligence and Security*, 516-519. https://doi.org/10.1109/CIS.2012.122

[29] Gentry, C., *et al.* (2009) Fully Homomorphic Encryption using Ideal Lattices. STOC, Number 2009, 169-178. https://doi.org/10.1145/1536414.1536440

[30] Gentry, C. (2009) A Fully Homomorphic Encryption Scheme. PhD Thesis, Stanford University.

[31] Brakerski, Z., Gentry, C. and Vaikuntanathan, V. (2014) (Leveled) Fully Homomorphic Encryption without Bootstrapping. *ACM Transactions on Computation Theory*, **6**, 13. https://doi.org/10.1145/2633600

[32] Brakerski, Z. and Vaikuntanathan, V. (2011) Efficient Fully Homomorphic Encryption from (Standard) LWE. 52*nd Annual Symposium on Foundations of Computer Science*, 97-106.

[33] Khedr, A., Gulak, G. and Vaikuntanathan, V. (2016) SHIELD: Scalable Homomorphic Implementation of Encrypted Data-Classifiers. *IEEE Transactions on Computers*, **65**, 2848-2858. https://doi.org/10.1109/TC.2015.2500576

[34] Liu, D. (2015) Practical Fully Homomorphic Encryption without Noise Reduction. IACR Cryptology ePrint Archive, 468.

[35] Zhou, T., Yang, X., Zhang, W. and Wu, L. (2016) Efficient Fully Homomorphic Encryption with Circularly Secure Key Switching Process. *International Journal of High Performance Computing and Networking*, **9**, 417-422. https://doi.org/10.1504/IJHPCN.2016.080414

[36] Conti, M. and Kumar, M. (2010) Opportunities in Opportunistic Computing. *Computer*, **43**, 42-50. https://doi.org/10.1109/MC.2010.19

[37] Avvenuti, M., Corsini, P., Masci, P. and Vecchio, A. (2007) Opportunistic Computing for Wireless Sensor Networks. *IEEE International Conference on Mobile Ad Hoc and Sensor Systems*, 1-6.

[38] Kulkarni, N.R. and Terdal, S. (2013) Pervasive Monitoring of M-Health Care using Android.

[39] Xing, H., Chen, C., Yang, B. and Guan, X. (2013) SymMatch: Secure and Privacy-Preserving Symptom Matching for Mobile Healthcare Social Networks. *International Conference on Wireless Communications & Signal Processing*, 1-6.

[40] Quinlan, J.R. (2014) C4.5: Programs for Machine Learning. Elsevier.

Acronyms

Acronym	Explanation
CDSS	Clinical Decision-Support Systems
MHSN	Mobile Health Social Networks
PHI	Patient Health Information
PHR	Patients Health Record
PPCDSS	Privacy-preserving Clinical Decision-Support System
PPECS	Privacy-preserving Emergency Call System
WBAN	Wireless Body Area Network
WBS	Wireless Body Sensors
WBSN	Wireless Body Sensor Network