International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Implementation of Mobile-Healthcare using Cloud Computing with Access Control, Security and Privacy

Smitha Kr[1], Rajashekar SA[2]

[1, 2]Computer Science and Engineering & East West Institute of Technology, Bangalore India

Abstract: ***Distributed m-healthcare systems support for efficient patient treatment of high quality, but it brings about series of challenges in personal health information confidentiality and patient's identity privacy. Many existing data access control and anonymous authentication schemes inefficient in distributed m- healthcare systems. To solve the problem, in this paper, establish a novel authorized accessible privacy model (AAPM) based on this propose a patient self-controllable multi-level privacy-preserving cooperative authentication scheme (PSMPA). Distributed m-healthcare realizing three levels of security and privacy requirement and patients can authorizes physicians by setting an access tree supporting flexible threshold predicates.***

Keywords: Authentication; access control; security and privacy; distributed m-healthcare; access tree

1. Introduction

Distributed m-healthcare cloud computing concept has emerged in recent years. We can say that it is a patient centric model as overall control of patient"s data is with patient. Due to the high cost of building and maintaining data centers, third-party service providers provide healthcare service. But while using third party service providers there are many security and privacy risks in the system. In m-healthcare social networks, the personal health information is always shared among the patients located in respective social communities suffering from the same disease for mutual support, and across distributed healthcare providers equipped with their own cloud servers for medical consultant in distributed m-healthcare cloud computing systems, which part of the patients' personal health information should be shared and which physician their personal health information should be shared with have become two intractable problems demanding urgent solutions.

In recent years, the distributed m-healthcare is emerged paradigm for exchanging the health information and allows to create, manage and control her personal health data, which has made the storage, retrieval, and sharing of medical information more efficient in cloud computing. The WHO defines the Mobile Healthcare is an area of the electronic health and it provide the heath information and services over mobile technologies such as mobile phones and personal digital Assistants (PDAs).The personal health information is always shared among the patients suffering from the same disease, between the patients and physicians as equivalent counterparts or even across distributed healthcare providers for medical consultant. This kind of personal health information sharing allows each collaborating healthcare provider to process it locally with higher efficiency and scalability, greatly enhances the treatment quality, significantly alleviates the complexity at the patient side and therefore becomes the preliminary component of a distributed m-healthcare system.

However, it also brings about a series of challenges, especially how to ensure the security and privacy of the patients' personal health information from various attacks in the wireless communication channel such as eavesdropping and tampering. Main issue regarding the security is the access control of the patient's personal information.

In distributed m-healthcare cloud computing system, only the authorized physicians or institutions that can recover the patient's personal information during data sharing. Most patients are concerned about the confidentiality of their personal health information since it is likely to make them in trouble for each kind of unauthorized collection and disclosure. For example, the patients' insurance application may be rejected once the insurance company has the knowledge of the serious health condition of its consumers. Therefore, in distributed healthcare a system, which part of the patients' personal health information should be shared and which part of physicians should their personal health information be sharing is the main problem. Here, simultaneously achieving both security and confidentiality with high efficiency. In distributed m-healthcare systems, all the members can be classified into three categories:

- the directly authorized physicians who are authorized by the patients,
- the indirectly authorized physicians who are authorized by the directly authorized physicians for medical consultant or research purpose and
- the unauthorized persons.

In this paper, by extending the techniques of attribute based access control and designated verifier signatures on de-identified health information by realize three different levels of privacy-preserving requirement: only the physicians directly authorized by the patients can access the patients' personal health information and authenticate their identities simultaneously; the physicians and research staff indirectly authorized by patients cannot authenticate the patients' identities but recover the personal health information; while the unauthorized persons can obtain neither. The main objective of this paper summarized as follows.

- Need to implement the authorized accessible privacy model (AAPM) for the multi level privacy preserving reliable authentication.
- Establish to allow the patients to authorize corresponding privileges to different kinds of physicians located in distributed health care by setting an access tree supporting flexible threshold.
- A patient self controllable multilevel privacy preserving co-operative authentication needs to provide in the distributed m-health care cloud computing system which have three different levels of security and privacy requirement for the patient.

2. System Architecture

Basic Architecture of the E-health System

The basic e-healthcare system illustrated in Figure mainly consists of three components: body area networks (BANs), wireless transmission networks and the healthcare providers equipped with their own cloud servers. The patient's personal health information is securely transmitted to the healthcare provider for the authorized physicians to access and perform medical treatment.

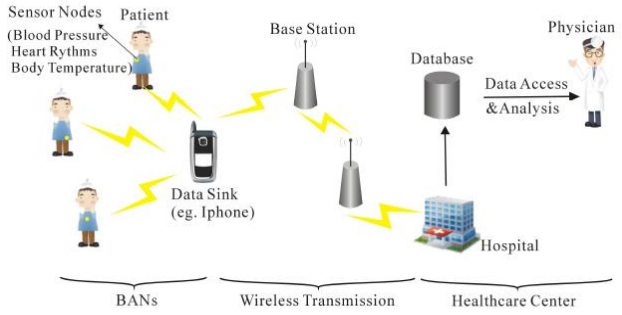

Figure 1: Basic Architecture of E-health System

Architecture of a Distributed m-Healthcare Cloud Computing System

The unique characteristics of distributed m-healthcare cloud computing systems where all the personal health information can be shared among patients suffering from the same disease for mutual support or among the authorized physicians in distributed healthcare providers and medical research institutions for medical consultation. A typical architecture of a distributed m-healthcare cloud computing system is shown in Figure . There are three distributed healthcare providers A,B,C and the medical research institution D, where Dr. Brown,Dr. Black, Dr. Green and Prof. White are working respectively. Each of them possesses its own cloud server. It is assumed that patient P registers at hospital A, all her/his personal health information is stored in hospital A's cloud server, and Dr. Brown is one of his directly authorized physicians. For medical consultation or other research purposes in cooperation with hospitals B,C and medical research institution D, it is required for Dr. Brown to generate three indistinguishable transcript simulations of patient P's personal health information and share them among the distributed cloud servers of the hospitals B,C and medical research institution D.

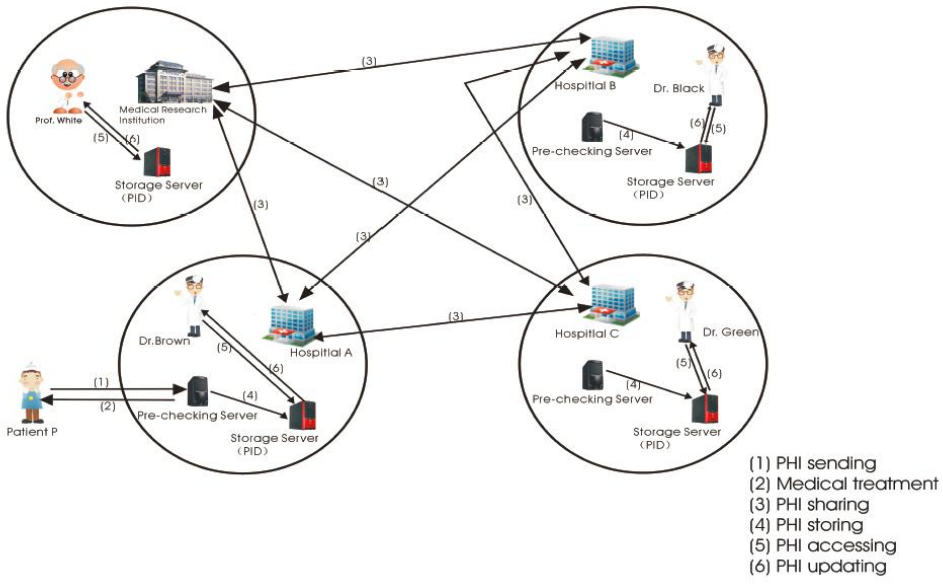

Figure 2: An Overview of Distributed m-Healthcare Cloud Computing System

3. Literature Survey

The previous studies, chiefly study the problem of information confidentiality within the central cloud computing architecture, contrarily leaving the difficult problem of realizing totally different security and privacy-preserving levels with respect to (w.r.t.) types of physicians accessing distributed cloud servers unresolved. Sun et. al. came with a solution for the privacy and emergency responses that are based on anonymous credential, pseudorandom number generator and proof of information.

Lu et. al. showcased a privacy-preserving authentication method in anonymous P2P systems considering Zero-knowledge Proof. The heavy computational overhead of Zero-Knowledge Proof makes it impractical once directly applied to the distributed m-healthcare cloud computing systems wherever the computational resource for patients is affected. Schechter et. al. projected an anonymous authentication of membership in dynamic teams, since the anonymous authentication mentioned above are established considering public key infrastructure (PKI), the requirement of an online certificate authority (CA) and one distinctive public key encryption for every symmetric key k for data encryption at the portal of authorized physicians formed the overhead of the construction grow linearly with size of the group.Finally, noticed that construction basically differs from the trivial combination of attribute based encryption (ABE) and designated verifier signature (DVS). Because the simulation results illustrate, simultaneously achieve the functionalities of both access control for personal health info and anonymous authentication for patients with significantly less overhead than the trivial combination of the 2 building blocks above. Therefore, PSMPA far outperforms the previous schemes in efficiently realizing access control of patients' personal health information and multi-level privacy-preserving cooperative authentication in distributed m-healthcare cloud computing systems

Few of the related works on the same proposed system are discussed below with the method and reason of failures.

1) Heart Failure monitoring system based on Wearable and Information Technologies [1]

In Europe, cardiovascular Diseases (CVD) can be seen as leading reason of death, which causes forty fifth of all deceases. Besides, failure of heart, the paradigm of CVD, principally affects individuals of age who fall over sixty five. In the present aging society, the European MyHeart Project was created, which had a mission to empower individuals to fight CVD by leading a preventive lifestyle and being able to be diagnosed at an early stage. Furthermore the paper presents the development of a heart failure Management System, considering daily observance of important Body Signals, with wearable and mobile technologies, for the continual assessment of this chronic disease.

a) Introduction: Now a days, heart failure (HF) could be a relatively common chronic disorder and is considered to be the paradigm of cardiac chronic diseases. The heart Failure Management System (HFMS) utilizes the most recent technologies to monitor the condition of heart, both with wearable garments (to measure ecg and Respiration); and moveable devices (such as Weight Scale and blood pressure Cuff) with Bluetooth capabilities. The important purpose of HFMS is to decrease the mortality and morbidity concerning the HF population.

The Front-end consists of the various textile sensors and electronics to record the important signals required by the application (ECG, Respiration and Activity).The User Interaction System (UIS), which relies on a personal digital assistant (PDA) device that receives data from the observation devices, processes it and encourages patients in the daily care of their heart. The Back-end, which incorporates the processing server and also the databases, manages the data gathered for each and every patient. The professionals will view and manage all data using a web access provided by a portal that relies on Cocoon Framework.

The timing tendency of data is automatically assessed so as to form sure an early detection of: a) attainable clinical de-compensations (clinical destabilization warning signs), b) continuous "out of hospital" arrhythmia risk stratification and, c) analysis of the HF progression. On the opposite hand, motivation methods were taken into consideration further to produce patients with pertinent and relevant information, in accordance with their physical and psychological situations.

b) Methods: The applied methodology relies on the goal directed design, within which the method may be bifurcated further into 5 iterative phases that are mentioned: research, Modeling, requirement, framework and Refinement.

Research Phase: In the due course of research phase, interviews to HF population, medical specialists (cardiologist and nurses) and business managers who are under the control of chronic problem area of hospitals, was carried out. In a span of 3 months within these interviews a mock-up system was validated completely. The validation was with respect to an open and close- ended questions then followed by the demonstration of system, furthermore permits the users for assessing the usability and comfort of the system.

In addition the system facilitates with security and confidence in individuals with HF, a rise within the quality of life boots the users to pay along with a smile on their face. Further, this system is perceived to result in an increase of productivity within the healthcare System. It doesn't prohibit the management of a larger range of individuals. Besides, this system boosts HF population to do moderated controlled amount of exercise, which helps a vital role in improving their quality of life and makes them alert to the importance of their healthcare. The system can create high expectations in users such as twenty four hours attention from physicians, which isn't the aim of such a system. The actual design isn't acceptable to the hot weather conditions. Moreover, some users have certain hindrance to tight garments. The system may be designed to include a better modularity, having the ability to offer different services to a various range of users, in function of their necessity.

Modeling Phase: Soon after the research phase, the Modeling phase generates both domain and user models, considering the input results from the above mentioned research phase. Domain models embody work flow diagrams. User models, or personal, are user archetypes that uphold the patterns of behavior, goals and motivations. They hold the awareness of their heart condition and are proactive to take a much better care. Moreover, they're ready to handle an electronic device, which is followed by an intuitive system. Besides, they do not have any special need in terms of accessibility (e.g. blind people).

Requirements Phase: The Requirements section utilizes scenario-based design strategies. End users will be prompted to obey a daily routine bifurcated into morning, exercise and before sleeping contexts. A context will be a collaboration of tasks (also named activities) to be performed along by the user at the same period of time throughout the day. As an example, a task or activity is the measurement of the blood pressure. And it may be done along with the weight measurement and also the morning questionnaire at the due course of the morning. Thus, all of them together will form up the morning context. The situations detected inside this system are 3. The first and third comprises a set of measurements, making use of the wearable garments and portable devices at home. Finally, the third situation sketches the professional interaction to assess the health status of their patients.

Framework Section: The analysis of the various situations is carried via an iterative refined context situation from the study of "day in the life" of the person throughout the Framework phase. The given daily routine is versatile enough to assemble for each respective patient. Further, the professional along with his patient can make a specific situation or routine relying on their desires and preferences. To check the system, a default routine for the user is scheduled on a fixed mode, so as to illustrate the functionality of the system. The professional accesses all data through the portal. The primary info that can be seen is an outline of each and every user emphasizing the foremost vital events. The professionals also can consult and edit the information related to a particular user and compare the present tendencies with those of previous weeks and months.

Refinement Phase: Thereafter the four previous phases, the Refinement phase takes the initiative to finalize with in depth documentation regarding all the necessities and specifications.

Advantages

- It has been proved that connectivity through the Internet and Web Services works as planned.
- Focuses on improvement of usability and minimizing interaction requirements giving the system more and more contextual awareness.

Disadvantages

- More studies about security issues need to be carried out.
- Future work encompasses the complete technical testing, clinical validation and a complete integration of data algorithms.

2) A Key Management Scheme in Distributed Sensor Networks Using Attack Probabilities [2]

For providing scalable data aggregation clustering approaches were found to be extra useful; security and coding for big scale Distributed sensor Networks (DSNs). Clustering (which is further named as sub-grouping) is more practical in containing and compartmentalizing node compromise in large scale networks. Additionally take into consideration the matter of designing a clustered DSN when the probability of node compromises in various deployment regions is understood a priori. Utilize a priori probability to design a variant of random key pre-distribution methodology that is capable enough to boost the resilience and conjointly the fraction of compromised communications compared to seminal works. in addition, relate the key ring size of the subgroup node to the probability of node compromise, and take a look at to design an efficient scalable security mechanism which will enhance the resilience to the attacks for the sensor subgroups.

a) Introduction: Mainly Distributed sensor Networks (DSNs) are widely utilized in several applications like real-time traffic monitoring, military sensing and tracking, wildlife observation and tracking, etc. DSNs are ad-hoc mobile networks that embody thousand of sensor nodes together with restricted computation and communications capabilities. DSN topology is dynamic and permits addition and deletion of sensor nodes after deployment. As a reason of the limited computation and communication capabilities of the sensor nodes, it is very difficult to bootstrap the establishment of a secure communications infrastructure from a set of sensor nodes which can have been pre-initialized with some secret info however has had no previous direct contact with one another.

To address the bootstrapping issue in DSNs, Eschenauer et al firstly projected the random key pre-distribution method that depends on probabilistic key sharing among the nodes of a DSN and uses easy and simple protocols for shared key discovery and path key establishment. The fundamental level of idea is that a random pool of keys is chosen from the key space. Then every sensor node receives a random subset of keys from the key pool before deployment. Any 2 nodes will be capable to find a standard key inside their individual subsets can use that key as their shared secret to initiate communication and to line up the secure connection.

Although previous schemes advised the employment of the random keys to build the secure connections between the nodes, the concept of various security requirements for various locations of nodes isn't taken into account.

The notable contributions of this projected paper are summarized within the following:

1) proposed a sub-grouping approach to isolate the effect of node captures into one specific subgroup, and to produce scalability for random key pre-distribution in DSN. Beneath the two-level hierarchical subgroup infrastructure, describe how to perform random key pre-distribution. Also analyze the corresponding performance metrics together with connectivity, resilience and fraction of compromised communications that are mentioned in later sections.

2) Came up with the concept of considering the probability of node compromise Pnc_i for each subgroup G_i so as to design a scalable security mechanism, such that resilience to the attacks for the sensor subgroup with larger probability of node compromise is improved. The proposed method will maintain flexibility in providing totally different security issues for various sensor subgroups.

b) Proposed Scheme

Subgrouping and random key predistribution: By utilizing the deployment information, the total N nodes group may be subdivide into different subgroups G_i, each

with Mi nodes, according to their deployment locations or the probability of node compromise as will be discussed in later sections. Different subgroup nodes will communicate with nodes in alternative subgroups through the controller node. Inside every subgroup G_i, This random key pre-distribution method consists of 3 phases, following the concept of the fundamental scheme, that are key pre-distribution, shared key discovery and path-key establishment. At the time of the key pre-distribution phase, a large key pool of S keys is first generated. Then randomly acquire mi keys out of S without replacement and store them into a key ring of each sensor node within the subgroup. The key identifiers of a key ring and also the associated sensor identifiers are saved by a controller node.

Probability of node compromise Pnc_i for a subgroup G_i: Since the sensor subgroups are located in different areas, they may have different chances of being attacked by the adversaries. Hence, as discussed, might actually assign different probability of node compromise Pnci into different subgroup Gi. The Pnci for a particular subgroup Gi, can also be defined as the normalized pre-assigned relative security weighting W_i of the subgroup G_i, i.e.

$$P\ nc_i = \frac{W_i}{\Sigma^{G}_{i=1} W_i}$$

The basic idea is that after the sub-grouping process, the whole network with N nodes is divided into G sub-groups; each contains Mi members according to their locations. Different Pnc_i values can be assigned to different subgroups and also vary the size of key ring in a node m_i for a particular subgroup G_i according to $P\ nc_i$. The objective is to improve the resilience R_i to that particular subgroup G_i . In this paper, R_i is defined as the probability that a given key in the subgroup G_i has not been compromised after x_i nodes in that subgroup are captured. Anyways, there is a tradeoff between the probability that a shared key exists between two sensor nodes p_i and the resilience R_i in that particular subgroup G_i

The random key pre-distribution scheme is to establish the secure connections between each sensor node within the sub-group. In fact, further use the same random key pre-distribution scheme to securely connect different controller nodes or different subgroups together 2. The objectives are to facilitate the efficient sub-grouping for the subgroup nodes and the controller nodes in each subgroup. It also simplifies the design of key distribution and management and provides scalability for node and subgroup addition or removal in the sensor network.

Advantages

- The cluster-based hierarchical topology not only isolates the effect of node compromise into one specific subgroup but even facilitates with scalability for node and subgroup addition.
- With a priori knowledge of the probability of node compromise, an effective scalable security mechanism that increases the resilience to the attacks for the sensor subgroups is designed.

Disadvantages

- Sacrifices a constant decrease of the probability that a shared key exists between two sensor nodes.
- Doesn't yield the expected results.

3) FDAC: Toward Fine-grained Distributed Data Access Control in Wireless Sensor Networks [3]

In recent years, to lend a supporting hand for numerous applications Distributed sensor information storage and retrieval has emerged with increasing significance. But on other side of a note distributed architecture enjoys an additional robust and fault-tolerant wireless sensor network (WSN), such design additionally poses a number of security challenges specifically once applied in mission-critical applications like battle field and e-healthcare. First, as sensor data are placed and maintained by individual sensors and unattended sensors are easily subject to strong attacks like physical compromise, it is significantly tougher to make sure data security. Second, in several mission-critical applications, fine-grained data access control is a must as illegal access to the sensitive data might cause fatal result and/or prohibited by the law. Last but not least, sensors typically are resource-scarce, which limits the direct adoption of costly cryptographic primitives. to deal with the above challenges, this method proposes a distributed data access control method that is capable enough fulfill fine-grained access control over sensor data and is resilient against strong attacks like sensor compromise and user colluding. The projected method exploits a completely unique cryptological primitive referred to as attribute-based cryptography (ABE), tailors, and adapts it for WSNs with reference to each performance and security needs.

a) Introduction: Wireless sensor networks (WSN) have been a space of significant research in recent years. A WSN sometimes consists of a large range of sensor nodes which will be easily deployed to other terrains of interest to sense the atmosphere. To accomplish the targeted application and fulfill its functionalities, a WSN typically generates a large quantity of data continuously over its life span. One among the biggest challenges then is how to store and access these sensed data.

Data storage and access in WSNs primarily follows 2 approaches, namely, centralized and distributed approaches. Within the centralized case, sensed data are collected from individual sensors and transmitted back to a central location, typically the sink, for storage and access. Within the distributed approach, when a sensor node has generated some data, it stores the information locally or at some selected nodes within the network, rather than instantly forwarding the data to a centralized location out of the network.

Compared to the centralized case, distributed data storage and access consumes less bandwidth since sensed data aren't any longer essentially transmitted to a centralized location out of the network. As energy-efficient storage devices are now attainable to be equipped with sensor nodes due to recent advances in IC manufacturing, reading data from local storage becomes far more efficient than sending over radio. Employment of distributed data storage and access therefore conjointly implies energy-efficiency.

As large amounts of sensed information are distributed and stored in individual sensor nodes, data security naturally becomes a very important concern. Actually, in several application situations data sensed by WSNs are closely associated with security and/or privacy problems and will be accessible solely to approved users. Moreover, in a mission-critical application situation numerous kinds of data generated by every kind of sensors might belong to different security levels, and thus are meant to be accessed solely by selected types of users. That is, accessibility of a specific style of data to users is predicated solely on necessity.

To provide distributed data access control, a naive resolution is to equip every sensor node with an access control list (ACL) as is typically adopted in wired networks. Upon each data access request, the sensor node verifies the user's identity with the ACL, and therefore the access request is approved as long as the user is within the list. Anyways, this naive solution will not be applicable to WSNs due to the subsequent facts. First, sensor nodes are usually deployed without any physical protection and lack of tamper- resistant hardware. Attackers might capture and compromise sensor nodes, and then scan historical data stored within the sensor nodes. Second, the ACL methodology is not scalable as it needs the sensor nodes to recollect each and every legitimate user. Naturally shift the attention to data encryption which might introduce 2 branches, namely symmetric key cryptography (SKC) based approaches and public key cryptography (PKC) based ones.

In SKC based approaches, data encryption and decryption share identical key. If the offender has compromised the sensor node, he is able to read the data encryption key kept in the sensor's memory and thus decrypt the historical data generated by the same identical sensor. To avoid this type of attacks, a natural throughway is to divide the lifetime of each and evey sensor into series of periods, and the data encryption keys for these periods are free of each other. Anyways, current SKC based approaches have 2 major drawbacks: first, fine-grained data access control is tough to understand because of the complexness introduced by key management; second, collusion attacks are doable given a proper number of colluding users. Hence, additional research remains desired for fine-grained distributed data access control utilising SKC based approaches.

PKC-based approaches will facilitate with better data access security than their SKC-based peers. In such approaches, sensor nodes encrypt the data items with public keys. One apparent advantage of this is that if data storage sensors are compromised, the attacker won't be able to recover the stored data because of lack of the corresponding personal keys. Hence, by applying PKC-based approaches to data access control in WSNs, can immediately get pleasure from the right resilience against sensor compromise. Anyways, for the purpose of distributed data access control in WSNs, the basic encryption paradigm is one-to-many such that one encrypted data item can be decrypted by a number of different approved users. To attain this goal, a simple approach is to use one-to-one public key cryptosystems, which is clearly inefficient since both the number of encryption operations and the size of cipher texts are linear to the overall number of approved users.

From the above discussion, it's clear that achieving fine-grained data access control with efficiency is still an open challenge in WSNs. In order to address this challenge, this paper showcased a Fine-grained Distributed data Access control method, particularly FDAC, specially tailored for WSNs. Base design on the observation of the inherent nature of the sensor data. As WSNs are generally deployed for specific application(s), it is typically simple and convenient to specify individual sensors (and hence their collected data) through a group of pre-defined attributes like sensor type, location, time, owner. Propose to associate each and every attribute of sensor nodes with a pre-defined keying material. And then, additional examine each and every user of the WSN with reference to their data access privileges and associate him with an access structure consequently. Such an access structure indesign is enforced via an access tree that specifies the categories of data that this user is authorized to access. Sensor data are then protected by being encrypted beneath their attributes such that solely the users whose access structures satisfy the desired data attributes can decrypt. In the access structure, every leaf node maps to a sensor/data attribute, and also the interior nodes will be threshold gates.

This resolution has many benefits. First, FDAC is efficient in terms of key storage, computation and communication overhead in the sensor node side. Second, it is resistant against user collusion, i.e., the cooperation of colluding users won't cause the revelation of extra sensor data. Last but not least, FDAC provides economical user revocation via a single broadcast, and the length of the broadcast message is just of several hundred bits.

In summary, This method makes the subsequent contributions. 1) It introduces the fine-grained data access control issue for the first time in WSNs. 2) FDAC applies and tailors KP- ABE to WSNs for achieving fined-grained access control. 3) The relevance of FDAC is demonstrated on the present generation of sensor nodes.

b) Models and Assumptions

Network Model: This work, take into account a wireless sensor network composed of a network controller that could be a trustworthy party, a large number of sensor nodes, and lots of users. Throughout this paper, will denote the network controller with the symbol T. Symbol U and N are utilized to represent the universe of the users and the sensor nodes respectively. Both users and sensor nodes have their distinctive and unique IDs. Symbol U_i are utilized to denote user i, and n_i is defined equally. The trusted party T may be on-line or off-line. It comes on-line just on necessity basis, e.g., in the case of intruders detected. Each and every sensor might be a high-end sensor node like iMote2 which has greater processing capability and a larger memory than typical sensor nodes. Sensor data might be stored locally or at some selected in-network location utilizing data storage schemes like TTDD.

Adversary Model: This work considers attackers whose main goal is to fetch sensor data that they're not approved to access. The adversaries might be either external intruders or

network users who are unauthorized to access the target sort of data. Because of lack of physical protection, sensor nodes are typically prone to strong attacks. Specifically, This take into account the adversary with both passive and active capabilities, which may eaves drop all the communication traffics within the WSN, and (2) compromise and control a little number of sensor nodes. Additionally, (3) unauthorized users might collude to compromise the encrypted data.

c) Security requirements

With relevance data access control in WSNs, it acknowledges the subsequent unique but not necessarily complete security needs.

Fine-grained data Access Control: As is mentioned in the previous section, fine-grained data access control is commonly desired by several mission-critical application situations. To facilitate fine-grained data access control, the projected method should give a technique that is ready to precisely specify the potential of various types of users to access sensor data of different sorts or security levels.

Collusion Resilience: As represented by the adversary model, unauthorized users might cooperate for the purpose of attaining the sensitive sensor network data. Hence, it is very much important to equip data access control method with the resilience against collusion attacks such that the cooperation of the unauthorized users won't offer them extra benefits over what they will directly get from executing attacks individually.

Sensor Compromise Resistance: Because of lack of compromise-resistant hardware, a little number of sensor nodes is inevitably to be compromised by the adversary in hostile environments. This method should at least secure sensor data such that, (1) compromising the sensor node doesn't disclose the sensor data generated before the sensor is compromised, and (2) compromising one sensor node doesn't offer the adversary any assistance to get sensor data generated by alternative sensor nodes.

Backward Secrecy: User management is a crucial functionality needed by most application situations. Particularly, the system should be ready to handle user revocation within the case of user leaving request or malicious behaviour detected.

d) FDAC: Fine-Grained Data Access Control Scheme

This section presents data access control scheme for distributed data storage.

Access Control Strategy: For the reason of achieving fine-grained data access control in WSNs, need to first explore the inherent natures of sensor networks. In general, the deployments of most WSNs are aimed toward data collection for specific application(s). Hence, will be ready to specify individual sensors (and hence the data collected by them) through a group of predefined attributes.

With the fine-grained access structures explicitly defined, the remaining is to hunt a way forcing the users to their specific pre-defined rules. to attain this, will predefine keying materials for each of the attributes, and encrypt sensor data beneath the keys corresponding to their attributes such that solely those whose access structures "accept"1 the data attributes are able to decrypt.

In FDAC, effort is created to associate each sensor node (and hence his collected data) a group of attributes, for each of that it define a public key. Every user is assigned an access structure, which is implemented via an access tree and embedded in the user secret key. Every leaf node of the access tree is labeled with an attribute and the interior nodes are threshold gates 2. Access structures are therefore ready to be represented using the logic expressions over the attributes. Specially, this type of definition allows access structures to represent sophisticated logic expressions, and be able to specify data access privileges of users in the fine-grained manner.

Sensor data later on are encrypted under the access structure such that only those whose attributes satisfy the access structure are able to decrypt. In this way, will be able to realize the same functionality in terms of the fine-grained data access control. Anyways, this strategy may not be applicable to WSNs due to the concerns on the performance in terms of computation and communication overload. In the proposed strategy, the complexity in terms of computation and communication overload is linear to the number of data attributes assigned to the sensor node. In practice, this complexity could be arguably low due to the fact that each sensor node (and hence their collected data) can be specified via a small number of attributes, though their universe in the whole network could be large. On the contrary, the complexity in the alternative strategy is determined by how complicated the access structure is.

e) Scheme Overview

In basic scheme, each sensor node is preloaded with a set of attributes as well as the public key PK. Each user is assigned an access structure and the corresponding secret key SK. The lifetime of the sensor network is divided into m stages, numbering as 1,2,⋯,m. The stage number is reset to 1 when it increases to m+1. Each period is further divided into n phases, numbering as 1, 2,⋯,n, where user can set $n < k$, $k = \max_{\forall i \in N} |Ii|$. Sensor nodes encrypt and store sensor data on the phase basis. For each sensor node, the sensor data are encrypted by symmetric encryption such as AES, and the data encryption keys during one stage form an one-way key chain, one data encryption key for each phase. Then will call the first key on this key chain by the master key, denoted by K. The master key of each stage is always generated during its preceding stage, and encrypted under the preloaded attributes. Upon request for sensor data, the sensor node responds with the encrypted master key as well as the ciphertext of the sensor data. If the user is an intended receiver, he is able to decrypt the master key and derive the data encryption key, and then obtain the sensor data. Based on the basic scheme, This advanced scheme goes one step further by providing the functionality of user revocation, which is demanded by most WSN application scenarios. In the advanced scheme, T is able to revoke any user via broadcasting a user revocation message to all the users and

all the sensor nodes respectively. In particular, the user revocation message for the sensor nodes contains merely a group element on G_T.

Advantages

- Each user is assigned an access structure which designates the access capability of the user.
- As the access structure is extremely expressive, it is able to control data access precisely, and thus achieve fine-grained access control.

Disadvantages

- There is a future gateway for the efficient implementation of FDAC on WSNS with low end sensor nodes.
- For low-end sensor nodes, Anyways, FDAC may be too expensive in terms of time cost and energy consumption.

4) A cross-platform model for secure Electronic Health Record communication [4]

During the past decade, there have been several regional, national and European projects focused on the enhancement of platforms for secure access and sharing of distributed patient info. A platform is required present local or enterprise-wide info systems are usually not meant for cross-organisational secure access of patient data. Most of the current secure platforms are local or regional. Usually used platform varieties in the health care atmosphere vary from secure point-to-point communication systems to internet-based portals. This paper defines an increased cross-security platform which makes it attainable for various types of local, regional, and national health info systems to have a communication in a secure manner. The projected evolutionary way interconnects regional or national security domains with the assistance of a cross-platform zone. An additional revolutionary model which is based on peer-to-peer Grid like networks and dynamic security credentials is additionally discussed. The projected evolutionary model uses cross-domain security and interloper ability services to make sure secure communication and inter operability between different security domains.

a) Introduction: E-health and telemedicine services are promising business areas in Europe. It is clear that e-health products and services will be sold and ordered from a distance and over national borders in the future. Typical cross-organisational e-health applications are:

- sharing of patient records among different healthcare professionals;
- access to distributed EHRs any place and any time;
- on-line tele-consultation, tele-monitoring and assistance;
- patient-doctor consultation services;
- Patient's access to their own EHRs.

The types of present health information systems vary from distributed to centralised systems. Most of the distributed systems are based on the messaging approach, Grid-like linking directory approach or are portals with clearinghouse functions. Centralised systems typically have one centralised patient repository.

E-health and telemedicine applications and services require not only cross-organisational but also trans-border data flow. At present, a few enterprise wide information systems have security services aimed at cross-organisational communication. In many cases, policy on trust, privacy and confidentiality is not harmonised even at national level.

b) Definitions: Security means that personal information can be communicated or stored in such a manner that access is limited to authorised parties. The security framework gives general rules and limitations for the processing of confidential health data. The security infrastructure defines components that support users or applications for exchanging sensitive information in a secure way. A PKI infrastructure is a typical secure infrastructure. Security platform means a platform where different health applications can run securely and exchange data and money privately. The most common security domain (a basic domain) is a health care unit or enterprise. When 2 or additional security domains share info, extra infrastructural security services are required. Cross-border communication forms the widest security domain. It makes it attainable to share sensitive info across borders in a trustworthy approach.

Elements of semantic inter operability are language, terminology and clinical coding, info structures, clinical protocols, and processes. With reference to interoperability levels of interoperability domain scanal so be distinguished. The fundamental domain exists at local or regional level. The foremost demanding level is that the cross-border interoperability domain.

c) Barriers for cross-organisational communication: The goal of a secure cross-organisational platform is to make communication possible between different platforms and across borders in spite of those barriers. The major security barriers are the lack of

- A harmonised legal and ethical framework;
- A harmonised policy on trust, privacy and confidentiality;
- Security services for trans-border communication;
- Common security standards.

d) Security requirements of an interoperable cross-platform model: It is rather unlikely or legally not possible for users from different organisations to understand or trust one another. Hence, there'll be a requirement of a mechanism to create trust between partners (organisations, persons and entities) and to fulfil security needs. As a result of a platform usually integrates 2 or more security domains having different internal security schemes, it has to facilitate common security bridging services for connected domains. The platform should additionally support both data transfer (e.g. messaging) and the data access modes of communication.

e) A proposed model for cross-platform security: Some current European projects have projected candidate solutions for secure inter-organisational communication and data sharing. One amongst the most attention-grabbing is the HARP model. Its original platform has been upgraded to a middle ware-like common secure cross-platform. For cross-

platform communication, the HARP project has defined an enhanced trusted Third Party (TTP) server with security policy mapping options. For internet access, the HARP model proposes that the user security profile, which determines all access rights within the client terminal, might be dynamically downloaded to the client.

This method proposes 2 attainable ways forward: an evolutionary and a revolutionary road. Within the evolutionary model initially must integrate enterprise-wide and regional platforms and form a national secure and interoperable platform. Thereafter, this stage will integrate different national platforms with the assistance of cross-platform security and interoperability services. The revolutionary platform could be a Grid-like peer network that dynamically connects national security domains. Security is archived through the utilization of digital credentials, with expanded attributes for dynamic access and privilege management control. The evolutionary model appears to be the foremost sensible cross-platform integration methodology. The platform integrates regional and national security domains with the assistance of an inter-domain zone. This zone offers common security and interoperability services for all connected domains. The platform can use existing PKI services for authentication where available. To make it possible for external (dynamic) users to access any of the EHRs inside connected domains, the platform can offer automatic security negotiation services. The interoperability services of the proposed platform consist of semantic services and EHR linking services. To make it possible to use local languages in communication, language clearinghouse services are included.

Advantages

- The method requires minimal changes to present legacy systems.
- It integrates present regional and national networks, and acts as a migration path to future.

Disadvantages

- It is rather unlikely or legally impossible for users from different organisations to know or trust each other.

4. System Requirement

Functional Requirements:

This project has the following modules

a) User (Physian, Hospital Admin, Patient etc)
b) Cloud Server
c) Health Care Provider

Algorithm: Advanced Encryption Standard (AES)

AES is based on a design principle known as a substitution-permutation network, combination of both substitution and permutation, and is fast in both software and hardware. Unlike its predecessor DES, AES does not use a Feistel network. AES is a variant of Rijndael which has a fixed block size of 128 bits, and a key size of 128, 192, or 256 bits. By contrast, the Rijndael specification per se is specified with block and key sizes that may be any multiple of 32 bits, both with a minimum of 128 and a maximum of 256 bits.

AES operates on a 4×4 column-major order matrix of bytes, termed the state, although some versions of Rijndael have a larger block size and have additional columns in the state. Most AES calculations are done in a special finite field. The key size used for an AES cipher specifies the number of repetitions of transformation rounds that convert the input, called the plaintext, into the final output, called the ciphertext. The numbers of cycles of repetition are as follows:

- 10 cycles of repetition for 128-bit keys.
- 12 cycles of repetition for 192-bit keys.
- 14 cycles of repetition for 256-bit keys.

Each round consists of several processing steps, each containing four similar but different stages, including one that depends on the encryption key itself. A set of reverse rounds are applied to transform ciphertext back into the original plaintext using the same encryption key.

High-level description of the algorithm

1. Key Expansions—round keys are derived from the cipher key using Rijndael's key schedule. AES requires a separate 128-bit round key block for each round plus one more.
2. Initial Round: Add Round Key—each byte of the state is combined with a block of the round key using bitwise xor.
3. Rounds

a) SubBytes—a non-linear substitution step where each byte is replaced with another according to a lookup table.

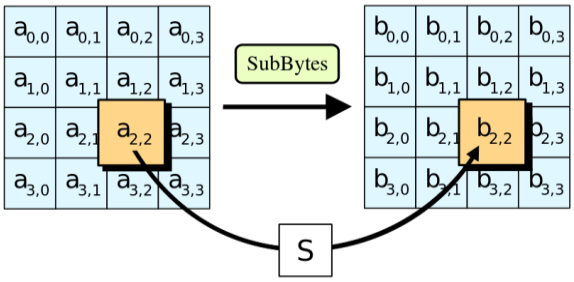

Figure1: SubBytes module

b) ShiftRows—a transposition step where the last three rows of the state are shifted cyclically a certain number of steps.

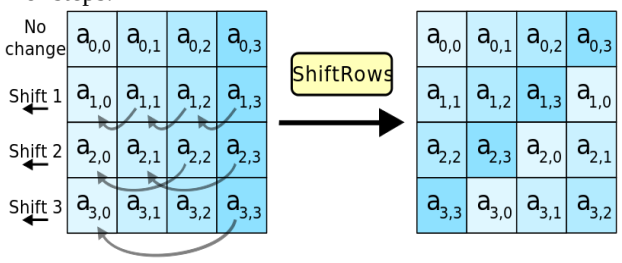

Figure 2: ShiftRow module

c) MixColumns—a mixing operation which operates on the columns of the state, combining the four bytes in each column.

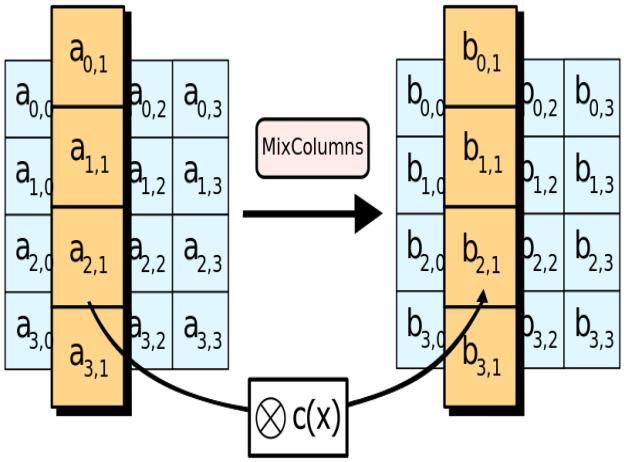

Figure 3: MixColumns module

d) AddRoundKey: In this step, each byte of the state is combined with a byte of the round subkey using the XOR operation

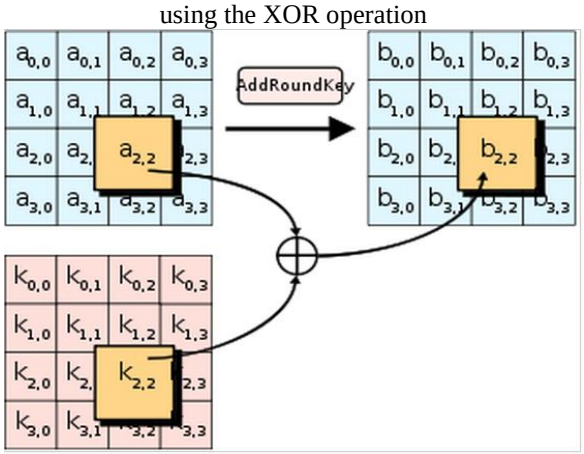

Figure 4: AddRoundKey module

5. Conclusion

In this paper, a novel authorized accessible privacy model (AAPM) and a patient self controllable multi-level privacy preserving cooperative authentication scheme (PSMPA) realizing three different levels of security and privacy requirement in the distributed healthcare cloud computing system are proposed, followed by the formal security proof and efficiency evaluations which illustrate our PSMPA can resist various kinds of malicious attacks and far outperforms previous schemes in terms of storage, computational and communication overhead.

References

[1] E. Villalba, M.T. Arredondo, S. Guillen and E. Hoyo-Barbolla, A New Solution for A Heart Failure Monitoring System based on Wearable and Information Technologies, In International Workshop on Wearable and Implantable Body Sensor Networks 2006-BSN 2006, April, 2006.

[2] J. Zhou and M. He, An Improved Distributed Key Management Scheme in Wireless Sensor Networks, In WISA 2008.

[3] S. Yu, K. Ren and W. Lou, FDAC: Toward Fine-grained Distributed Data Access Control in Wireless Sensor Networks, In IEEE Infocom 2009.

[4] J. Sun and Y. Fang, Cross-domain Data Sharing in Distributed Electronic Health Record System, IEEE Transactions on Parallel and Distributed Systems, vol. 21, No. 6, 2010.

[5] D. Slamanig, C. Stingl, C. Menard, M. Heiligenbrunner and J. Thierry, Anonymity and Application Privacy in Context of Mobile Computing in eHealth, Mobile Response, LNCS 5424, pp. 148-157, 2009.

[6] J. Zhou and Z. Cao, TIS: A Threshold Incentive Scheme for Secure and Reliable Data Forwarding in Vehicular Delay Tolerant Networks, In IEEE Globecom 2012.

[7] F.W. Dillema and S. Lupetti, Rendezvous-based Access Control for Medical Records in the Pre-hospital Environment, In HealthNet 2007.

[8] J. Sun, Y. Fang and X. Zhu, Privacy and Emergency Response in Ehealthcare Leveraging Wireless Body Sensor Networks, IEEE Wireless Communications, pp. 66-73, February, 2010.

[9] X. Lin, R. Lu, X. Shen, Y. Nemoto and N. Kato, SAGE: A Strong Privacy-preserving Scheme against Global Eavesdropping for Ehealth Systems, IEEE Journal on Selected Areas in Communications, 27(4):365-378, May, 2009.

[10] J. Sun, X. Zhu, C. Zhang and Y. Fang, HCPP: Cryptography Based Secure EHR System for Patient Privacy and Emergency Healthcare, ICDCS'11.

[11] L. Lu, J. Han, Y. Liu, L. Hu, J. Huai, L.M. Ni and J. Ma, Pseudo Trust: Zero-Knowledge Authentication in Anonymous P2Ps, IEEE Transactions on Parallel and Distributed Systems, Vol. 19, No. 10, October, 2008.