EXPLORATIONS ON SCIENCE LETTERS (ESL)
VOLUME 1, ISSUE 1 (2016):PP.7-13
SANA ACADEMIC PRESS

# Resistance Of Attacks In Patient M-Health Care System

**Yashmeen.A[1], Lina.S[2], Brindha .S[3]**
[1]*Research Scholar, St. Peter's University, Chennai.*
*yashmeen92@gmail.com*
[2]*Asst. Prof, Dept. of Computer Science & Applications, St. Peter's University, Chennai.*
[3]*Asst. Prof, Dept. of Computer Science & Applications, St. Peter's University, Chennai*

***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*

## I. 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.

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.

## II. MATERIAL AND 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.

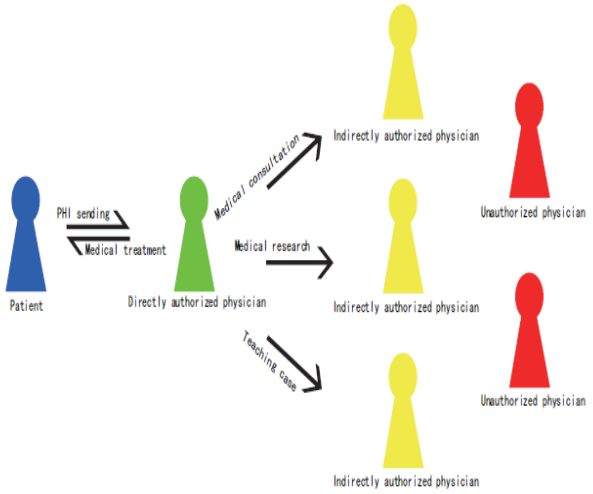
**Disadvantages**

- 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.

## III .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.




## IV. 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 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 failure

a) **Heart Failure monitoring system based on Wearable and Information Technologies** 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.

b) **A Key Management Scheme in Distributed Sensor Networks Using Attack Probabilities** 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.

c) **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 crypto logical primitive referred to as attribute-based cryptography (ABE), tailors, and adapts it for WSNs with reference to each performance and security needs.

## V. 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.

## VI. 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 behavior detected.

**Functional Requirements:** This project has the following modules
a) User (Phrygian, 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 Festal network. AES is a variant of Randal which has a fixed block size of 128 bits, and a key size of 128, 192, or 256 bits. By contrast, the Randal 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 Randal 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 cipher text. 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 cipher text 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 Randal'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 or.

3. Rounds

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

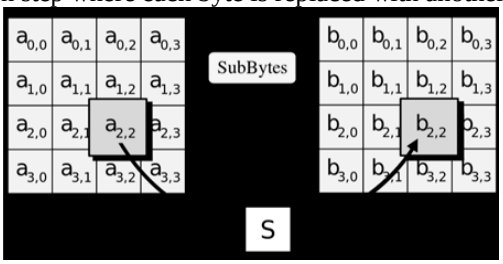



**Figure1:** Sub Bytes module.

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

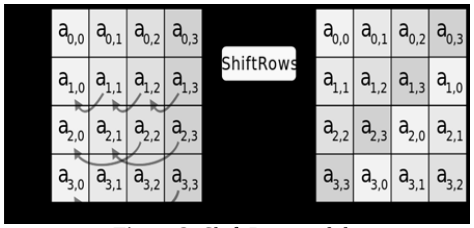



**Figure 2:** Shift Row module

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

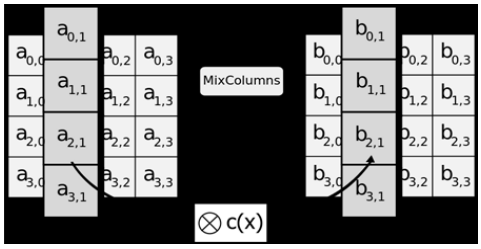
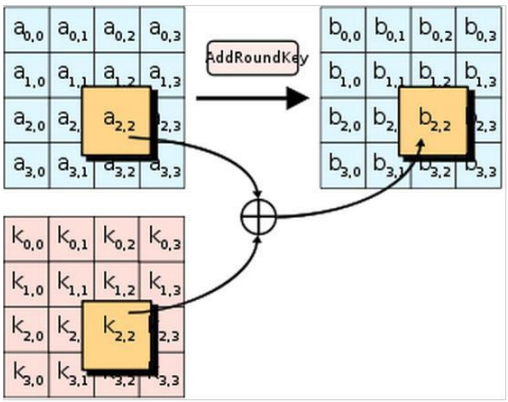



**Figure 3:** Mix Columns module

d) Add Round Key: In this step, each byte of the state is combined with a byte of the round sub key using the XOR operation.




## VII. 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. Villella, M.T. Arredondo, S. Guilin and E. Hobo- Barbell, 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. Rend and W. Lou, FDAC: Toward Fine-grained Distributed Data Access Control in Wireless Sensor Networks, In IEEE Nifco 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. Slamming, C. Stings, C. Menard, M. Heiligenbrunner and J. Thierry, Anonymity and Application Privacy in Context of Mobile Computing in healthy, 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. Dilemmas 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. H u, J. Hay, 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.
[12]. N. Cao, Z. Yang, C. Wang, K. Ran, and W. Lou, "Privacy-preserving query over encrypted graph-structured data in cloud computing," in Proc. 31st Int. Conf. Distrib. Comput. Syst., 2011, pp. 393–402.
[13]. F. Cao and Z. Cao, "A secure identity-based multi-proxy signature