Special Issue Published in International Journal of Trend in Research and Development (IJTRD), ISSN: 2394-9333, www.ijtrd.com

Mining Human Activity Patterns from Smart Home Big Data for Healthcare Application

[1]S.Anitha, [2]B.S.Sangeetha
[1]M.phil Scholar, [2]Head of the Department,
[1,2]Department Of Computer Science, Shri Sakthi kailassh Women's College, Salem, India

Abstract: The Distributed m-healthcare cloud computing system considerably facilitates secure and efficient patient treatment for medical consultation by sharing personal health information among the healthcare providers. This system should bring about the challenge of keeping both the data confidentiality and patients' identity privacy simultaneously. Many existing access control and anonymous authentication schemes cannot be straightforwardly exploited. To solve the problem proposed a novel authorized accessible privacy model (AAPM) is established. Patients can authorize physicians by setting an access tree supporting flexible threshold predicates. Our new technique of attribute based designated verifier signature, a patient self-controllable multi-level privacy preserving cooperative authentication scheme (PSMPA) realizing three levels of security and privacy requirement in distributed m-healthcare cloud computing system is proposed. The directly authorized physicians, the indirectly authorized physicians and the unauthorized persons in medical consultation can respectively decipher the personal health information and/or verify patients' identities by satisfying the access tree with their own attribute sets.

I. INTRODUCTION

Distributed m-healthcare cloud computing systems have been increasingly adopted worldwide including the European Commission activities, the US Health Insurance Portability and Accountability Act (HIPAA) and many other governments for efficient and high-quality medical treatment. 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 (HPs) equipped with their own cloud servers for medical consultant. 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 As to the security facet, one of the main issues is access control of patients' personal health information, namely it is only the authorized physicians or institutions that can recover the patients' personal health information during the data sharing in the distributed m-healthcare cloud computing system. In practice, 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.

Therefore, in distributed m-healthcare cloud computing systems, which part of the patients' personal health information should be shared and which physicians their personal health information should be shared with have become two intractable problems demanding urgent solutions. There has emerged various research results focusing on them. A fine-grained distributed data access control scheme is proposed using the technique of attribute based encryption (ABE). A rendezvous-based access control method provides access privilege if and only if the patient and the physician meet in the physical world. Recently, a patient-centric and fine-grained data access control in multi-owner settings is constructed for securing personal health records in cloud computing. However, it mainly focuses on the central cloud computing system which is not sufficient for efficiently processing the increasing volume of personal health information in m-healthcare cloud computing system.

Moreover, it is not enough for to only guarantee the data confidentiality of the patient's personal health information in the honest-but-curious cloud server model since the frequent communication between a patient and a professional physician can lead the adversary to conclude that the patient is suffering from a specific disease with a high probability. Unfortunately, the problem of how to protect both the patients' data confidentiality and identity privacy in the distributed m-healthcare cloud computing scenario under the malicious model was left untouched. In this paper, we consider simultaneously achieving data confidentiality and identity privacy with high efficiency. As is described in Fig. 1, in distributed m-healthcare cloud computing systems, all the members can be classified into three categories: the directly authorized physicians with green labels in the local healthcare provider who are authorized by the patients and can both access the patient's personal health information and verify the patient's identity and the indirectly authorized physicians with yellow labels in the remote healthcare providers who are authorized by the directly authorized physicians for medical consultant or some research purposes (i.e., since they are not authorized by the patients, we use the term 'indirectly authorized' instead). They can only access the personal health information, but not the patient's identity. For the unauthorized persons with red labels, nothing could be obtained. By extending the techniques of attribute based access control and designated verifier signatures (DVS) on de-identified health information

II. RELATED WORK

Lately, there has been a growing interest in using smart home technologies for detecting human activity patterns for health monitoring applications. The main goal is to learn occupants' behavioural characteristics as an approach to understand and predict their activities that could indicate health issues. In this section, we review existing work in the literature, which employ smart homes data to analyze users' behaviour. Detecting human activities in smart homes by means of analyzing smart meters data is studied in. The paper proposes two approaches to analyze and detect user's routines. One approach uses Semi-Markov-Model (SMM) for data training and detecting individual habits and the other approach introduces impulse based method to detect Activity in Daily Living (ADL) which focuses on temporal analysis of activities that happen simultaneously. Similarly, the work in proposes human activity detection for wellness monitoring of elderly people using classification of sensors related to the main

activities in the smart home. Smart meters data are also used in for activity recognition using Non-intrusive Appliance Load Monitoring(NALM) and Dumpster-Shafer (D-S) theory of evidence. The study collects pre-processed data from homes to determine the electrical appliance usage patterns and then employs machine learning-based algorithm to isolate the major activities inside the home. The issue is that the study has to perform two steps on the data to completely isolate the main activities. Exploiting appliance usage patterns and identifies them for sudden behavioural change is presented in. The aim of the study is to provide around the clock monitoring system to support people's suffering from Alzheimer or Parkinson disease at minimum intrusion level. The study uses classification techniques to detect abnormal behavior of personal energy usage patterns in the home. Other studies such as, and although do not utilize smart meters data; they use Internet of Things (IoT) infrastructures in smart cities for developing applications that monitor and provide health services for patients. Using data analytics for smart meters to detect and predict behavioral abnormality for remote health monitoring is discussed in. The authors in use everyday appliances usage from smart meter and smart plug data to trace regular activities and learn unique time segment groups of appliance's energy consumption. The study employs hierarchical probabilistic model-based detection to infer about discovered anomalous behavior. This in tern can be used to understand the criticality of some abnormal behaviors for sustaining better health care. In an experimental demonstration for observing and measuring energy consumption of appliances is presented. The study aims to provide a portrait profile of activities of daily living for elderly patients independently living at home. The data is also used to mine important patterns of changes for short-term and long-term anomaly detection of urgent health conditions. The work I, uses Bayesian networks to predict occupant behavior from collected smart meters data. The study proposes behavior as a service based on a single appliance, but does not provide a model to be applied for real-world scenarios. Authors in and, used time series multi-label classifier to forecast appliance usage based on decision tree correlations, however, the study takes only the last 24-hour window along with appliance sequential relationships. The authors in suggest a clustering approach to identify the distribution of consumers' temporal consumption patterns, however, the study does not consider appliance level usage details. This might not be applicable for human activity recognition since specific activities require individual and multiple appliance to appliance and time associations. The work in considers the appliances' ON and OFF status to detect usage pattern using hierarchical and c-means clustering. However, the study does not consider the duration of appliance usage or the expected variations in the sequence of appliance usage. The work in proposes graphical model based algorithm to predict human behavior and appliance interdependency patterns and use it to predict multiple appliance usages using a Bayesian model. The above-discussed approaches do not consider appliance level usage patterns, which is critical in determining human activity variations. Furthermore, our experiments are conducted using a much larger dataset than existing studies although there are similarities in data analytics techniques between the proposed study and existing work.

III. LITERATURE SURVEY

J. Misic and V. B. Misic, "Implementation of security policy for clinical information systems over wireless sensornetwork(2007) J. Misic and V. Misic, "Enforcing patient privacy in healthcare WSNs through key distribution algorithms,"(2008) M. Li, S. Yu, K. Ren, and W. Lou, "Securing personal health records in cloud computing: Patient-centric and fine-grained data access control in multi-owner settings,"(2010) J. Sun and Y. Fang, "Cross-domain data sharing in distributed electronic health record system,"(2010) R. Lu, X. Lin, X. Liang, and X. Shen, "A secure handshake scheme with symptoms-matching for mhealthcare social network,"(2011). A. Yassine, A. A. N. Shirehjini, and S. Shirmohammadi, "Smart meters big data: Game theoretic model for fair data sharing in deregulated smart grids,"(2015). A. Yassine and S. Shirmohammadi, "Measuring users' privacy payoff using intelligent agents," in (2009).]"A business privacy model for virtual communities,"(2009). Y. C. Chen, H. C. Hung, B. Y. Chiang, S. Y. Peng, and P. J. Chen, "Incrementally mining usage correlations among appliances in smart homes,"(2015). K. Jack and K. William, "The UK-DALE dataset, domestic appliance-level electricity demand and whole-house demand from five UK homes,"(2015).] J. Clement, J. Ploennigs, and K. Kabitzsch, Detecting Activities of Daily Living with Smart Meters. Springer, Germany(2014) Q. Ni, A. B. Garca Hernando, and I. P. de la Cruz, "The elderlys independent living in smart homes: A characterization of activities and sensing infrastructure survey to facilitate services development,"(2015).

IV. EXISTING SYSTEM

Existing system data confidentiality is much important but in existing system framework it is not enough for to only guarantee the data confidentiality of the patient's personal health information in the honest-but-curious cloud server model since the frequent communication between a patient and a professional physician can lead the adversary to conclude that the patient is suffering from a specific disease with a high probability. Unfortunately, the problem of how to protect both the patients' data confidentiality and identity privacy in the distributed m-healthcare cloud computing scenario under the malicious model was left untouched.

Patients are unwilling to accept the EHR system unless their protected health information (PHI) containing highly confidential data is guaranteed proper use and disclosure, which cannot be easily achieved without patients' control over their own PHI. However, cautions must be taken to handle emergencies in which the patient may be physically incompetent to retrieve the controlled PHI for emergency treatment a secure EHR system, HCPP (Health care system for Patient Privacy), based on cryptographic constructions and existing wireless network infrastructures, to provide privacy protection to patients under any circumstances while enabling timelyPHI retrieval for life-saving treatment in emergency situations.

DISADVANTAGS

- Data confidentiality is low.
- Data redundancy is high.
- There is a violation in data security.

V. PROPOSED SYSTEM

We presented a new architecture of pseudonymiaztion for protecting privacy in E-health (PIPE) integrated pseudonymization of medical data, identity management, obfuscation of metadata with anonymous authentication to prevent disclosure attacks and statistical analysis in and suggested a secure mechanism guaranteeing anonymity and privacy in both the personal health information transferring and storage at a central m-healthcare cloud server. We proposed an

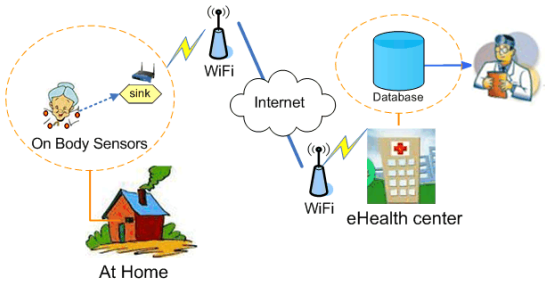
anonymous authentication of membership in dynamic groups. However, since the anonymous authentication mentioned above are established based on public key infrastructure (PKI), the need of an online certificate authority (CA) and one unique public key encryption for each symmetric key k for data encryption at the portal of authorized physicians made the overhead of the construction grow linearly with size of the group. Furthermore, the anonymity level depends on the size of the anonymity set making the anonymous authentication impractical in specific surroundings where the patients are sparsely distributed.

In this paper, the security and anonymity level of our proposed construction is significantly enhanced by associating it to the underlying Gap Bilinear Diffie-Hellman (GBDH) problem and the number of patients' attributes to deal with the privacy leakage in patient sparsely distributed scenarios significantly, without the knowledge of which physician in the healthcare provider is professional in treating his illness, the best way for the patient is to encrypt his own PHI under a specified access policy rather than assign each physician a secret key. As a result, the authorized physicians whose attribute set satisfy the access policy can recover the PHI and the access control management also becomes more efficient.

ADVANTAGES

- M-healthcare system is fully controlled and secured with encryption standards.
- There is no data loss and data redundancy.
- System provides full protection for patient's data and their attributes.

VI. SYSTEM ARCHITECHURE



V. RESEARCH METHODOLOGY

Attribute Based Designated Verifier Signature Scheme We propose a patient self-controllable and multi-level privacy-preserving cooperative authentication scheme based on ADVS to realize three levels of security and privacy requirement in distributed m-healthcare cloud computing system which mainly consists of the following five algorithms: Setup, Key Extraction, Sign, Verify and Transcript Simulation Generation. Denote the universe of attributes as U.

VI. MODULE

- E-healthcare System Framework
- Authorized accessible privacy model
- Security Verification
- Performance Evaluation

Module Description

A. E-healthcare System Framework:

E-healthcare System 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. Illustrate 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.

B. Authorized accessible privacy model

Multi- level privacy- preserving cooperative authentication is established to allow the patients to authorize corresponding privileges to different kinds of physicians located in distributed healthcare providers by setting an access tree supporting flexible threshold predicates. Propose a novel authorized accessible privacy model for distributed m-healthcare cloud computing systems which consists of the following two components: an attribute based designated verifier signature scheme (ADVS) and the corresponding adversary model.

C. Security Verification

The security and anonymity level of our proposed construction is significantly enhanced by associating it to the underlying Gap Bilinear Diffie-Hellman (GBDH) problem and the number of patients' attributes to deal with the privacy leakage in patient sparsely distributed scenarios. More significantly, without the knowledge of which physician in the healthcare provider is professional in treating his illness, the best way for the patient is to encrypt his own PHI under a specified access policy rather than assign each physician a secret key. As a result, the authorized physicians whose attribute set satisfy the access policy can recover the PHI and the access control management also becomes more efficient.

D. Performance Evaluation

The efficiency of PSMPA in terms of storage overhead, computational complexity and communication cost. a patient-centric and fine-grained data access control using ABE to secure personal health records in cloud computing without privacy-preserving authentication. To achieve the same security, our construction performs more efficiently than the traditional designated verifier signature for all the directly authorized physicians, where the overheads are linear to the number of directly authorized physicians.

CONCLUSION

In this project, a novel authorized accessible privacy model and a patient self-controllable multi-level privacy preserving cooperative authentication scheme realizing three different levels of security and privacy requirement in the distributed m-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] J.Misic and V. B. Misic, "Implementation of security policy for clinical information systems over wireless

sensor network," Ad Hoc Netw., vol. 5, no. 1, pp. 134–144, Jan. 2007.

[2] J. Misic and V. Misic, "Enforcing patient privacy in healthcare WSNs through key distribution algorithms," Security Commun. Netw. J., vol. 1, no. 5, pp. 417–429, 2008

[3] M. Li, S. Yu, K. Ren, and W. Lou, "Securing personal health records in cloud computing: Patient-centric and fine-grained data access control in multi-owner settings," in Proc. 6th Int. ICST Conf. Security Privacy Comm. Netw., 2010, pp. 89–106.

[4] J. Sun and Y. Fang, "Cross-domain data sharing in distributed electronic health record system," IEEE Trans. Parallel Distrib. Syst., vol. 21, no. 6,

[5] pp. 754–764, Jun. 2010.

[6] R. Lu, X. Lin, X. Liang, and X. Shen, "A secure handshake scheme with symptoms-matching for mhealthcare social network," J. Mobile Netw. Applications, vol. 16, no. 6, pp. 683–694, Dec. 2011.

[7] A. Yassine, A. A. N. Shirehjini, and S. Shirmohammadi, "Smart meters big data: Game theoretic model for fair data sharing in deregulated smart grids," IEEE Access, vol. 3, pp. 2743–2754, 2015.

[8] A. Yassine and S. Shirmohammadi, "Measuring users' privacy payoff using intelligent agents," in 2009 IEEE International Conference on Computational Intelligence for Measurement Systems and Applications, May 2009, pp. 169–174.

[9] "A business privacy model for virtual communities," Inderscience Publishers International journal of web based communities, vol. 5, 2009.

[10] Y. C. Chen, H. C. Hung, B. Y. Chiang, S. Y. Peng, and P. J. Chen, "Incrementally mining usage correlations among appliances in smart homes," in Network-Based Information Systems (NBiS), 2015 18th International Conference on, 9 2015, pp. 273–279.

[11] K. Jack and K. William, "The UK-DALE dataset, domestic appliance-level electricity demand and whole-house demand from five UK homes," Scientific Data, vol. 2, no. 150007, 2015.

[12] J. Clement, J. Ploennigs, and K. Kabitzsch, Detecting Activities of Daily Living with Smart Meters. Springer, Germany, 11 2014, ch. Advance Technology and Societal Change, pp. 143–160. [Online].Available:https://link.springer.com/chapter/10.1007/ 978-3-642-37988-8 10.

[13] Q. Ni, A. B. Garca Hernando, and I. P. de la Cruz, "The elderlys independent living in smart homes: A characterization of activities and sensing infrastructure survey to facilitate services development," Sensors, vol. 15, no. 5, pp. 11 312–11 362, 2015. [Online]. Available: http://www.mdpi.com/1424-8220/15/ 5/11312Fig.