M-Healthcare Cloud Computing System for Multilevel and Single Handled Privacy Preserving Cooperative Authentication in Patient Diagnosis

Mr. S.N. Patil[1] Prof. B.S.Borkar[2] Prof. R.N. Muneshwar[3]
[1,2,3]Savitribai Phule Pune University, AVCOE Sangamner

Abstract— A patient attribute-based designated verifier signature a patient self controllable multi-level privacy-preserving cooperative authentication security and privacy requirement in distributed m-healthcare cloud computing system. Distributed m-healthcare cloud computing system significantly sencourages productive patient treatment for therapeutic discussion by sharing individual wellbeing data among human services suppliers. Nonetheless, it brings regarding the challenge of keeping each the information confidentiality and patients' identity privacy at the same time. Numerous current get to control and unknown validation plans can't be clearly abused. To take care of the issue, in this paper, a novel approved open protection Model (AAPM) is set up. Patients can authorize physicians by setting an access tree supporting flexible threshold predicates. At that point, in light of it, by formulating another method of characteristic based assigned verifier signature, a patient self-controllable multi-level privacy-preserving cooperative validation scheme (PSMPV) realizing three levels of security and privacy requirement in distributed m-healthcare cloud computing system is proposed. The directly approved physicians, the indirectly approved physicians and the unauthorized persons in medical consultation can restorative decipher the personal health information and/or verify patients' identities by satisfying the access tree with their own attribute sets. Privacy in the distributed m-healthcare cloud the formal security evidence and simulation results illustrate our scheme can resist various kinds of attacks and far outperforms the past ones as far as computational, communication and capacity overhead.

Key words: Multi-Level Privacy, Authentication, Access control, Security and Privacy, Distributed cloud computing, M-healthcare system

I. INTRODUCTION

Distributed m-healthcare cloud computing systems have been increasingly adopted world wide including the European Commission exercises, the US Health Insurance Portability and Accountability Act (HIPAA) and numerous different governments for efficient and high-quality medical treatment [1-3]. The individual health information is always shared among the patients situated in respective social communities suffering from the similar disease for mutual support, and across distributed healthcare providers (HPs) equipped with their own cloud servers for medical consultant [28-29]. However, it likewise achieves a progression of difficulties, particularly how to guarantee the security and protection of the patients' personal health data from different assaults in the remote correspondence channel such as eavesdropping and tampering [26]. As to the security facet, one of the main issues is access control of patients' personal health information, to be specific it is just the approved doctors or institutes that can recover the patients' personal health information through the data sharing in the distributed m-healthcare cloud computing system.

Most patients are concerned about the confidentiality of their personal health data since it is likely to make them in trouble for each kind of unauthorized collection and disclosure. In this way, in distributed m healthcare cloud computing frameworks, 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 immovable issues requesting earnest arrangements. There has developed different research comes about [8-9] concentrating on them. A fine-grained appropriated information get to control plan is proposed utilizing the system of characteristic based encryption (CBE). A meet based get to control strategy provides access privilege if and only if the patient and the physician meet in the physical world. Recently, a patient-driven and fine-grained data access control in multi-proprietor settings is constructed for securing personal health records in distributed computing. In any case, it fundamentally concentrates on the central cloud computing system which is not sufficient for proficiently handling the expanding volume of personal health information in m-healthcare distributed computing framework. Moreover, it is not enough for [30] to only guarantee the data confidentiality of the patient's personal health information in the honest-but-curious cloud server model the incessant correspondence 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 the issue 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.

We consider simultaneously achieving data secrecy and identity protection with high efficiency. As is described in distributed m-healthcare cloud computing systems, all the members can be classified into three categories: the specifically approved physicians with green names in the local healthcare provider who are authorized by the patients and can both access the patient's personal health information and check 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 we realize three different levels of privacy-preserving requirement mentioned above. The main contributions of this paper are outlined as follows.

1) A novel authorized approved privacy model (AAPM) for the multi-level privacy-preserving cooperative authentication is established to allow the patients to

approve relating privileges to different kinds of physicians located in distributed healthcare providers by setting an access tree supporting flexible threshold predicates.

2) Based on AAPM, a patient self-controllable multilevel protection cooperative authentication scheme (PSMPA) in the distributed m-healthcare cloud computing system is proposed, realizing three different levels levels of security and protection prerequisite for the patients.
3) The formal security proof and simulation results show that our scheme far outperforms the previous constructions in terms of privacy-preserving capability, computational, communication and capacity overhead. The rest of this paper is organized as follows. We discuss related work in the next section. In Section 3, the system model of a distributed m-healthcare cloud computing system is illustrated.

II. RELATED WORK

Besides the constructions for authorized access control of patients' personal health information [8-11].We mentioned above, there exist anonymous identification schemes by pseudonyms and other privacy-preserving techniques [4, 10-14]. Lin et. al. proposed SAGE achieving not only the content oriented privacy but also the contextual privacy against a strong global adversary [12]. Sun et. al. proposed a solution to privacy and emergency responses based on anonymous credential, pseudorandom number generator and proof of knowledge [11, 13]. Lu et. al. proposed a privacy-preserving authentication scheme in anonymous P2P systems based on Zero-Knowledge Proof [14]. However, the heavy computational overhead of Zero-Knowledge Proof makes it cannot be directly applied to the distributed m-healthcare systems where the computational resource for both patients and physicians is limited. Riedl et. al. presented a new architecture pseudonymiaztion of information for privacy in E-health (PIPE) [25].There exist a series of constructions for authorized access control of patients' personal health information [8], [9], [10],[11], [15], [16], [18]. As we discussed in the previous section, they mainly study the issue of data confidentiality in the central cloud computing architecture, while leaving the challenging problem of realizing different security and privacy-preserving levels with respect to kinds of physicians accessing distributed cloud server sun solved. On the other hand, anonymous identification schemes are emerging by exploiting pseudonyms and other privacy-preserving techniques [4], [10], [11], [12]. Lin et. al. proposed SAGE achieving not only the content-oriented privacy but also the contextual privacy against a strong global adversary [12]. Sun et al. proposed a solution to privacy and emergency responses based on anonymous credential, pseudorandom number generator and proof of knowledge [11], [13]. Lu et al. proposed a privacy-preserving authentication scheme in anonymous P2P systems based on Zero-Knowledge Proof [14]. However, the heavy computational overhead of Zero-Knowledge Proof makes it impractical when directly applied to the distributed m-healthcare cloud computing systems where the computational resource for patients is constrained. Misic and Misic suggested patients have to consent to treatment and be alerted every time when associated physicians access their records [31], [32]. Riedl et al. presented a new architecture of pseudonymiaztion for protecting privacy in E-health (PIPE) [25]. Slamanig and Stingl integrated pseudonymization of medical data, identity management, obfuscation of metadata with anonymous authentication to prevent disclosure attacks and statistical analysis in [26] 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 [7]. Schechter et al. proposed an anonymous authentication of membership in dynamic groups [6]. However, since the anonymous authentication mentioned above [6], [7] 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 in [6], [7]. 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 satisfies the access policy can recover the PHI and the access control management also becomes more efficient.

III. PROPOSED SYSTEM

The fundamental e-medicinal services framework represented in Fig. 1 basically comprises of three parts: body zone networks (BANs), remote transmission systems and the social insurance suppliers furnished with their own particular cloud servers. The patient's close to home wellbeing data is safely transmitted to the medicinal services supplier for the approved doctors to get to and perform restorative treatment.

The Drawbacks of Existing system are they overwhelmingly focuses on the central conveyed figuring structure which is not satisfactory for capably taking care of the extending the volume of individual prosperity information and most patients are stressed over the mystery of their own prosperity information since it is at risk to bring them up in hellfire for each kind of unapproved collection and introduction.

Overcoming of this issue, a novel approved available protection model is set up, patients can approve doctor by setting a get to tree supporting adaptable limit predicates. A patient self-controllable multilevel protection saving agreeable approval plot acknowledging three levels of security and security necessity in appropriated m-human services framework is proposed. In our proposed system the patient request is being time bounded and provide symptoms in terms of body temperature and pulse rate, in which the doctor can examine symptoms of the patient and recommended appropriate treatment.

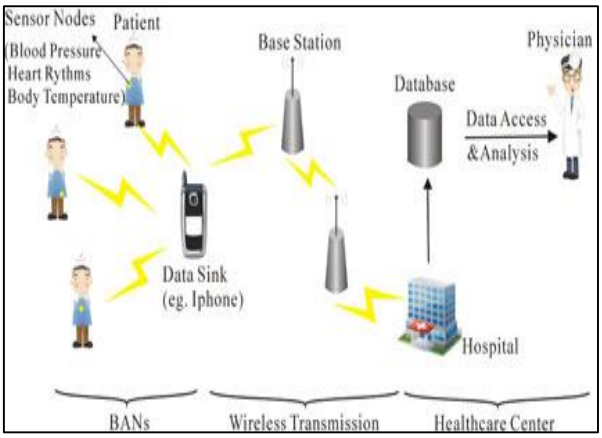

Fig. 1: A basic architecture of the e-health system.

A. *Network Model*

The basic e-healthcare system illustrated in Fig. 2 mainly consists of three components: body area networks (BANs), wireless transmission networks and the healthcare providers equipped with their own cloud servers [1], [2]. The patient's personal health information is securely transmitted to the healthcare provider for the authorized physicians to access and perform medical treatment.

We further 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. A typical architecture of a distributed m-healthcare cloud computing system is shown in Fig. 3. 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.

System can be divided in to four parts

1) Patient
2) Clinical Data Collection
3) Administrator
4) Physician

1) Patient

The patient must register at hospital and he can enter he/her all the information of his/her health information. After stored patient information in hospital server the physician checks patient.

2) Clinical Data Collection

The Hardware kit contains sensors like temperature and heart bit counter. Using that sensors the patients heart bit and body temperature readings collection are done. Using Radio frequency that readinds are send to the mobile device like laptop, tablet etc. the receiver side receive that readings and uploads on physician cloud.. With the PMHS, each patient will have control over their personal medical information the information clinical institutions may not have, which will help reduce the complexity of health care delivery to each individual significantly.

3) Administrator

This module is use to assign the patient which is registered at hospital to the respective specialist. It manages each patients uploaded files such as CDA files, medical images, medical video files, and any other related medical documents (e.g. medical charts, immunization records, etc.). The files will be uploaded by each individual and may be shared with physicians when necessary for the treatment.

4) Physician

Physicians are two categories: The directly authorized physicians are identified with green labels in the local health-care provider they are authorized by the patients and these physicians can access the patients personal health information and verify the patients identity. The indirectly authorized physicians identified with yellow labels in the remote health-care providers they are authorized by the directly authorized physicians for medical consultant or some research purposes. Since they are not authorized by the patients called indirectly authorized physicians. They can only access the personal health information, but not the patients identity.

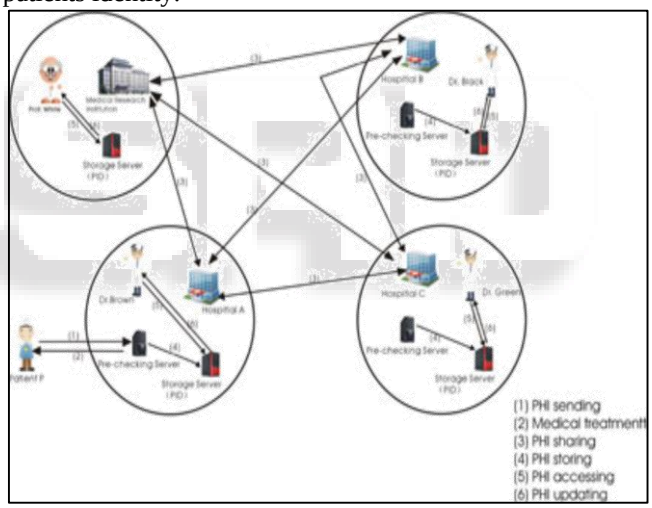

Fig. 2: An overview of our distributed m-healthcare cloud computing system.

IV. Conclusion

We provide 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.

Acknowledgement

I thankful our partners from AVCOE, Sangamner who gave knowledge and mastery that significantly helped the dissertation.I want to demonstrate my appreciation to the Prof. B. S. Borkar for offering his pearls of intelligence to

me over the span of this dissertation. I am additionally gigantically greatful to Dr. B. L. Gunjal (H.O.D) for her remarks on a prior rendition of the original copy.

REFERENCES

[1] L. Gatzoulis and I. Iakovidis, "Wearable and portable E-health systems," IEEE Eng. Med. Biol. Mag., vol. 26, no. 5, pp. 51–56, Sep.-Oct. 2007.
[2] I. Iakovidis, "Towards personal health record: current situation, obstacles and trends in implementation of electronic healthcare records in europe," Int. J. Med. Inf., vol. 52, no. 1, pp. 105–115, 1998.
[3] 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," in Proc. Int.Workshop Wearable Implantable Body Sens. Netw., Apr. 2006, pp. 150–153.
[4] R. Lu and Z. Cao, "Efficient remote user authentication scheme using smart card," Comput. Netw., vol. 49, no. 4, pp. 535–540, 2005.
[5] M. D. N. Huda, N. Sonehara, and S. Yamada, "A privacy management architecture for patient-controlled personal health record system," J. Eng. Sci. Technol., vol. 4, no. 2, pp. 154–170, 2009.
[6] S. Schechter, T. Parnell, and A. Hartemink, "Anonymous authentication of membership in dynamic groups in," in Proc. 3rd Int. Conf. Financial Cryptography, 1999, pp. 184–195.
[7] D. Slamanig, C. Stingl, C. Menard, M. Heiligenbrunner, and J. Thierry, "Anonymity and application privacy in context of mobile computing in eHealth," in Mobile Response, New York, NY, USA: Springer, 2009 pp. 148–157.
[8] J. Zhou and Z. Cao, "TIS: A threshold incentive scheme for secure and reliable data forwarding in vehicular delay tolerant networks," in Proc. IEEE Global Commun. Conf., 2012, pp. 985–990.
[9] S. Yu, K. Ren, and W. Lou, "FDAC: Toward fine-grained distributed data access control in wireless sensor networks," in Proc. IEEE Conf. Comput. Commun., 2009, pp. 963–971.
[10] F. W. Dillema and S. Lupetti, "Rendezvous-based access control for medical records in the pre-hospital environment," in Proc. 1st ACM SIGMOBILE Int. Workshop Syst. Netw. Support Healthcare Assisted Living, 2007, pp. 1–6.
[11] J. Sun, Y. Fang, and X. Zhu, "Privacy and emergency response in e-healthcare leveraging wireless body sensor networks," IEEE Wireless Commun., vol. 17, no. 1, pp. 66–73, Feb. 2010.
[12] X. Lin, R. Lu, X. Shen, Y. Nemoto, and N. Kato, "SAGE: A strong privacy-preserving scheme against global eavesdropping for Ehealth systems," IEEE J. Sel. Areas Commun., vol. 27, no. 4, pp. 365–378, May 2009.
[13] J. Sun, X. Zhu, C. Zhang, and Y. Fang, "HCPP: Cryptography based secure EHR system for patient privacy and emergency healthcare," in Proc. 31st Int. Conf. Distrib. Comput. Syst., 2011, pp. 373–382.
[14] 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 Trans. Parallel Distrib. Syst., vol. 19, no. 10, pp. 1325–1337, Oct. 2008.
[15] J. Zhou and M. He, "An improved distributed key management scheme in wireless sensor networks," in Proc. 9th Int. Workshop Inf. Security Appl., 2008, pp. 305–319.
[16] J. Zhou, Z. Cao, X. Dong, X. Lin, and A. V. Vasilakos, "Securing mhealthcare social networks: challenges, countermeasures and future directions," IEEE Wireless Commun., vol. 20, no. 4, pp. 12– 21, Aug. 2013.
[17] M. Chase and S. S. Chow, "Improving privacy and security in multi-authority attribute-based encryption," in Proc. 16th ACM Conf. Comput. Commun. Security, 2009, pp. 121–130.
[18] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in Proc. IEEE Symp. Security Privacy, 2007, pp. 321–334.

