Apr - Jun © 2016 Transactions; 3(10): 443-448

International Journal of Research and Applications

ISSN (online): 2349-0020 ISSN (print): 2394-4544 http://www.ijraonline.com/

Case Study

PSMPAL: Patient Self-Controllable, Multi-Level Privacy-Preserving Cooperative Authentication and Load balancing in Distributed M-Healthcare Cloud Computing System

[1] A.Sampath Kumar, [2] K. Srinivas and [3] K. Obulesh

Corresponding Author:
amaravathi.sampath@gmail.com

DOI:
http://dx.doi.org/
10.17812/IJRA.3.10(75)2016

Manuscript:
Received: 6th Apr, 2016
Accepted: 15th May, 2016
Published: 28th June, 2016

Publisher:
Global Science Publishing Group, USA
http://www.globalsciencepg.org/

ABSTRACT

Distributed m-healthcare cloud computing system significantly facilitates efficient patient treatment for medical consultation by sharing personal health information among healthcare providers. However, it brings about the challenge of keeping both the data secure and balancing load to improve the efficiency. Many existing access control and anonymous authentication schemes cannot be straightforwardly exploited. To solve the problem, in this paper, a novel authorized accessible privacy model (AAPM) is established with efficient Load balancing. Patients can authorize physicians by setting an access tree supporting flexible threshold predicates. Then, based on the technique of attribute-based designated verifier signature, a patient self-controllable multi-level privacy-preserving cooperative authentication scheme (PSMPA) adding Load balancing (PSMPAL) for increasing the efficiency in realizing three levels of security and privacy requirement in distributed m-healthcare cloud computing system is proposed.

Keywords: Authentication, access control, security and privacy, distributed cloud computing, m-healthcare system, Load balancing.

[1] PG scholar, [2 3] Associate Professor, [1 2 3] Department of CSE
[1 2 3] Avanthi Institute of Engineering& Technology, Hyderabad, Andhra Pradesh.

IJRA - Year of 2016 Transactions:
Month: April - June
Volume – 3, Issue – 10, Page No's: 443-448
Subject Stream: Computers

Paper Communication: Author Direct

Paper Reference Id: IJRA-2016: 3(10)443-448

DOI: 10.17812/IJRA.3.10(75)2016

International Journal of Research and Applications
April-June © 2016 Transactions 3(10): 443-448

eISSN : 2349 – 0020
pISSN : 2394 – 4544
www.ijraonline.com

COMPUTERS CASE STUDY

PSMPAL: Patient Self-Controllable, Multi-Level Privacy-Preserving Cooperative Authentication and Load balancing in Distributed M-Healthcare Cloud Computing System

[1] A.Sampath Kumar, [2] K. Srinivas and [3] K. Obulesh

[1] PG scholar, [2 3] Associate Professor, [1 2 3] Department of CSE

[1 2 3] Avanthi Institute of Engineering& Technology, Hyderabad, Andhra Pradesh.

amaravathi.sampath@gmail.com, srinivas.kmt1@gmail.com , obul_is@yahoo.co.in

ABSTRACT

Distributed m-healthcare cloud computing system significantly facilitates efficient patient treatment for medical consultation by sharing personal health information among healthcare providers. However, it brings about the challenge of keeping both the data secure and balancing load to improve the efficiency. Many existing access control and anonymous authentication schemes cannot be straightforwardly exploited. To solve the problem, in this paper, a novel authorized accessible privacy model (AAPM) is established with efficient Load balancing. Patients can authorize physicians by setting an access tree supporting flexible threshold predicates. Then, based on the technique of attribute-based designated verifier signature, a patient self-controllable multi-level privacy-preserving cooperative authentication scheme (PSMPA) adding Load balancing (PSMPAL) for increasing the efficiency in realizing three levels of security and privacy requirement in distributed m-healthcare cloud computing system is proposed.

Keywords: Authentication, access control, security and privacy, distributed cloud computing, m-healthcare system, Load balancing.

1. 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 [1], [2], [3]. 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 [28], [29]. How-ever, 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 wire-less communication channel such as eavesdropping and tampering [5], [26].

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 have emerged various research results [8], [9], [10], [11], [15], [16], [18], [19] focusing on them. A fine-grained distributed data access control scheme [9] is proposed using the technique of attribute based encryption (ABE). A rendezvous-based access control method [10] 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 con-troll in multi-owner settings is constructed for securing personal health records in cloud computing [30]. 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 [30] 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

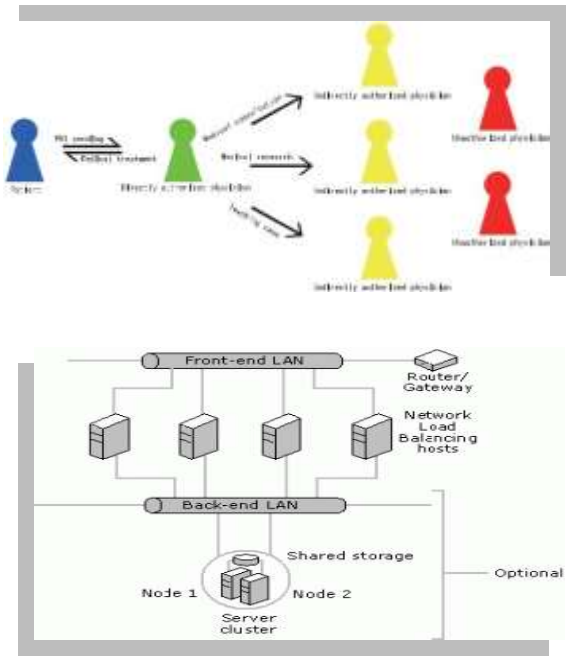

Fig. 1. Multiple security, privacy levels and load balancing in m-Healthcare cloud computing system.

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 and load balancing. 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 [22] and designated verifier signatures (DVS) [21] on de-identified health information [27], we realize three different levels of privacy-preserving requirement mentioned above. The main contributions of this paper are summarized as follows.

(1) A novel authorized accessible privacy model (AAPM) for the 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.

(2) Based on AAPM, a patient self-controllable multi-level privacy-preserving cooperative authentication scheme (PSMPA) in the distributed m-healthcare cloud computing system is implemented [31], realizing three different levels of security and privacy requirement 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 storage overhead.

(4) Network Load Balancing is superior to other software solutions such as round robin DNS (RRDNS), which distributes workload among multiple servers but does not provide a mechanism for server availability. If a server within the host fails, RRDNS, unlike Network Load Balancing, will continue to send it work until a network administrator detects the failure and removes the server from the DNS address list. This results in service disruption for clients. Network Load Balancing also has advantages over other load balancing solutions—both hardware- and software-based—that introduce single points of failure or performance bottlenecks by using a centralized dispatcher. Because Network Load Balancing has no proprietary hardware requirements, any industry-standard compatible computer can be used. This provides significant cost savings when compared to proprietary hardware load balancing solutions.

The rest of this paper is organized as follows. We discuss related work in the next section. In Section 3, the network model of a distributed m-healthcare cloud computing system is illustrated. We provide some background and preliminaries required throughout the paper in Section 4. Section 5 describes the suggested model for Load balancing. Finally, Section 6 concludes the paper.

2. RELATED WORK

There exist a series of constructions for authorized access control of patients' personal health information [8], [9], [10], [11], [15], [16], [18], [19], [31], 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 (w.r.t.) kinds of physicians accessing distributed cloud servers unsolved. On the other hand, anonymous identification schemes are emerging by exploiting pseudonyms and other privacy-preserving techniques [4], [10], [11], [12], [13], [14], [17], [20], [23], [25]. 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. pro-posed 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], Riedl et al. presented a new architecture of pseudonymiaztion for protecting privacy in E-health (PIPE) [25]. Slamanig and Sting integrated pseudonymization of medical data, identity management, and 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-health-care 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.

3. Network Load Balancing

Network Load Balancing scales the performance of a server-based program, such as a Web server, by distributing its client requests among multiple servers within the cluster. With Network Load Balancing, each incoming IP packet is received by each host, but only accepted by the intended recipient. The cluster hosts concurrently respond to different client requests, even multiple requests from the same client. For example, a Web browser may obtain the various images within a single Web page from different hosts in a load-balanced cluster. This speeds up processing and shortens the response time to clients.

Each Network Load Balancing host can specify the load percentage that it will handle, or the load can be equally distributed among all of the hosts. Using these load percentages, each Network Load Balancing server selects and handles a portion of the workload. Clients are statistically distributed among cluster hosts so that each server receives its percentage of incoming requests. This load balance dynamically changes when hosts enter or leave the cluster. In this version, the load balance does not change in response to varying server loads (such as CPU or memory usage). For applications, such as Web servers, which have numerous clients and relatively short-lived client requests, the ability of Network Load Balancing to distribute workload through statistical mapping efficiently balances loads and provides fast response to cluster changes.

Network Load Balancing cluster servers emit a *heartbeat message* to other hosts in the cluster, and listen for the heartbeat of other hosts. If a server in a cluster fails, the remaining hosts adjust and redistribute the workload while maintaining continuous service to their clients. Although existing connections to an offline host are lost, the Internet services nevertheless remain continuously available. In most cases (for example, with Web servers), client software automatically retries the failed connections, and the clients experience only a few seconds' delay in receiving a response.

4. A DYNAMIC LOAD BALANCING MODEL

The dynamic load balancing schemes we are proposing are based on a general four-phase load balancing model. A detailed description of the model is given in [32]. The four phases are described as follows.

1. ***Processor Load Evaluation.*** A load value is estimated for each processor in the system. These values are used as input to the load balancer to detect load imbalances and make load migration decisions.
2. ***Load Balancing Profitability Determination.*** The *imbalance factor* quantifies the degree of load imbalance within a processor domain. It is used as an estimate of potential speedup obtainable through load balancing and is weighed against the load balancing overhead to determine whether or not load balancing is profitable at that time.
3. ***Task Migration Strategy:*** Sources and destinations for task migration are determined. Sources are notified of the quantity and destination of tasks for load balancing.
4. ***Ta.sk Selection Strategy.*** Source processors select the most suitable tasks for efficient and effective load balancing and send them to the appropriate destinations.

The first and fourth phases of the model are application dependent and purely distributed. Both of these phases can be executed independently on each individual processor. For the purpose of this paper, we assume a simple problem characterization in which the problem is partitioned into a fixed number of tasks. All tasks are independent and may be executed on any processor in any sequence. Furthermore, due to the unpredictable nature of the task requirements, each task is estimated to require equal computation time. The initial task distribution is made based on the estimated requirements. Hence, the Processor *Load Evaluation Phase is* reduced to a simple count of the number of tasks pending execution. Similarly, the *Task Selection Strategy* is simplified since no distinction is made between tasks, and the issue of locality is ignored. For the case where tasks are created dynamically, if the arrival rate is predictable then this information can be incorporated into the load evaluation [33], if not predictable, then the potential arrival of new tasks can effectively be ignored.

Our focus is on the Profitability Determination and Task Migration phases, the second and third phases, of the load balancing process. As the program execution evolves, the inaccuracy of the task requirement estimates leads to un- balanced load distributions. The imbalance must be detected and measured (Phase 2) and an appropriate migration strategy devised to correct the imbalance (Phase 3). These two phases may be performed in either a distributed or centralized fashion. Centralized approaches tend to be more accurate since the entire system's state information is accumulated to a single point, and a high degree of knowledge is used

in the decision process. However, the accumulation of information requires synchronization which incurs an overhead and a delay. This overhead may become prohibitively large for highly parallel systems and the delay may increase to a point where the information accumulated ages and loses validity. Alternatively, distributed approaches, although less accurate since they o p erate with less information, incur a smaller synchronization overhead.

The above model with PSMPA, is applied to distributed m-healthcare cloud computing system to facilitate efficient patient treatment for medical consultation by sharing personal health information among healthcare providers.

5. CONCLUSIONS

In this paper, 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 with load balancing are proposed. The future enhancement is to implement the PKI system and use certificate authority in issuing certificates whenever the health information is transmitted in between intended parties

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 man-agement 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 authenti-cation 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 distrib-uted 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 E-health systems," IEEE J. Sel. Areas Commun., vol. 27, no.
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 m-healthcare 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 attri-bute-based encryption," in Proc. IEEE Symp. Security Privacy, 2007, pp.321-334.

[19] N. Cao, Z. Yang, C. Wang, K. Ren, and W. Lou, "Privacy-pre-serving query over encrypted graph-structured data in cloud computing," in Proc. 31st Int. Conf. Distrib. Comput. Syst., 2011, pp.393-402.

[20] F. Cao and Z. Cao, "A secure identity-based multi- proxy signature scheme," Comput. Electr. Eng., vol. 35, pp. 86–95, 2009.

[21] X. Huang, W. Susilo, Y. Mu, and F. Zhang, "Short designated veri-fier signature scheme and its identity-based variant," Int. J. Netw. Security, vol. 6, no. 1, pp. 82–93, Jan. 2008.

[22] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proc ACM Conf. Comput. Commun. Security, 2006, pp. 89–98.

[23] J. Li, M. H. Au, W. Susilo, D. Xie, and K. Ren, "Attribute-based signature and its applications," in Proc. 5th ACM Symp. Inf., Com-put. Commun. Security, 2010, pp. 60–69.

[24] PBC Library, [online] 2006. http://crypto.stanford.edu/pbc/times. Html.

[25] B. Riedl, V. Grascher, and T. Neubauer, "A secure e-health archi-tecture based on the appliance of pseudonymization," J. Softw., vol. 3, no. 2, pp. 23–32, Feb. 2008.

[26] D. Slamanig and C. Stingl, "Privacy aspects of E-health," in Proc. 3rd. Int. Conf. Availab., Rel. Security, 2008, pp. 1226–1233.

[27] De-identified Health Inf., [online] http://aspe.hhs.gov/admnsimp/ bannerps.htm, 2007.

[28] 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.

[29] J. Sun and Y. Fang, "Cross-domain data sharing in distributed electronic health record system," IEEE Trans. Parallel Distrib. Syst., vol. 21, no. 6, pp. 754–764, Jun. 2010.

[30] 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.

[31] Jun Zhou, Xiaodong Lin, Xiaolei Dong, and Zhenfu Cao, "Patient Self-Controllable and Multi-Level Privacy-Preserving Cooperative Authentication in Distributed m-Healthcare Cloud Computing System" IEEE Transactions On Parallel And Distributed Systems, Vol. 26, No. 6, June 2015,PP.1693-1702.

[32] M. Willebeek - LeMair and A. P. Reeves, "A general dynamic load balancing model for parallel computers" Tech. Rep. EE-CEG-89-1, Cornell Scholl of Electrical Engineering, 1989.

[33] M. Hailperin, "Load balancing for massivelly-paralle soft-real-rime system" in Proc., 2nd Symp. Frontiers of Massively Parallel Computation, 1988, pp. 159-163.