International Journal of Security and Its Applications
Vol.8, No.5 (2014), pp.131-138
http://dx.doi.org/10.14257/ijsia.2014.8.5.13

A Lightweight Trust-based Access Control Model in Cloud-Assisted Wireless Body Area Networks

Xu Wu

Department of Computer Science, Xi'an University of Posts and Telecommunications, Xi'an, China
xrdz2006@163.com

Abstract

The integration of Wireless Body Area Networks (WBANs) with cloud computing will enable users (including physicians and nurses) to globally access the electronic healthcare data at competitive costs. However, some new issues on data access control are associated with the integration of WBANs and cloud computing. In order to address these issues, we propose a lightweight trust-based access control model, where the users can acquire their access control privileges for the electronic healthcare data according to the user role and trust value in the trust certificates. Simulation results show that our method can better alleviate the communication overhead and energy consumption problem.

Keywords: *Wireless Body Area Networks, trust model, cloud computing*

1. Introduction

Wireless Body Area Networks (WBANs) have emerged as a promising technology for medical and non-medical applications. Cloud computing is expected to play a significant role in achieving the aforementioned objectives. The cloud computing environment links different devices ranging from miniaturized sensor nodes to high-performance supercomputers for delivering people-centric and context-centric services to the individuals and industries. The integration of WBANs and Cloud computing is expected to facilitate the development of cost-effective, scalable, and datadriven pervasive healthcare systems, which must be able to realize long-term health monitoring and data analysis of patients in different environments. This WBAN-cloud will enable users (including physicians and nurses) to globally access the processing and storage infrastructure at competitive costs. Nevertheless, the research into cloud-enabled WBAN platforms (also called wMCC platforms) is still in its infancy, Current studies related to wMCC platforms mainly focus on architectural design to realize a health monitoring and analysis system. The security of patient-related data is an indispensable component of the wMCC platform [1]. Therefore, both the cloud providers and the users must take strong security measures to protect the storage infrastructure.

In designing a secure wMCC platform, a number of design factors including encryption, scalability, access control, data partitioning, user diversity, and mobile access should be considered. The current research on the security of a wMCC platform includes key management and encrypted storage. In [2], Li, *et al.*, looked into two important data security issues for WBANs: secure and dependable distributed data storage, and fine-grained distributed data access control for sensitive and private patient medical data. In the paper, we mainly focus on data access control issue. A trust-based

ISSN: 1738-9976 IJSIA

access control model is proposed, where the users can acquire their access control privileges for the electronic healthcare data according to the user role and trust value in the lightweight trust certificates. The lightweight trust certificate is established based on Kerberos [10]. This paper is organized as follows. Section 2 describes related work. Section 3 presents the proposed trust-based access control model in details. Section 4 contains simulation-based experimental study. Finally, we conclude this paper in Section 5.

2. Related Work

Wireless body area networks (WBANs) can be applied to provide healthcare and patient monitoring. However, user privacy can be vulnerable in a WBAN unless security is considered. Access to authorized users for the correct information and resources for different services can be provided with the help of efficient user access control mechanisms. This section briefly discusses the existing related user access control schemes that are currently proposed in resource-constrained wireless sensor networks.

The author discussed various practical issues required to fulfill the security and privacy requirements in WBANs [2]. They explored the relevant security solutions in sensor networks and WBANs while analyzing various applications. A new user access control scheme is proposed for a WBAN in [3]. The proposed scheme makes use of a group-based user access ID, an access privilege mask, and a password. Wang, *et al.*, [4] builds the user access control on commercial off-the-shelf sensor devices as a case study to show that the public-key scheme can be more advantageous in terms of the memory usage, message complexity, and security resilience. Meanwhile, their work also provides insights in integrating and designing public-key based security protocols for sensor networks. They implemented the access control protocol on a test bed of TelosB motes [5]. Based on ECC, they provided the local authentication. By using certificate-based authentication, the user access was verified by the sensor nodes.

A distributed privacy preserving access control scheme is presented for WSNs in [6]. They identified the characteristics of a single-owner multi-user sensor network and the requirements of a distributed privacy preserving access control. A user access control scheme is proposed for a wireless multimedia sensor network in [7]. In this scheme, an authorized user can access the real time multimedia data. Their proposed scheme used Chinese Remainder Theorem-based group rekeying.

An identity-based user authentication and access control protocol is proposed in [8]. The ECC (Elliptic Curve Cryptography) based digital signature algorithm (DSA) is used for signing a message and verifying a message for a wireless sensor networks. An ECC-based user access control scheme is proposed in [9]. This paper describes a public-key implementation of access control in a sensor network.

3. The Proposed Model

3.1. Access Control Process

Instead of being measured face-to-face, with WBANs patients' health-related parameters can be monitored remotely, continuously, and in real time, and then processed and transferred to medical databases. This medical information is shared among and accessed by various users such as healthcare staff, researchers, government agencies, and insurance companies. However, in real life WBAN scenarios, all users

should not have the same network access privileges. A particular user should only be able to access required information. To provide controlled user access for WBANs, we propose a new access control model utilizing the user role and trust value in the lightweight certificates. The user trust value in the certificate can be calculated by a user behavior-based trust scheme. Each user can acquire their access control privileges according to its role and trust value. An authenticated user with a lower level of privilege is not allowed to access higher privilege information. An example of a user access is shown in Figure 1.

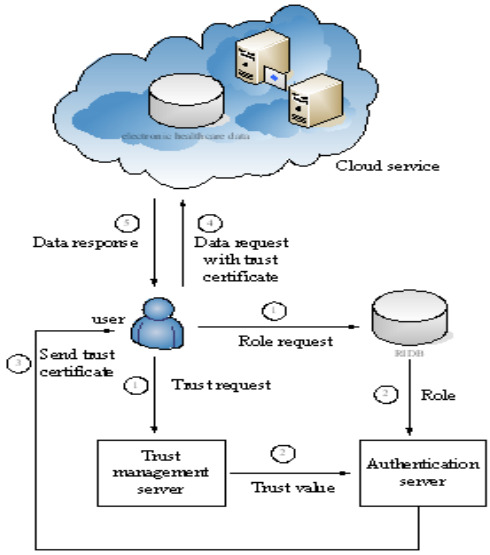

Figure 1. An Example of a User Access

The access control process runs as follows:

Step1: The user sends his identity information and requests his role information from the RIDB. The user sends his identity information and requests his trust value from the TMS (trust management server);

Step2: The RIDB responds by sending his role to the AS (authentication server). The TMS responds by sending his trust value to the AS (authentication server);

Step3: The AS sends the trust certificate encrypted by the private key of AS back to user;

Step 4: The user sends the data request with trust certificate to cloud service platform;

Step 5: Cloud service platform sends response to user.

The proposed method can achieve identity authentication and authorization simultaneity in a cloud-assisted wireless body area network. Thus, compared with other cryptography-based method, our method can better alleviate the communication overhead and energy consumption problem. Figure 2 shows that the trust certificate consists of trust information and authorization information of users.

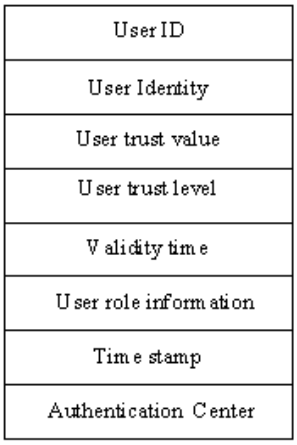

Figure 2. The Configuration Information of Trust Certificate

3.2. Trust Value Computation

The user trust value in the certificate can be calculated by a user behavior-based trust scheme. User trust computing in our scheme has two major steps: trust evidences acquirement and trust aggregation. The trust evidences are considered as the input of the trust model. All evidences form a trust vector, $T = (t_1, t_2, t_3, \ldots, t_n)$ which is the output of the trust model. All trust values are normalized with $\sum_i T_i = 1$, where $i = 1, 2, \ldots n$ and n is a size of WBANs. The trust of a user is calculated by the weighted sum of the trust evidence received. The most important problem is how to combine behavior evidence to form the evaluation of user behavior trust. Analytic Hierarchy Process (AHP) is a combination of qualitative and quantitative analysis of multi-objective decision, which simplifies the complexity of problem analysis, and can test the consistency of the major Subjective mistakes. However, AHP also has strong disadvantage of subjectivity of depending on the expert's expertise. Weize Wang and Xinwang Liu [11] consider the *t*-norm and *t*-conorm as Einstein operations and develop the intuitionistic fuzzy Einstein weighted averaging ($IFWA^{\epsilon}$) operator. In the paper, an AIFS (Atanassov's intuitionistic fuzzy set)-based algorithm is proposed to determine the weight of sub-trust and behavior evidence.

4. Experiment Study

In this section, we perform functionality and security analyses of our proposed access control model.

We consider the communication overhead of our model for authentication phase. Based on the authentication phases of our model, it is clear that the user Uj, the RIDB, the TMS and AS must exchange five messages. We have calculated the bitwise and packetwise communication overhead for our proposed model during the authentication phases. For computing the number of packets required for transmission, we considered a CC2420 transmitter (CC2420:2.4 GHz IEEE 802.15.4, 2011). A CC2420 transmitter supports a packet size of 128 bytes, *i.e.*, 1024 bits. To calculate the communication overhead, we used the bitwise size of different parameters as shown in Table 1. In Table 2, we calculated the number of bits and packets required for each message in our scheme during the authentication phases. It should be noted that we required a

communication overhead of 472 bits and the transmission of only 5 packets during the authentication phases.

Table 1. Size (in bits) of Different Parameters used for Our Model

Type	Bitwise size
User identifier (Uj)	16
Role information (Rj)	16
Trust value (Ti)	8
Hash value	160
Encryption ($E_{k,AS}$)	128
Trust certificate (Cj)	128

Table 2. Message Size and Number of Packets to be Transmitted per Message for Our Model during the Authentication Phases

Message exchange between	Size	Number of packet
User and RIDB	16	1
User and TMS	16	1
RIDB and AS	16	1
TS and AS	8	1
User and AS	256	1

Based on [12], we evaluated the energy consumption for communication through the following three-case model:

Case I: Success: both data packets and acknowledgments are successfully transmitted.

Case II: PF: Unsuccessful data packet transmission.

Case III: AF: Successful data packet transmission followed by an unsuccessful acknowledgment transmission.

According to Zhang, *et al.*, (2012), the total energy consumption for communication can be calculated as

$$E(\cdot) = E(\cdot|Success) + E(\cdot|PF) \times N_{PF}(\cdot) + E(\cdot|AF) \times N_{AF}(\cdot)$$

where $E(\cdot|Success)$, $E(\cdot|PF)$, and $E(\cdot|AF)$ represent the energy required for Case I: successful transmission, Case II: packet failure, and Case III: acknowledgment failure. $N_{PF}(\cdot)$ denotes the expected number of packet transmission failures, and $N_{AF}(\cdot)$ is the expected number of acknowledgment transmission failures. For a detailed analysis, refer to [12].

Table 3. Transmission Power Levels of CC2420

Index *i*	Transmission power	Transmission current
1	-75	2.8
2	-60	4.6
3	-45	6.3
4	-30	7.6
5	-15	9.7
6	-7	12.4
7	-3	14.9
8	0	16.8

5. Conclusion

A trust-based access control model is proposed, where the users can acquire their access control privileges for the electronic healthcare data according to the user role and trust value in the lightweight trust certificates. The lightweight trust certificate is established based on Kerberos. The user trust value in the certificate can be calculated by a user behavior-based trust scheme. Each user can acquire their access control privileges according to its role and trust value. An authenticated user with a lower level of privilege is not allowed to access higher privilege information. Our scheme is efficient in terms of communication and energy overheads.

Acknowledgements

The work in this paper has been supported by Scientific Research Program Funded by Natural Science Basis Research Plan in Shaanxi Province of China (Program No.2011JQ8006) and Shanxi Provincial Education Department (Program No.11JK1060 and 2013JK1132) and National Natural Science Foundation of China (Program No. 61373116) and special funding for key discipline construction of general institutions of higher learning from Shanxi province and special funding for course development from Xi'an University of Posts and Telecommunications.

References

[1] J. Wan, C. Zou, S. Ullah, C.-F. Lai, M. Zhou and X. Wang, "Cloud-Enabled Wireless Body Area Networks for Pervasive Healthcare," IEEE Network, vol. 27, no. 5, **(2013)**, pp. 56-61.
[2] M. Li, W. Lou and K. Ren, "Data Security and Privacy in Wireless Body Area Networks," IEEE Wireless Communications, vol. 17, no. 1, **(2010)**, pp. 51–58.
[3] S. Chatterjee, A. K. Das and J. K. Sing, "A novel and efficient user access control scheme for wireless body area sensor networks," Journal of King Saud University-Computer and Information Sciences, Available online, **(2013)** October 26.
[4] H. Wang, B. Sheng, C. C. Tan, Q. Li, "Comparing symmetrickey and public-key based security schemes in sensor networks: a case study of user access control", In: Proceedings of 28th International Conference on Distributed Computing Systems, **(2008)**.
[5] "Atmel Corporation", Available from: http://www.atmel.com, **(2010)**.
[6] D. He, J. Bu, S. Zhu, S. Chan and C. Chen, "Distributed access control with privacy support in wireless sensor networks", IEEE Transactions on Wireless Communications, vol. 10, no. 10, **(2011)**, pp. 3473–3481.
[7] M. Wen, J. Lei, J. Li, Y. Wang and K. Chen, "Efficient user access control mechanism for wireless multimedia sensor networks", Journal of Computational Information Systems, vol. 7, no. 9, **(2011)**, pp. 3325–3332.

[8] A. A. Mahmud, M. C. Morogan, "Identity-based authentication and access control in wireless sensor networks", International Journal of Computer Applications, vol. 41, no. 13, **(2012)**, pp. 18-24.
[9] H. Wang, B. Sheng and Q. Li, "Elliptic curve cryptography-based access control in sensor networks", International Journal of Security and Networks, vol. 1, no. 3/4, **(2006)**, pp. 127–137.
[10] S. Gajek, T. Jager, M. Manulis and J. Schwenk, "A Browser-Based Kerberos Authentication Schene," Proc. 13th European Symposium on Research in Computer Security, LNCS 5283,Springer,Spain, **(2008)**, pp. 115-129.
[11] W. Wang and X. Liu, "Intuitionistic Fuzzy Information Aggregation Using Einstein Operations," IEEE Trans. Fuzzy Syst., vol. 20, no. 5, **(2012)**, pp. 923-938.
[12] Z. Zhang, H. Wang, A. V. Vasilakos and H. Fang, "ECG Cryptography and Authentication in Body Area Networks," IEEE Transactions on Information Technology in Biomedicine, vol. 16, no. 6, **(2012)**, *pp. 1070-*1078.

Authors

Xu Wu, she received her Ph.D. degree in Computer Science, from the Beijing University of Technology, in 2010. She is an associate professor of Xi'an University of Posts and Telecommunications. She is currently doing postdoctoral research at the MOEKLINNS Lab, Department of Computer Science and Technology of Xian Jiaotong University. Her research interests include trusted computing, pervasive computing, mobile computing, and software engineering. She has published more than 30 technical papers and books/chapters in the above areas.