Cloud-Assisted Privacy Preserving Authentication Scheme for Telecare Medical Information Systems

Presented by:

Sujata Mohanty

Department of Computer Science and Engineering
National Institute of Technology Rourkela
Rourkela, Odisha, 769008, India

OUTLINE

Introduction

- The advancement in technology have made the internet an efficient to utilize for various remote services such as as e-banking, e-rail, e-health etc.
- Telecare Medical Information System(TMIS) one such online service provides facilities to the patient in which both telecare server and patient communicate with each other.
- The innovation of cheaper and robust telecommunication methods makes TMIS a convenient and effortless system.

Introduction (Cont.)

- TMIS helps to reduce proximity between the patient and healthcare systems using the existing network connections.
- However, these network connections might be insecure and prone to various attacks.
- To ensure the authorized and secure communication, user and server should verify each other.

Introduction (Cont.)

- Knowledge factors: e.g. Passwords, PIN numbers
- Possession factors: e.g. Smart cards, Security tokens
- Inherence factors: Biometric, e.g. iris scan, fingerprint, palm print

Introduction (Cont.)

Smart Card

- A smart card is a pocket sized plastic card with an embedded computer chip.
- The chip can either be a microprocessor with internal memory or a memory chip with non-programmable logic.
- They can be programmed to accept, store and send data.

Biometric

- Biometric based scheme has many advantages such as difficult to forget, guess, share, distribute, etc. over password, and smart card based schemes.
- So, the biometric based scheme is more reliable than the password and smart card based schemes.

Related Work

Year	Author	Description
2012	Padhy *et al.*[1]	Suggested a cloud-based healthcare information system model for rural healthcare center.
2014	Chen *et al.* [2]	Introduced a cloud-based medical data exchange protocol to solve the privacy preservation issues.
2016	Chiou *et al.* [3]	Enhanced the Chen et al.'s scheme pointed that the scheme fails to provide user anonymity and message authentication.
2017	Mohit *et al.* [4]	Chiou et al. et al.'s scheme could not withstand stolen mobile device attack and it fails to achieve patient anonymity.
2018	Li *et al.*[5]	Li et al. pointed that Mohit et al.'s scheme insecure against report revelation and report forgery attacks. Also, could not provide patient anonymity and patient unlinkability

The Proposed Scheme

- To overcome the limitations, we have proposed privacy-preserving authentication scheme for TMIS.
- The scheme can achieve patient anonymity as well as resistant to several passive and active attacks.
- We assume that there are four communicating parties.
- The proposed scheme consists of five phases.
  - Registration phase
  - Healthcare center data upload phase (HUP)
  - Patient data upload phase (PUP)
  - Treatment phase (TP)
  - Checkup phase (CP)

Notations Used

Table 1: Notations used

Notation	Description
HC	Health care center
P_i	i^{th} Patient
D_i	i^{th} Doctor
CS	Cloud server
ID_h	Health care center Identity
ID_p	Patient Identity
ID_d	Doctor Identity
$Data_h$	Health care center inspection report
$Data_p$	Patient inspection report
$Data_d$	Doctor inspection report
A_v	Adversary
x, y, z	Master key of cloud CS
$h(\cdot)$	One way hash function
$\oplus$	Bitwise XOR operator
$\Vert$	Concatenation operation

Registration of HC with Cloud Server

Patient(P_i)	Healthcare(HC)	Cloud server(CS)
	Input Health center ID_h	
	$\xrightarrow[(Secure\ channel)]{\{ID_h\}}$	
		Generate a master key x, y, z
		$HC_1 = h(x\|\|111)$
		$HC_2 = h(x) \oplus HC_1$
		$HID_i = h(ID_h\|\|HC_1)$
		$HT_1 = E_{HC_1}(HID_i)$
	$\xleftarrow[(Secure\ channel)]{\{HID_i, HC_2, HT_1\}}$	
	Stores $\{HID_i, HC_2, HT_1\}$	

Performance Evaluation

Table 2: Computational and Communicational Cost Analysis of Scheme

Scheme	Chiou *et al.* [3]	Mohit*et al.* [4]	Li *et al.* [5]	Proposed scheme
Registration phase	–	–	–	$7T_{HS}$+$5T_{EM}$
HUP	$1T_{Sig} + 3T_{BP} + 2T_{EM} + 7T_{HS}$	$1T_{Sig} + 3T_{EM} + 11T_{HS}$	$1T_{Sig} + 3T_{EM} + 11T_{HS}$	$11T_{HS}$+$2T_{EM}$
PUP	$1T_{Sig} + 4T_{BP} + 2T_{EM} + 12T_{HS}$	$2T_{Sig} + 2T_{EM} + 10T_{HS}$	$2T_{Sig} + 4T_{EM} + 10T_{HS}$	$9T_{HS}$+$2T_{EM}$
TP	$2T_{Sig} + 4T_{BP} + 4T_{EM} +$ $7T_{HS} + 4T_{MUL}$	$2T_{Sig} + 3T_{EM} + 9T_{HS}$	$3T_{Sig} + 6T_{EM} + 10T_{HS}$	$8T_{HS}$+$4T_{EM}$
CP	$1T_{Sig} + 2T_{BP} + 2T_{EM} + 8T_{HS}$	$1T_{Sig} + 2T_{EM} + 5T_{HS}$	$1T_{Sig} + 2T_{EM} + 6T_{HS}$	$6T_{HS}$+$2T_{EM}$
Total cost	$5T_{Sig} + 13T_{BP} + 10T_{EM} +$ $33T_{HS} + 4T_{MUL}$	$6T_{Sig} + 9T_{EM} + 35T_{HS}$	$7T_{Sig} + 15T_{EM} + 37T_{HS}$	$41T_{HS}$+$15T_{EM}$
Total Time	2.7705s	2.086s	2.4709s	0.1495s
Communicational Cost	5280 bits	5120 bits	3680 bits	3648 bits

Performance Evaluation

Table 3: Security Comparison of Schemes

Scheme	A1	A2	A3	A4	A5	A6
Chiou *et al.* [3]	×	×	✓	✓	×	✓
Mohit*et al.* [4]	×	×	✓	×	×	✓
Li *et al.* [5]	✓	×	✓	✓	✓	✓
Proposed scheme	✓	✓	✓	✓	✓	✓

$A1$-Patient Anonymity $A2$-Known-key security, $A3$-Report confidentiality, $A4$-Resistance to report forgery attack, A_5-Patient unlinkability, $A6$-Mutual Authentication ✓- Prevent Attack, ×- Attack not prevented.

Conclusion

- We have presented a privacy preservation authentication scheme for TMIS using cloud which achieves patient anonymity even though all the participants can send their data through an insecure channel.
- The proposed scheme is lightweight as we have used hash functions in various phases.
- The scheme is cost effective in terms of computational and communicational cost.
- Due to its low computational cost on the patient's side, a resource constraint device such as mobile is used.

References I

1. Padhy, Rabi Prasad and Patra, Manas Ranjan and Satapathy, Suresh Chandra. Design and implementation of a cloud based rural healthcare information system model *Univers J Appl Comput Sci Technol*, 2(1):149–157, 2012.
2. C.-L. Chen, T.-T. Yang, and T.-F. Shih, “A secure medical data exchange protocol based on cloud environment. *Journal of medical systems*, vol. 38, no. 9, p. 112, 2014.
3. S.-Y. Chiou, Z. Ying, and J. Liu, “Improvement of a privacy authentication scheme based on cloud for medical environment *Journal of medical systems*, vol. 40, no. 4, p. 101, 2016.
4. P. Mohit, R. Amin, A. Karati, G. Biswas, and M. K. Khan, “A standard mutual authentication protocol for cloud computing based health care system *Journal of medical systems*, vol. 41, no. 4, p. 50, 2017.
5. C.-T. Li, D.-H. Shih, and C.-C. Wang, “Cloud-assisted mutual authentication and privacy preservation protocol for telecare medical information systems. *Computer methods and programs in biomedicine*, vol. 157, pp. 191–203, 2018.
6. D. He, N. Kumar, J. Chen, C.-C. Lee, N. Chilamkurti, and S.-S. Yeo, “Robust anonymous authentication protocol for health-care applications using wireless medical sensor networks. *Multimedia Systems*, vol. 21, no. 1, pp. 49–60, 2015.

References II

7. H. Debiao, C. Jianhua, and Z. Rui, “A more secure authentication scheme for telecare medicine information systems. *Journal of Medical Systems*, vol. 36, no. 3, pp. 1989–1995, 2012.

8. P. Pawar, V. Jones, B.-J. F. Van Beijnum, and H. Hermens, “A framework for the comparison of mobile patient monitoring systems. *Journal of biomedical informatics*, vol. 45, no. 3, pp. 544–556, 2012.

9. Z. Tan, “A user anonymity preserving three-factor authentication scheme for telecare medicine information systems. *Journal of medical systems*, vol. 38, no. 3, p. 16, 2014.

10. O. Mir and M. Nikooghadam, “A secure biometrics based authentication with key agreement scheme in telemedicine networks for e-health services. *Wireless Personal Communications*, vol. 83, no. 4, pp. 2439– 2461, 2015.

Thank You!