HASH CHAIN BASED AUTHENTICATED SECURE COMMUNICATION FOR HEALTHCARE SYSTEM

[1]SUNGHYUN CHO, [2]HYUNSUNG KIM

[1,2]Dept. of Cyber Security, Kyungil University
[2]Dept. of Mathematical Sciences, University of Malawi
E-mail: [1]chosh1110@naver.com, [2]kim@kiu.ac.kr

Abstract - With the growing average life expectancy, interest in health has also increased. Ubiquitous healthcare system has been introduced with keen attention these days because medical services are available at any time and any place. Since healthcare environment is based on wireless networks, security vulnerability can be a serious limitation. In this paper, we propose an authenticated secure communication based on hash chain and proxy signature for healthcare environment, which provides anonymity and untraceability. Accordingly, the risk of personal information leakage is removed in the proposed authenticated secure communication scheme. Furthermore, the proposed scheme also provides the required security features for healthcare system. The proposed scheme is expected to be used not only in healthcare environment but also in the fields handling sensitive information.

Index Terms - Healthcare system, Authentication, Public Key Cryptography, Privacy, Hash Chain

I. INTRODUCTION

Advancements in telecommunication and information technology helped to eliminate distance barriers while providing healthcare [1]-[4]. Patient safety security are two important factors that indicate the quality status of health services and are considered the priority in healthcare. Maintaining patient safety is an increasingly complex task, as it involves potential risk and there is no method that can guarantee the absence of errors [5]-[6]. It should be noted that, in healthcare tasks, there is a combination between factors inherent to the environment and human actions, and this is a possible cause of what are called adverse events, which are possibly caused by a combination of environmental factors and human actions.

Big data in healthcare refers to sets of electronic medical health data that are large and complex. Due to their huge volume and complexity, it is difficult to manage those data sets using traditional software and hardware [7]-[9]. The diversity and volume of medical data and efficient accessibility of these datasets make it irresistible. As these systems are integrated with application software, this is an environment in which users' medical sensitivity information is exposed through man in middle attacking, sniffing, etc., where medical services are performed remotely, or by wireless communication [10]-[11]. To solve the problem, Mark and John applied for a patent regarding the provision of security to short message service (SMS) during medical data exchange [12]. The work used mobile phone as a tool for sending the data packets to the medical service station which receive the packets. To ensure the security to communication, the messages were encrypted and signed before being sent. Lee et al. proposed a system that portable mobile healthcare has the potential to reduce long-term costs to improve the quality of medical services, but it also faces many technical challenges [13]. Recently, a system which provides secure transmission of data in distributed wireless medical sensor networks (WMSNs) in hospitals was proposed by Othman et al. [14]. The WMSNs continually update the status of the patient under continuous supervision to the doctor to make emergency decisions on demand based on the sensitive data collected from the body of the patient. Liu et al. proposed a certificateless secure authentication scheme in barns with reduced computational complexity and protection from the adversaries [15]. In order to ensure security to multicast SMS communications with minimized computational and communication overheads, Liu et al.'s protocol differs from the previous works in [11]-[14]. To solve the mentioned research problems, Vijayakumar et al. proposed a secure communication scheme for healthcare system using wearable devices such as sensors are embedded in the body of a patient to continuously monitor the health condition [16]. However, the scheme does not provide privacy of each entity nor integrity of messages.

The purpose of this paper is to solve the security and privacy problems by introducing a new authenticated communication scheme for healthcare system, which is based on a hash chain, elliptic curve cryptosystem (ECC) and symmetric key cryptosystem. Especially, the proposed authenticated communication scheme provides privacy based on dynamic identifier.

II. BACKGROUND

This section reviews the targeting system model and cryptographic preliminaries for the proposed scheme.

A. System Model

The proposed system model consists of patient with mobile phone (Mi), service server (SSi) and hospital management system (HMS). It is assumed that if a patient needs to be constantly monitored based on

sensors, then each patient visits the HMS in person and hands over the necessary details of him (or her) to HMS. The registration details include the patient identity (ID), mobile numbers, corresponding doctor, the ambulance service, an immediate relative who needs to be alerted during emergency situations and so on. On successful registration, HMS creates a secret key and sends it to the mobile phone. Moreover, the details submitted by the patient are used for sending emergency messages.

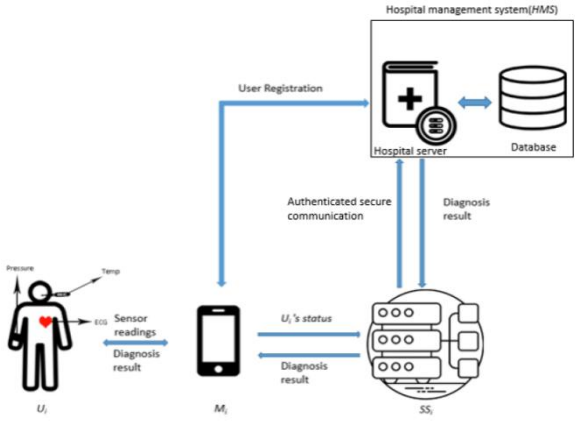


Fig. 1. System model for the proposed scheme

Fig. 1 illustrates the system model for the proposed authenticated secure communication. In the architecture, the patient is constantly monitored for some treatments by HMS. Sensors are fixed in the patients' body for sensing abnormal conditions and the emergency situation, if arises any, shall be informed to HMS via Mi and SSi over the Internet. For this, sensors collect the data such as body temperature, blood pressure and electro cardio gram (ECG). They sent them to Mi through Zigbee or Bluetooth. Mi forms a message and sends it to SSi. SSi after receiving the request from Mi, forwards it to HMS where the patient data is analyzed for any emergency scenarios. If any emergency situation arises, the appropriate message is sent to the entities registered in the healthcare database.

B. Security Preliminaries

This subsection provides basic overviews on a hash chain, ECC and symmetric key cryptosystem [17]. [Hash chain] A hash function is any function that can be used to map data of arbitrary size to data of a fixed size. Hash functions are also useful in cryptography. A cryptographic hash function allows one to easily verify that some input data maps to a given hash value, but if the input data is unknown, it is deliberately difficult to reconstruct it by knowing the stored hash value. By using the concept of one-way hash function, a hash chain was suggested. A hash chain is the successive application of a cryptographic hash function h( ) to a string x. For example, h(h(h(h(h(x))))) gives a hash chain of length 5, often denoted h(5)(x). Advantages derived from mentioned examples are freshness of hash chain, and thus cannot be duplicated by an attacker.

[ECC] ECC is an approach to public key cryptography based on the algebraic structure of elliptic curves over finite fields. ECC requires smaller length of key size compared to non-EC cryptography to provide equivalent security. The properties of the ECC also allows for the assertion of security which are elliptic curve discrete logarithm problem (ECDLP), elliptic curve computational Diffie Hellman problem (ECCDHP) and elliptic curve decisional Diffie Hellman problem (ECDDHP). Each property has different meanings. Assume that A, B, C and D are all points on the elliptic curve, and x and y are integers. When A and B are known in B=xA, x is unknown, which is the difficulty of ECDLP. When B=xA and C=yA is known, D=xyA is unknown, which is based on ECCDHP. When D=xyA is known, B=xA and C=yA is unknown, which is the difficulty of ECDDHP.

[Symmetric key cryptosystem] Symmetric key cryptosystem is a system which uses the same cryptographic keys for both encryption of plain text and decryption of cipher text. The keys may be identical or there may be a simple transformation to go between the two keys. The keys, in practice, represent a shared secret between two or more parties that can be used to maintain a private information link. In the proposed scheme, we use advanced encryption standard (AES) with 128 bits of key size for confidentiality. It is symmetric block cipher which can encrypt and decrypt message.

III. HASH CHAIN BASED AUTHENTICATED SECURE COMMUNICATION

In this part, proposed authenticated secure communication is consisted of 4 phases: setup, user registration, online authenticated communication, and i-th offline authenticated communication. Table I defines notations used in the proposed scheme.

Notation	Definition
p, q	The prime numbers satisfying $q \mid (p\text{-}1)$
P	The generator of the cyclic additive group
M_i	Mobile phone of patient i
SS_i	Service Server i
HMS	Trustable hospital management system server
ID_i	The identity of an entity i
PW_i	The password of M_i
x, x_v	The private keys of HMS
(K, σ)	The proxy key pair of M_i
K_{SH}	A symmetric key between SS_i and HMS
$E_{N1}[M]$	A symmetric encryption of M with the key N_1
$D_{N1}[C]$	A symmetric decryption of C with the key N_1
$h()$	An one-way hash function
SK	A session key
$\oplus$	The XOR operation
$\|\|$	The message concatenation operation

Table I. Notations

A. Setup Phase

HMS selects a symmetric key KSH for SSi, two private keys x and xv and computes the public keys v=xP and yv =xvP. HMS and SSi share KSH, xv and v.

B. User Registration Phase

When an user Ui with a mobile device Mi wants to register to HMS, Ui using Mi inputs an identity IDi and a password PWi, generates a random number d and computes AIDi=h(IDi||d) and APWi=h(PWi||d). Then, Mi sends <AIDi, APWi> to HMS. After receiving the user registration request, HMS generates a random number k and computes a proxy key pair K=kP and σ=x+kh(K)mod q for Mi. Then, HMS stores the proxy key pair (σ, K) in it's database. HMS computes W=h(AIDi||APWi)⊕ (σ||K) and transmits the proxy key pair (σ, K), xv and yv to Mi securely. After that, Mi computes D=h(IDi||PWi)⊕d and Y=h(AIDi||APWi||d) and stores <W, yv, D, Y> in it's SIM card.

C. Online Authenticated Communication Phase

In a service network environment, SSi without having permission to use the health care network needs online authentication steps to obtain permission to access data through HMS. For online authentication session, Mi computes h(1)(n1||n2), h(2)(n1||n2), … h(n+1)(n1||n2) using SSi's random number n1 and it's own random number n2 and stores it in it's database where n is the total number of offline authentications. Fig. 2 shows the steps of it and the detailed processes are as follows.

Step 1: Mi sends a login request to SSi.

Step 2: SSi generates a random number n1 and sends {n1, n, IDA} to Mi.

Step 3: Mi asks user to input IDi' and PWi' into SIM card and SIM card generates a random number n2, computes a hash chain based on n1 and n2, keeps the hash chain in it's memory and retrieves N1=h(n+1)(n1||n2) from the hash chain. After that, it computes d'=D⊕ h(IDi'||PWi'), AIDi'=h(IDi'||d'), APWi'=h(PWi'||d') and Y'=h(AIDi'||APWi'||d'). Then, SIM card checks if Y is equal to Y'. If not, SIM card stops the session. Otherwise, SIM card withdraws (σ'||K')=W⊕h(AIDi' ||APWi'), forms a message M and computes C1= EN1[M] and M1=N1⊕K'. Then SIM card generates a random number t, computes r1=tP, r2=IDi⊕h(tyv), s=σ'h(M1||IDA||IDi||r1||C1)+t mod q and V1=h(r1|| r2||s||M1||C1||IDA||IDi) and sends {r1, r2, s, V1, M1, C1} to SSi.

Step 4: SSi computes tyv'=xv·r1, IDi'=r2⊕h(tyv') and V1'=h(r1 ||r2||s||M1||C1||IDA||IDi') and checks if V1 is equal to V1'. If the validation is failed, it terminates the session. Otherwise, SSi generates a random number n3 and computes C2=EKSH[n3||IDi'] and V2=h(IDA||IDi'||M1||C1||C2||n3||s||r1) and sends {IDA, V2, M1, C1, C2, s, r1} to HMS.

Step 5: HMS decrypts n3'||IDi''=DKSH[C2] and computes V2'=h(IDA||IDi''||M1||C1||C2||n3'||s||r1). Then HMS checks if V2 is equal to V2'. If not, HMS stops the session. Otherwise, HMS withdraws K from it's database by using IDi'', computes sP and h(M1||IDA ||IDi''||r1||C1)(v+Kh(K))+r1 and checks whether the computed two values are same. If not, HMS stops the session. Otherwise, HMS computes N1'=M1⊕K and decrypts M'=DN1'[C1]. HMS generates a random number n4, forms a reply message R, computes Cn=EN1'[R], C3=EKSH[n4], SK=h(N1'||n3'||n4||σ), CT1= SK⊕K, V3=h(Cn||C3||CT1||n4), V4=h(Cn||C3||CT1 ||SK) and sends {Cn, C3, CT1, V3, V4} to SSi.

Step 6: SSi decrypts n4'=DKSH[C3], computes V3'= h(Cn||C3||CT1||n4') and checks if V3'=V3. If the validation is successful, SSi sends {Cn, C3, CT1, V4} to Mi. Otherwise, SSi stops the session.

Step 7: SIM card computes SK'=CT1⊕K and checks if V4 is the same as h(Cn||C3||CT1||SK'). If not, SIM card stops the session. Otherwise, SIM card computes R'=DN1[Cn].

D. i-th Offline Authenticated Communication Phase

Mi retrieves h(n-i+1)(n1||n2) from its database and sends ECi[h(n-i+1)(n1||n2), M] to SSi and HMS. After receiving the encrypted message, HMS decrypts the message and computes h(h(n-i+1)(n1||n2)). SSi and HMS checks if h(h(n-i+1)(n1 ||n2)) is the same to h(n-i+2)(n1||n2). If the result is true, SSi and HMS replace h(n-i+2)(n1||n2) with h(n-i+1)(n1||n2) and computes a new session key Ci+1= h(h(n-i+1)(n1||n2), Ci) and increases i=i+1.

IV. SECURITY AND PERFORMANCE ANALYSIS

In this section, we will describe security analysis and performance analysis of the proposed authenticated secure communication scheme.

A. Security Analysis

Security analysis is focused on user anonymity, password guessing attack, stolen smart card attack and replay attack. Furthermore, we provide the security comparison with Vijayakumar et al.'s scheme in [16] as shown in Table II.

UA-User anonymity: Based on the design of our scheme, user anonymity can be guaranteed by using amplified identity. Attacker cannot know Mi's real identity by conducting security attacks in our scheme. In online authenticated communication phase, Mi only use the amplified identity r2=IDi⊕h(tyv). Thus, there is no way attacker withdraw IDi from r2 without knowing xv. It means that identity of Mi is sent to the other entity in amplified with secret, and the identity will be randomized at each session's random number, which is based on ECDLP. As a result, our scheme can provide user anonymity.

PG-Password guessing attack: In user registration phase, user uses IDi and PWi and password related value is stored in SIM card as Y=h(AIDi||APWi||d), which APWi is computed as h(PWi||d). Even HMS only knows APWi but not PWi itself. Although the privileged-insider of HMS can obtain the registration message <AIDi, APWi>, it is unable to know the user's PWi because PWi is amplified with the random number d. Note that deriving PWi from APWi is equal to the brute-force attack to crack the one-way hash function. Hence, our scheme eliminates the possibility of password guessing attack.

SC-Stolen smart card attack: Assume that SIM card of Mi stored values <W, yv, D, Y> and try to impersonate Mi to is lost or stolen to an attacker. The attacker could get the stored values <W, yv, D, Y> and try to impersonate Mi to



Fig. 2. Online authenticated communication phase

successfully login to SSi. The attacker cannot guess correct IDi and PWi at the same time and compute d'=D⊕h(IDi||PWi), AIDi'=h(IDi||d'), APWi'=h(PWi||d'), and Y'=h(AIDi'||APWi'||d'). In the proposed scheme, the probability of guessing both of them is approximately 1/(26l+6m) where IDi is assumed to be composed of exact l characters and PWi with m characters. This probability is negligible, and the attacker has no feasible solution to derive IDi and PWi in a polynomial time.

RA-Replay attack: The random numbers are common countermeasure to prevent replay attack in the authentication process. Since the messages {n1, n, IDA}, {r1, r2, s, V1, M1, C1}, {IDA, V2, M1, C1, C2, s, r1}, {Cn, C3, CT1, V3, V4} and {Cn, C3, CT1, V4} contain fresh random numbers n1, n2, n3, n4, and t. Furthermore, these random numbers are also embedded in the messages. Thus, each participant first checks the freshness of the received random numbers and verifies whether the correct random numbers are present in the messages. Hence, this design of the proposed scheme discards the possibility of replay attack, which is based on ECDLP, ECCDHP and ECDDHP.

Security / Scheme	UA	PG	SC	RA
Vijayakumar et al.'s	No	Yes	Yes	Yes
Proposed	Yes	Yes	Yes	Yes

Table II. Security comparison

B. Performance Analysis

In this section, we analyze computation overheads of the proposed scheme and provide comparisons with Vijayakumar et al.'s scheme in [16]. To facilitate the evaluation of it, TA, TS and Th are defined as the time cost of an ECC point multiplication, an AES encryption and decryption and a hash function, respectively. Generally, TA is much larger than TS and Th, and according to the reference [18], TA, TS and Th are 0.427576 ms, 0.0214835 ms and 0.005174 ms, respectively. Table III shows the performance comparisons of the online authenticated secure communication phase of the proposed scheme with Vijayakumar et al.'s scheme.

Scheme / Entity	Vijayakumar et al.'s	Proposed
User (M_j)	$4T_S+1T_A$	$9T_h+2T_S+2T_A$
SS_j (HAM)	$4T_S$	$4T_h+2T_S+1T_A$
HMS (AuS_j)	$4T_S+1T_A$	$5T_h+3T_S+2T_A$
Total	$12T_S+2T_A$ =1.112954 *ms*	$18T_h+7T_S+5T_A$ =2.3813965 *ms*

Table III. Computation costs comparison of online phase Scheme Entity Vijayakumar et al.'s Proposed

It can be seen from Table III that the proposed scheme almost needs double computation costs compared to Vijayakumar et al.'s scheme. However, the online phase is only required once to our scheme but the other sessions require the offline phase as shown in Table IV, which requires only 5% overhead than the other one.

Protocol / Feature	Vijayakumar et al.'s	Proposed
User (M_j)	$4T_S+1T_A$	$1T_S$
SS_j (HAM)	$4T_S$	$1T_h$
HMS (AuS_j)	$4T_S+1T_A$	$1T_h+1T_S$
Total	$12T_S+2T_A$ =1.112954 *ms*	$2T_h+2T_S$ =0.053315 *ms*

Table IV. Computation costs comparison of offline phase Protocol Feature Vijayakumar et al.'s Proposed

CONCLUSION

In this paper, we proposed an authenticated secure communication for healthcare system to provide security and privacy. In the proposed scheme, a secure mutual authentication is achieved among three entities by obtaining the proxy delegation from HMS. In the meantime, a session key is also established between communication entities. The analysis proves that the scheme provides security and privacy. The performance analysis shows that the proposed scheme has compatible efficiency compared to the related scheme. It is also expected that the proposed scheme will strengthen the security and the privacy of healthcare system in various scenarios.

ACKNOWLEGDEMENTS

Hyunsung Kim is the corresponding author. This work was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (NRF-2017R1D1A1B04032598).

REFERENCES

[1] K. A. Wager, F. W. Lee, J. P. Glaser, Health Care Information Systems: A Practical Approach for Health Care Management, Jossey-Bass, Mar. 2017.

[2] S. Challa, A. K. Das, V. Odelu, N. Kumar, S. Kumari, M. K. Khan, A. V. Vasilakos, "An efficient ECC-based provably secure three-factor user authentication and key agreement protocol for wireless healthcare sensor networks," Computers and Electrical Engineering, vol. 69, pp. 534-554, 2018.

[3] K. Mtonga, E. J. Yoon, H. Kim, "Authenticated Privacy Preserving Pairing-Based Scheme for Remote Health Monitoring Systems," Journal of Information Security, vol. 8, no. 1, pp. 75-90, 2017.

[4] H. Kim, S. W. Lee, "Freshness Preserving Secure Data Gathering Protocol over Wireless Sensor Networks," International Journal of Control and Automation, vol. 8, no. 6, pp. 411-420, 2015.

[5] D. C. Kaelber, D. W. Bates, "Health information exchange and patient safety," Journal of Biomedical Informatics, vol. 40, no. 6, pp. S40-S45, 2007.

[6] H. Koivula-Tynnila, A. Axelin, H. Leino-Kilpi, "Informational Privacy in the Recovery Room-Patients' Perspective," Journal of PeriAnesthesia Nursing, vol. 33, no. 4, pp. 479-489, 2018.

[7] M. Chen, J. Yang, Y. Hao, S. Mao, and K. Hwang, ''A 5G cognitive system for healthcare,'' Big Data Cognitive Computing, vol. 1, no. 1, 2017
[8] S. S. Ketkar, D. D. Sawant, "Big Data: Theory, Challenges and Application's Roadmap," Asian Journal of Convergence in Technology, vol. 2, no. 3, 2016.
[9] M. Chen, S. Mao, Y. Liu, ''Big data: A survey,'' Mobile Networks and Applications, vol. 19, no. 2, pp. 171-209, Apr. 2014.
[10] E. Mehraeen, H. Ayatollahi, M. Ahmadi, "Health Information Security in Hospitals: the Application of Security Safeguards," Journal of Academy of Medical Sciences of Bosnia and Herzegovina, vol. 23, no. 1, pp. 47-50, 2016.
[11] B. K. Sarkar, "Big data for secure healthcare system: a conceptual design," Complex & Intelligent systems, vol. 3, no. 2, pp. 133-151, 2017.
[12] L. Mark, F. John, "Remote control of medical devices using instant messaging infrastructure," U. S. Patent CA2718696 A1, Dec. 7, 2011,
[13] D. H. Lee, A. Rabbi, J. Choi, R. Fazel-Rezai, "Development of a mobile phone and e-health monitoring application," International Journal of Advanced Computer Science and Applications, vol. 3, no. 3, pp. 38-42, 2012.
[14] S. B. Othman, A. Trad, H. Youssef, "Security architecture for at-home medical care using wireless sensor network," Proc. Of International Conference on Wireless Communications and Mobile Computing Conference, pp 304-309, 2014.
[15] J. Liu, Z. Zhang, X. Chen, K. S. Kwak, "Certificateless remote anonymous authentication schemes for wireless body area networks," IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 2, pp. 332-342, 2014.
[16] P. Vijayakumar, P. Pandiaraja, M. Karuppiah, L. J. Deborah, "An efficient secure communication for healthcare system using wearable devices," Computers and Electrical Engineering, vol. 63, pp. 232-245, 2017.
[17] B. Schneier, "Applied Cryptography: Protocols, Algorithms, and Source Code in C," John Wiley & Sons, 1996
[18] F. Wu, L. Xu, S. Kumari, X. Li, A. K. Das, M. K. Khan, M. Karuppiah, R. Baliyan, "A novel and provably secure authentication and key agreement scheme with user anonymity for global mobility networks," Security and Communication Networks, vol. 9, pp. 3527-3542, 2016.

★★★