Jurnal Ilmu Komputer dan Informasi (Journal of a Science and Information). 11/1 (2018), 1-9
DOI: http://dx.doi.org/10.21609/jiki.v11i1.562

SECURING COMMUNICATION IN THE IOT-BASED HEALTH CARE SYSTEMS

Bayu Anggorojati[1] and Ramjee Prasad[2]

[1]Faculty of Computer Science, Universitas Indonesia, Kampus UI, Depok, 16424, Indonesia
[2]Future Technologies for Business Ecosystem Innovation (FT4BI), Aarhus University, Nordre Ringgade 1, 8000 Aarhus, Denmark

E-mail: ramjee@btech.au.dk

Abstract

Rapid development of Internet of Things (IoT) and its whole ecosystems are opening a lot of opportunities that can improve humans' quality of life in many aspects. One of the promising area where IoT can enhance our life is in the health care sector. However, security and privacy becomes the main concern in the electronic Health (eHealth) systems and it becomes more challenging with the integration of IoT. Furthermore, most of the IoT-based health care system architecture is designed to be cross-organizational due to many different stakeholders in its overall ecosystems – thus increasing the security complexity. There are several aspects of security in the IoT-based health care system, among them are key management, authentication and encryption/decryption to ensure secure communication and access to health sensing information. This paper introduces a key management method that includes mutual authentication and secret key agreement to establish secure communication between any IoT health device with any entity from different organization or domain through Identity-Based Cryptography (IBC).

Keywords: *IoT, eHealth, Security, Authentication, ID-based cryptography*

Abstrak

Perkembangan Internet yang cepat dari Things (IoT) dan keseluruhan ekosistemnya membuka banyak kesempatan yang dapat memperbaiki kualitas hidup manusia dalam banyak aspek. Salah satu area yang menjanjikan dimana IoT dapat meningkatkan kehidupan kita ada di sektor perawatan kesehatan. Namun, keamanan dan privasi menjadi perhatian utama dalam sistem Kesehatan Elektronik (eHealth) dan ini menjadi lebih menantang dengan integrasi IoT. Lebih jauh lagi, sebagian besar arsitektur sistem perawatan kesehatan berbasis IoT dirancang untuk menjadi lintas organisasi karena banyak pemangku kepentingan yang berbeda dalam keseluruhan ekosistemnya - sehingga meningkatkan kompleksitas keamanan. Ada beberapa aspek keamanan dalam sistem perawatan kesehatan berbasis IoT, di antaranya adalah manajemen kunci, otentikasi dan enkripsi / dekripsi untuk memastikan komunikasi yang aman dan akses terhadap informasi penginderaan jauh. Makalah ini memperkenalkan metode manajemen kunci yang mencakup saling otentikasi dan kesepakatan kunci rahasia untuk membangun komunikasi yang aman antara perangkat kesehatan IoT dengan entitas dari berbagai organisasi atau domain melalui Identity-Based Cryptography (IBC).

Kata Kunci: *IoT, eHealth, Keamanan, Autentikasi, Kriptografi berbasis ID*

1. Introduction

The convergence of IT and medical world – also known as eHealth – have been transforming the way health care services are delivered. eHealth offers a new means for utilizing health resources, such as information, money, medications, etc, and then help all the relevant stakeholders to utilize those resources more efficiently [1]. For a country that has high population where some of them are living in remote areas, such as Indonesia that consists of thousands of islands, delivering health care services is a big issue especially when the specialist doctors are not well distributed throughout the country [2], [3]. In such situation, tele monitoring of patients' health status by using electronic medical devices that is able to communicate remotely through Internet with the advancement of IoT is a promising solution.

Various IoT health care services and applications have been introduced, such as ECG! (ECG!), glucose level, and blood pressure monitoring, medication management, and a lot more health applications for smart phones, as reported in [4]. Furthermore, many well known companies are developing more products and services within the IoT for health care solutions [4]. It was also reported by McKinsey Global Institute in [5] that the IoT-based health care applications are projected to create about $1.1 - $2.5 trillion in

growth annually by the global economy by 2025 and form the biggest economic impact compared to the IoT applications in other areas. It shows that the IoT in health care has a very bright future, both in terms of benefits for people, technology and economy.

With all those encouraging facts about IoT-based health care solution, there lies big concern about security and privacy. There are many security and privacy challenges pertaining IoT-based health care system, such as physical attack and device vulnerabilities, security in the communication channel and ecosystem (e.g. mutual authentication, key management and cryptographic support), attack on the stored information, etc [1], [6]. On the other hand, an IoT device that transmit patient's health information needs to comply with Health Insurance Portability and Accountability Act (HIPAA). The IoT devices are also considered as having limited power, computation and memory capability which imply that the security mechanism needs to utilize the device's resources efficiently. Furthermore, the architecture of IoT-based health care system in general involves several stakeholders that belong to different organizations with different security domain and policy, which is adding more complexity to the security task.

Based on the circumstances mentioned earlier, it is important to provide key management that supports mutual authentication and secure data transmission between two entities within the IoT-based health care system that belong to different organizations or domains. This paper presents a security scheme based on IBC that supports all the capabilities stated before. The IBC-based scheme is chosen because it is essentially a asymmetric key scheme, which is easier in key distribution and more scalable than the symmetric ones, while it requires no certificate in the practical key distribution like the other asymmetric key schemes, e.g. Rivest, Shamir, and Adelman (RSA) and Elliptic Curve Cryptography (ECC). The scheme provides mutual authentication and key agreement for secure communication between entities across different organizations or domains, and is developed based on variant of Identity-Based Encryption (IBE) that removes the key escrow problem in original IBC which was introduced by Zhaohui Cheng et al. in 2004 [7].

The rest of this paper is structured as follows: Security and privacy challenges especially in the context of IoT-based health care system are reviewed in Section II. The IoT-based health care system architecture that is referred in this work is presented in Section III. The proposed key management, authentication and key agreement scheme is explained in Sec- tion IV. The security and efficiency analysis of the proposed scheme is discussed in Section V. Finally the conclusion and some future works are given in section VI.

2. Methods

Security Challenges and Possible Solutions

This section reviews some of the security challenges on the IoT-based health care system. The challenges consists of two main categories: challenges concerning the inherent nature of IoT which impact the security solution and security challenges related to the IoT system, especially in health care area. Further, some possible solutions of the reviewed challenges are also presented based on some related works.

IoT health devices are embedded with low-speed processors. The central processing unit (CPU) in such devices is not very powerful in terms of its speed. In addition, these devices are not designed to perform computationally expensive operations. That is, they simply act as a sensor or actuator. Therefore, finding a security solution that minimizes resource consumption and thus maximizes security performance is a challenging task [4]. On the other hand, the number of IoT devices has increased gradually, and therefore more devices are getting connected to the global information network. thus, designing a highly scalable security scheme without compro- mising security requirements is another challenge [4].

Medical data contain very sensitive information about patient's health status that must be kept secure and private from any unauthorized people. Hence, hospitals and health care providers are obligated to exchange patients private information securely to comply with HIPAA. With the ubiquitous and pervasive nature of IoT, security breaches and privacy violations are highly possible if the automatic data collection is not verified and managed properly. Patients' sensitive personal and medical information could be a tampered, used or compromised in the absence of having real time monitoring. This will not only cause a threat to infrastructure but has a catastrophic impact of peoples lives. Malicious users could hijack applications and wearable devices taking control of peoples private information and introduce a devastating health and security risks [6].

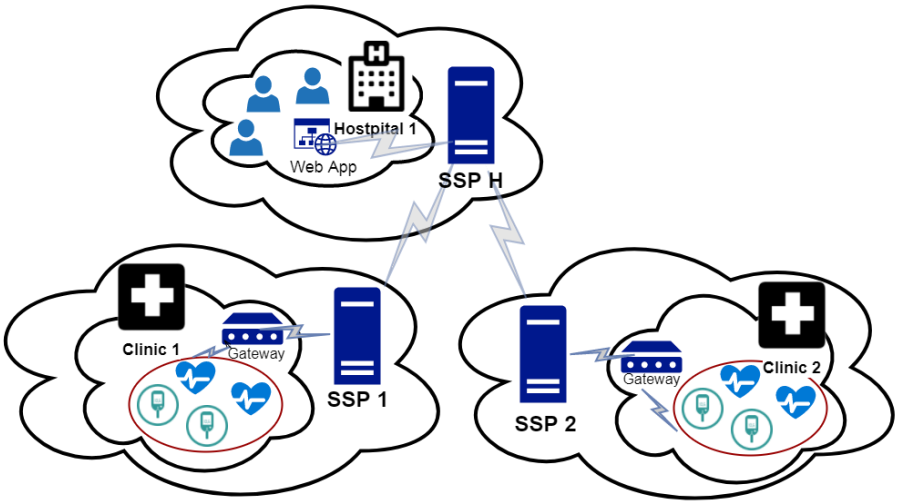

Figure 1. Reference architecture of IoT-based health care across domains

The other challenge is managing credentials and controlling access to applications and patients confidential information. For instance, medical care givers are allowed to access devices in response to patients sensor devices request but the internet connection used may be a public or insecure Wi-Fi network that can be easily tampered to conduct man-in-the-middle attacks. Many authentication techniques could be implemented so that patients are capable to verify and allow medical doctors to access their internally embedded devices. but all of the sudden they lost conscious and they are still desperate to get doctors assistance and guidance. Some IoT healthcare manufacturing companies provide a permanent hard coded password to be used while accessing IoT devices which, the passwords are publicly available in the device manual and would be used to misconfigure the device that introduce risk to patient life [6].

Another challenge is implementing and deploying cryptographic protocols in IoT health cloud correctly. Managing cryptographic keys is crucial but strenuous due to IoT pervasive and continuous capabilities. IoT ecosystem demands the use of concurrent authentication operation with quick real time respose [6].

HIPAA regulation related to Transmission Security Encryption 164.312(e)(2)(ii) mention that entities should implement a mechanism to encrypt and decrypt patient's health information whenever deemed appropriate. Entities shall prepare documentation of the encryption technology that is implemented including policies and procedures, how cryptographic key management are exchanged and restricting access to create and alter cryptographic keys. Furthermore, hardening the con- fidential processes such as managing and sharing keys is also should be audited and enforced [6].

Several security schemes that attempted to solve issues related to the IoT in various applications have been proposed, in which the approaches can also be applied in the health care area. The issue of secure transmission in IoT as required in HIPAA regulation is strongly connected with cryptographic protocols given the fact that IoT consists of constrained-devices (e.g. low computation, memory and power) and big numbers of IoT nodes that has scalability implications. Furthermore, the used for encryption in secure communication needs proper management which is also related to the authentication.

Initially, symmetric key cryptography based scheme was extensively researched due to its small key size that fits the requirement of constrained devices. However, it suffers from major drawback in scalability. In order to address scalability issue, some attempts to introduce Public Key Cryptography (PKC) based scheme in constrained devices have also been made. It have been shown that it is computationally feasible to implement PKC in constrained device, especially by using ECC which require shorter key size compared to RSA based PKC. An example of Public Key Infrastructure (PKI) based encryption implementation in IoT m-health devices was pre- sented in [8].

Yet, traditional PKC requires certificate which consumes bigger memory size and complex to manage. To overcome this shortcoming, a certificateless PKC scheme, known as IBC [9], [10], has been proposed. The basic idea of original IBE is, first there is a central entity called Private Key Generator (PKG) which is responsible to generate some public parameters and a master key that is

kept secret. That master key is then used to generate private keys for all other parties, who trust that particular PKG, given their IDs. Now, the encryption-decryption process can be done in the same manner as the traditional PKC with an exception that the public key can be generated by any entity using a known ID. Due to its benefits, e.g. certicateless and low resource requirements, some IBC based security schemes have also been applied for constrained device, such as Mobile Ad-hoc Networks (MANET) [11]. In IBC, any arbitrary string, such as the identity of participating party in communication, can be used as public key, thus replacing the role of certificate in traditional PKC.

Several IBC schemes have also been proposed for IoT. A key establishment scheme between two communicating entities in which one of them is constrained device and with the help of a proxy is proposed in [12]. An IBC protocol design pattern for Machine-to-Machine (M2M) was proposed in [13]. Federated end-to-end authentication for constrained IoT using IBC and ECC has been suggested by Markmann et al. [14]. Finally, an IBC based authentication scheme for M2M has also been proposed by Shuo Chen et al. [15].

Security Challenges and Possible Solutions

This section reviews possible architecture of IoT-based health care system from several references. Based on the reviews, a reference architecture will be chosen for this work. Furthermore, the chosen reference architecture will be used as a use case scenario for building our proposed security scheme.

According to Gabriel Neagu et al. [16], the sensing services delivered by IoT in general is based on interaction of four entities: sensor owners (SO), sensor publishers (SP), extended service providers (ESP), and sensor data consumers (SDC). The SO might be a private or a public organization, a commercial sensor provider or an individual. In case the SO decides that the data provided by these sensors will be available in the cloud it has to define the access policy to these data that potential SP should implement and potential users should comply with. When a SDC (e.g. government, business organization, academic institution, scientific research community or individual) is interested in accessing data provided by a published sensor, the SP mediates a service agreement between this SDC and respective SO where the SO responsibilities regarding sensing data availability and quality for the requested period of time, as well as their compliance with existing standards are detailed.

Another entity called Sensing Service Provider (SSP) was also introduced in [16] which simplifies the interaction between SDC and other entities in its interests, including SO (for data availability, compliance and quality), SP (for access services to sensor data) and other extended service providers (for value added services). In health care specific scenario, SDC could be a medical institution (e.g. hospital, clinics, etc) or any health care service provider. Depending on available financial, human and technical resources, those SDC in health care may decide to implement IoT-based health care service either as an extension of their existing IT infrastructure or by outsourcing it to specialized providers. In most cases, the second option would be more preferable especially by small medical institutions (e.g. clinics, general practitioners). Finally, the authors in [16] proposed that the SSP is a major actor who interacts with other stakeholders: SO, SP and health care provider as SDC.

On the practical perspective, there can be many different ways of architecture design and deployment model of IoT-based health care system. According to [3], one of the ongoing telehealth pilot project in Indonesia, called tele-ECG!, is carried out in such a way that a well known cardiac hospital becomes the center of the project and it is serving other remotely located health care providers. Remote health care providers that lack of cardiologists may send the ECG! data of their patients to the cardiologists that belong to the referred hospital through tele-ECG! to get their diagnosis pertaining the cardiac issues of the patients' in the remote area.

Combining the proposed model in [16] and the scenario presented in [3], a reference architectural model that will be used to develop our security use case is proposed in Figure 1. The model shown in Figure 1 is a simplified version of the model from [16], in which SP is assumed to be the SSP itself and the SO is part of the health care providers (Clinic 1 and 2), while Hospital 1 is the SDC. It is also assumed that each of the health care provider outsourced the IoT-based health care system to a specialized provider (e.g. SSP 1, SSP2 and SSP H).

Concerning the proposed IBC security scheme which requires PKG, the reference architecture in Figure 1 will have three PKG for each SSP domain, e.g. P KGSSP 1 ,P KGSSP 2 and P KGSSP H. For security reason, PKG is only accessible by entities within its domain. As PKGs, they generate master secret keys and public parameters for each domain. Additionally, P KGSSP 1 and P KGSSP 1 also generates identities and corresponding private keys for all devices in each domain, including S1/S2, device gateways and medical sensors. Besides, the P KGSSP H

TABLE 1.
SUMMARY OF ALL ALGORITHMS IN IBE WITHOUT KEY ESCROW

Algorithm	Input	Output
Setup	1^K: a security parameter	*s*: system's master-key (private) params: system's public parame- ters
Extract	ID: Identity *s* and params	QID: public key dID: private key
Publish	params	tID: sub-private key NID: sub-public key
Encrypt	*m*: plaintext ID, params, NID	*C*: ciphertext
Decrypt	*C*: ciphertext $dID, t,$ params	m': plaintext

generate private keys for all registered users in Hospital 1. It is important to note that the user identity in hospital domain are created in registration process and then the private key is generated accordingly by the P KGSSP H .

Proposed Method

IBE Scheme without Key Escrow

As earlier mentioned, the proposed scheme is developed based on a variant of IBE that is key-escrow free which is adapted from [7]. In the original IBE scheme by Boneh Franklin [10], there are four randomized algorithms involved, namely Setup, Extract, Encrypt, and Decrypt, while another algorithm called Publish is included in the IBE's variant without key escrow. A summary of inputs and outputs for all five algorithms is listed in Table 1, while the detail procedures can be reviewed in [7].

Please note that the Setup algorithm occur fully in the PKG which could happen, for instance in the system initialization. In the Extract algorithm, the PKG receives an input ID from a communicating entity, then after the algorithm is executed in the PKG, QID is published in a publicly available directory while dID is sent to the communicating entity secretly. Finally, the rest of the algorithms (i.e. Publish, Encrypt and Decrypt) happen in the communicating entity, except that NID as one of the results of Publish algorithm is published in a public directory.

Before explaining the other mechanisms in the proposed schemes, i.e. system and device initialization as well as authentication with key agreement, the definitions of the notations used in the proposed scheme is defined in Table 2.

System and Device Initialization

System initialization refers to the process related to IBE when PKG of an SSP! (SSP!) is started, while device initialization refers to the process followed when gateway and constrained device join the SSP!. During system initialization, the most important operation is generating params and master-key, then making params publicly available as explained in the previous section. In addition to that, it is important for the PKG of SSP! to have an identifier that is recognized by everybody(thing) through the Internet. Therefore, we propose the domain name as the primary identity representing the IoT Service Provider (IoTSP) and then the device identity will be appended with this domain name. Having such identifier scheme is beneficial in the lookup process even though the communicating entity is located in different domain.

With regards to the device initialization, there are two important mechanisms need to be performed, i.e. generation and distribution of device identifier and associated private key of the device by the PKG, and then the generation of sub-public and sub-private key pair by the device itself. In principle, distribution of device's identifier and the corresponding private key by PKG can either be done offline and online. Offline method requires configuration of identifier and corresponding private key statically during the flashing time of the device, while online method can be done more dynamically. In this case, online method is chosen and a secure way of delivering device's private key is proposed.

The proposed online device initialization is secured by two symmetric keys, namely KInitReq and KInitRsp, which are one-time randomly generated, i.e. they will be destroyed after device initialization. There can be several ways in obtaining those keys. One practical way is by performing a device registration through web interface. After the registration process, unique device identifier, KInitReq and KInitRsp will be gen- erated for and transfered to the registered device (e.g. they can be loaded to the device by cable data after downloading from PKG). The reason why unique device identifier is generated at this point because it is possible to include more human friendly name into it, such as type of device (gateway, ECG, diabetic sensor, etc) and location of the device (hospital 1 or house 1, etc). Afterwards, the device can request its identifier and corresponding private key securely using Authenticated Encryption with Associated Data (AEAD) [17]. The reason of choosing AEAD being that it is more secure to properly authen-

TABLE 2.
DEFINITION OF USED NOTATIONS

Notation	Definition
s	Master secret key
paramsx	Public system parameter of domain x
IDi	Identity of entity i
Qi	Public key of corresponding entity i
di	Private key of corresponding entity i
Ni	Sub-public key of corresponding entity i
ti	Sub-private key of corresponding entity i
Pm	Plaintext from a message m or a result of decryption
Cm	Ciphertext, a result of encrypting message m
E(k, N, P, A)	AEAD encryption of plaintext P, using key k, nonce N and associated data A
D(k, N, C, A)	AEAD decryption of ciphertext C, using key k, nonce N and associated data A
Eij(m)	ID based encryption of message m using Qj, Nj, and ti
Dij (m)	ID based decryption of message m using Qj, Nj, and ti
Sm	Digest of message m as a result of Message Authentication Code (MAC)

ticate the ciphertext than having simply the encryption, while it works faster than secure implementation of Hash-based Message Authentication Code (HMAC) that requires two keys for encryption and authentication. The detail protocol of secure device initialization is shown in Fig. 2.

Authentication Mechanism with Key Agreement

Fig. 3 illustrates a scenario that using the proposed authentication mechanism with key agreement. In this scenario, a mobile application's user A wants to access sensor B that belongs to an IoTSP domain. For simplicity, user A and sensor B will be referred as A and B respectively from this point onwards. Moreover, A has to go through IoT Server (IoTS) as the entry point to B. It is assumed that the activity of A in this scenario is done by the mobile app (either the mobile app itself or the server that provides API to mobile app), hence it is shown as one entity in Fig. 3. It can also be assumed that practically the entity in each domain (initially) does not have knowledge of system parameters and sub-public key of entities in other domains, therefore a lookup function needs to take place before encryption is performed. Detail of authentication mechanism is explained as follows: (1) First of all, A performs lookup in order to obtain paramsIoT SP and NIoT S by using IDIoT S as input. After successful lookup, it generates QIoT S = H1IoT SP (IDIoT S), where H1IoT SP is included in paramsIoT SP. Note that other paramters in paramsIoT SP are also used for encryption. After-wards, C1 is created by encrypting IDA, IDB, and timestamp T using QIoT S, NIoT S and tA as keys. Here T is used to prevent replay attack. Then, IDA, IDIoT S, and C1 are sent to IoTS; (2) After receiving message from A, IoTS will perform lookup based the received IDA, to obtain paramsM A and NA. After successful lookup, it decrypts C1 using dIoT S, tIoT S and NA to obtain IDA, IDB, and T. After that, T is validated, and IDA is also verified if it similar with the received one. If they are valid the process is continued else, it stops and sends error message to A. After successful validation, a message that contains NB is encrypted as C2 using QA, NA and tIoT S, then C2 is sent to A. Another message that contains paramsM A and NA is encrypted as C3 by using QB, NB and tIoT S and then it is sent to B, informing that A wants to access it; (3) Upon receiving C2, it is then decrypted by A using dA, tA and NIoT S to obtain NB. Afterwards, A generates nonceA, then encrypt it along with IDA using QB, NB and tA as C4 and finally sends it to B; (4) Upon receiving C3 from IoTS, B decrypts it using dB, tB and NIoT S to obtain paramsM A and NA; (5) After receiving C4 from A, B decrypts it using dB, tB and NA to obtain nonceA. B then generates nonceB and use it along with nonceA and IDB to generate shared secret key with A, kBA, using a key derivation function such as HMAC-based Key Derivation Function (HKDF) [18]. After that, IDB and nonceB is encrypted using QA, NA and tB as C5 and a digest S1 is created using a message authentication code, such as HMAC [19], from message that consists of IDB, IDA, and nonceA with key kBA. Then, IDB, IDA, C5 and S1 are sent to A; (6) After C5 and S1 are received by A, C5 is decrypted by using dA, tA and NB to obtain nonceB. After obtaining nonceB, kBA is generated from nonceA, nonce and ID. After that, another S/ is generated the same way as B generated it using newly created kBA, and it is then verified against the received S1. After S1 is verified, another digest S2 is created from IDA, IDB, and nonceA with kBA and then sent to B; (7) After S2 is received, it is then verified by B. After successful verification both A and B will use kAB as they shared secret key.

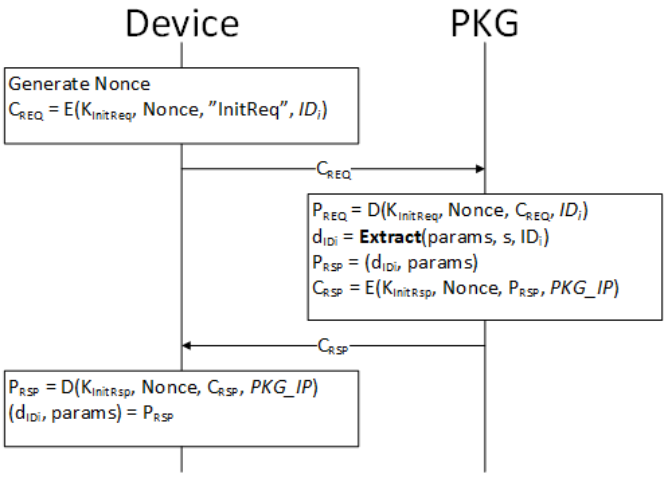

Figure 2. Device initialization protocol in a SSP! Domain

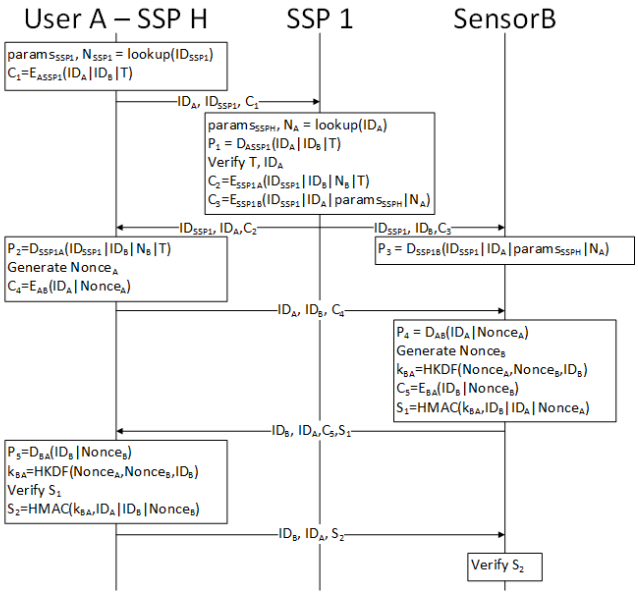

Figure 3. Authentication mechanism with entity in different domain

By the end of this phase, both user A and sensor B are mutually authenticated. They can further communicate securely using symmetric key encryption, such as Advanced Encryption Standard (AES), with kBA that is lightweight than public key encryption, thus more suitable for constrained device.

3. Results and Analysis

In this section, the security capabilities of the proposed scheme is analyzed. First of all, the threat model for the security analysis is presented. Then, the security features of the proposed scheme is analyzed. Finally, the security in terms of mutual authentication is discussed.

Threat Model

There are three types of attacker to be discussed in this section: (1) Oustide Attacker such as eaves-drops on every message transmitted in the system, replays the previous message to receiver, decom-poses the eavesdropped message into pieces, reassembles the pieces into new message, and sends the message to any legal entity, decrypts cipher text if obtain the corresponding key and modifies the decrypted plaintext, and utilizes the

public key of legal entity to forge message.; (2) Compromised Device such as capable of everything the outside attacker could do and utilizes the own secret key shared with MSP to decrypt eavesdropped message or forge message; and (3) Compromised SSP such as capable of everything the outside attacker could do and utilizes the own private key to decrypt eavesdropped message or forge message.

Security Feature of The Proposed Scheme

There are two main characteristics of the proposed scheme: (1) the message is authenticated when it is encrypted: When sender i communicates with receiver j, the sender needs to use ti to encrypt the message, and the receiver needs to use Ni to decrypt the message. Only the correct (ti, Ni) pair could ensure the message is encrypted and decrypted correctly. That means only if the message is encrypted by a legitimate sender i, the receiver could decrypt it by corresponding Ni. So the message is authenticated with the encryption and no more signatures are needed; and (2) the scheme is without key escrow problem: When a receiver j wants to decrypt a message, it needs to use dj and tj. The dj is known to the receiver, and the SSP and the tj is only known to the receiver. So even the SSP is compromised or the private key dj is leaked, the message could still only be decrypted by the receiver because of the tj. So the existence of tj solves the key escrow problem. Whats more, the updating of tj improves the security of the authentication scheme.

Mutual Authentication

A mutual authentication among a user from hospital, a medical sensor, and the SSP1! (SSP1!) can be achieved with the authentication scheme. The ID of hospital user is verified by the SSP1! in step 2 of the authentication mechanism. Only message encrypted by legitimate hospital user could be decrypted by the SSP1! with associated sub-public key NID. Furthermore, the sub-secret key tID ensures that only the legitimate mobile user could make the message authenticated with encryption and only the target sensor could decrypt that message and the other way around.

4. Conclusion

To ensure the security and privacy of IoT-based health care system is a very challenging task. It becomes more challenging due to the fact that IoT is mostly used to connect between patients with medical institutions or among several health care providers that are located across different domains with different trust authority. A scheme based on IBC has been proposed to secure communication in IoT-based health care system across multiple domains. The main contributions include authentication mechanism based on IBE that has key-escrow free feature, mechanism to lookup for IBE system parameters in other domains and to generate shared secret key for secure communication between communicating entities. Security analysis on the threat model, security feature, and mutual authentication has also been presented.

In order to enable verification and add more security on the identity, a cryptographic identity could be used instead of a plain identity, which is still left as an open issue. Furthermore, an extension of the proposed scheme with the extended IoT- based health care system architecture needs to be considered in order to take into account more stakeholders as discussed in the model proposed by [16]. Finally, implementation of the proposed scheme in the prototype or actual IoT system is another future work in order to measure the performance and practical feasibility of it.

References

[1] D. Lake, R. Milito, M. Morrow, and R. Vargheese, “Internet of things: Architectural framework for ehealth security,” Journal of ICT Standardization, vol. 1, no. 3, pp. 301–328, mar 2014.

[2] W. Jatmiko et al., “Developing smart telehealth system in indonesia: Progress and challenge,” in 2015 International Conference on Advanced Computer Science and Information Systems (ICACSIS), Oct 2015, pp. 29–36.

[3] B. Wiweko, A. Zesario, and P. G. Agung, “Overview the development of tele health and mobile health application in indonesia,” in 2016 Inter- national Conference on Advanced Computer Science and Information Systems (ICACSIS), Oct 2016, pp. 9–14.

[4] S. M. R. Islam et al., “The internet of things for health care: A comprehensive survey,” IEEE Access, vol. 3, pp. 678–708, June 2015.

[5] A. Al-Fuqaha et al., “Internet of things: A survey on enabling tech- nologies, protocols, and applications,” IEEE Communications Surveys Tutorials, vol. 17, no. 4, pp. 2347–2376, Fourthquarter 2015.

[6] S. Alasmari and M. Anwar, “Security privacy challenges in iot-based health

cloud," in 2016 International Conference on Computational Science and Computational Intelligence (CSCI), Dec 2016, pp. 198– 201.

[7] Z. Cheng, R. Comley, and L. Vasiu, "Remove key escrow from the identity-based encryption system," in Exploring New Frontiers of Theoretical Informatics: IFIP 18th World Computer Congress TC1 3rd International Conference on Theoretical Computer Science (TCS2004), J.-J. Levy, E. W. Mayr, and J. C. Mitchell, Eds. Springer US, 2004, pp. 37–50.

[8] C. Doukas et al., "Enabling data protection through pki encryption in iot m-health devices," in 2012 IEEE 12th International Conference on Bioinformatics Bio-engineering (BIBE), Nov 2012, pp. 25–29.

[9] A. Shamir, "Identity-based cryptosystems and signature schemes," in Advances in Cryptology: Proceedings of CRYPTO 84, G. R. Blakley and D. Chaum, Eds. Springer Berlin Heidelberg, 1985, pp. 47–53.

[10] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," in Advances in Cryptology — CRYPTO 2001: 21st Annual International Cryptology Conference, J. Kilian, Ed. Springer Berlin Heidelberg, 2001, pp. 213–229.

[11] S. Zhao, A. Aggarwal, R. Frost, and X. Bai, "A survey of applications of identity-based cryptography in mobile ad-hoc networks," IEEE Communications Surveys Tutorials, vol. 14, no. 2, pp. 380–400, Second 2012.

[12] A. Papanikolaou, K. Rantos, and I. Androulidakis, "Proxied ibe-based key establishment for llns," in The 10th International Conference on Digital Technologies 2014, July 2014, pp. 275–280.

[13] F. Corella and K. P. Lewison, "Identity-based protocol design patterns for machine-to-machine secure channels," in 2014 IEEE Conference on Communications and Network Security, Oct 2014, pp. 91–96.

[14] T. Markmann, T. C. Schmidt, and M. Wa¨hlisch, "Federated end-to-end authentication for the constrained internet of things using ibc and ecc," in Proceedings of the 2015 ACM Conference on Special Interest Group on Data Communication, ser. SIGCOMM '15. ACM, 2015, pp. 603– 604.

[15] S. Chen, M. Ma, and Z. Luo, "An authentication scheme with identity- based cryptography for m2m security in cyber-physical systems," Security and Communication Networks, vol. 9, no. 10, pp. 1146–1157, 2016.

[16] G. Neagu, Preda, A. Stanciu, and V. Florian, "A cloud-iot based sensing service for health monitoring," in 2017 E-Health and Bioengi- neering Conference (EHB), June 2017, pp. 53–56.

[17] D. McGrew, "An interface and algorithms for authenticated encryption," RFC 5116, January 2008.

[18] H. Krawczyk and P. Eronen, "Hmac-based extract-and-expand key derivation function (hkdf)," RFC 5869, May 2010.

[19] H. Krawczyk, M. Bellare, and R. Canetti, "Hmac: Keyed-hashing for message authentication," RFC 2104, February 1997.