Chiang *et al. BioMed Eng OnLine* 2018, **17**(Suppl 2):154
https://doi.org/10.1186/s12938-018-0582-5

BioMedical Engineering OnLine

RESEARCH Open Access

Robust IoT-based nursing-care support system with smart bio-objects

Cheng-Fa Chiang[1,2†], Fang-Ming Hsu[1†] and Kuo-Hui Yeh[1*†]

From International Conference on Biomedical Engineering Innovation (ICBEI) 2016 Taichung, Taiwan. 28 October–1 November 2016

*Correspondence: khyeh@gms.ndhu.edu.tw
†Cheng-Fa Chiang, Fang-Ming Hsu and Kuo-Hui Yeh contributed equally to this work
[1] Department of Information Management, National Dong Hwa University, Hualien 97401, Taiwan, ROC
Full list of author information is available at the end of the article

Abstract

Background: The significant advancement in the mobile sensing technologies has brought great interests on application development for the Internet-of-Things (IoT). With the advantages of contactlessness data retrieval and efficient data processing of intelligent IoT-based objects, versatile innovative types of on-demand medical relevant services have promptly been developed and deployed. Critical characteristics involved within the data processing and operation must thoroughly be considered. To achieve the efficiency of data retrieval and the robustness of communications among IoT-based objects, sturdy security primitives are required to preserve data confidentiality and entity authentication.

Methods: A robust nursing-care support system is developed for efficient and secure communication among mobile bio-sensors, active intelligent objects, the IoT gateway and the backend nursing-care server in which further data analysis can be performed to provide high-quality and on-demand nursing-care service.

Results: We realize the system implementation with an IoT-based testbed, i.e. the Raspberry PI II platform, to present the practicability of the proposed IoT-oriented nursing-care support system in which a user-friendly computation cost, i.e. 6.33 ms, is required for a normal session of our proposed system. Based on the protocol analysis we conducted, the security robustness of the proposed nursing-care support system is guaranteed.

Conclusions: According to the protocol analysis and performance evaluation, the practicability of the proposed method is demonstrated. In brief, we can claim that our proposed system is very suitable for IoT-based environments and will be a highly competitive candidate for the next generation of nursing-care service systems.

Background

With the rapid growth of information and communications technologies, such as Bluetooth Low Energy (BLE), 3G/4G/5G and NFC/RFID, a comprehensive evolution of the Internet has given rise to a ubiquitous network consisting of mobile intelligent objects, called the Internet of Things (IoT). In IoT-based environments, "contactless data sensing" and "collecting and information analyzing and retrieving" are fundamental components for the provision of human value-added services in a more transparent and faster

way than before. Among these services, in particular, the development of IoT-oriented nursing-care service systems are one the most promising and important directions, and are therefore a major focus of government and industry. A nursing-care service system is exploited for data collection, data storing, data retrieval and information display needed in nursing activities via modern information and communication technologies. With the advantages of contactlessness and efficiency brought by the data retrieval on intelligent IoT-objects, innovative types of on-demand nursing-care service systems have promptly been developed in these years. Meanwhile, the issue of system security and patient privacy has been focused by governments and research community. The potential to reveal patient privacy and system security vulnerability may exist wherever personally identifiable information is collected, processed, or stored in a hospital information system. Based on our survey, we present the major principles during patient private data processing: (1) be processed and used for lawful purposes; (2) unauthorized or unlawful processing must be measured; (3) accountability is required; (4) consent for data processing must be guaranteed; (5) be processed with an adequate level of protection and (6) adequate and relevant to the purpose for which it is processed.

In this paper, we present a robust IoT-based nursing-care support system in which fixed environmental sensing objects and intelligent smart objects are deployed in the field and on patients, respectively, to support high-quality nursing-care service. To satisfy the security and privacy requirements, we argue that sturdy cryptographic primitives must be implemented on IoT-objects to construct robust communications among entities. Nevertheless, based on current semiconductor technology, most of IoT-objects cannot afford heavy cryptographic primitives, such as asymmetric cryptography, due to limited computational resources. Therefore, a refinement of the traditional secure communication scheme should be launched in terms of the performance standpoint. That is, we have to thoroughly consider the trade-off between efficiency and the robustness of the adopted cryptographic components to appropriately meet the hardware limitation of IoT-objects and the security requirements we need. According to the analyses, the robust cryptographic module with a reasonable and acceptable computation cost, i.e. SHA-384, SHA-215 and SHA-3 [1, 2], will be good candidate techniques to simultaneously satisfy the security and performance requirements. In conclusion, we would like to demonstrate an efficient IoT-based communication mechanism for nursing-care service systems in which SHA-3 are mainly adopted as the major data protection technique to simultaneously achieve system security and patient privacy during the operation of the proposed system.

In the following, we present the state of the art of IoT application and security. In 2012, Jara et al. [3] proposed an IoT-based knowledge acquisition and management platform. This platform is composed of two parts, i.e. a wireless transmission of continuous vital signs through 6LoWPAN and a patient identification through RFID. The presented system also adopted a data analysis model and pre-processing module for patient health management. Next, Berhanu et al. [4] introduced an e-Health system with IoT devices in which a robust security scheme is included. The authors investigated the impact of antenna orientation on energy consumption to examine the validation of the proposed system. The issue of scalability is also studied through the feasibility of embedding the lightweight security solutions into the ASSET (adaptive security for smart Internet of

Things in e-health) [5]. Later, Torjusen et al. [6] verified that an enabler integrating into the ASSET adaptive security framework and provided an e-healthcare security framework via the IoT. Critical requirements for run-time verification are presented as formal specifications. After that, Bello and Zeadally [7] proposed an intelligent routing cooperation scheme for device-to-device communication. The operation of different network standards in the case of intermittent connection is considered in which the device will be affected by it's limited resources. In 2016, Gope and Hwang [8] proposed an IoT application system for healthcare on body sensor networks (BSN), called BSN-Care, which is able to provide effective real-time monitoring, patient information management and security needs for healthcare. In order to achieve the claimed services, a comprehensive integration of clinical devices and efficient collection of data are demonstrated. Note that the authors also introduced a similar concept for secure communication on IoT in [9].

Yao et al. [10] modified the fast one-way accumulator, proposed by Nyberg [11], to build a lightweight multicast authentication mechanism. However, the proposed method is only applicable to the small-scale IoT networks. It is limited by it's scalability. After that, Ning et al. [12] demonstrated an aggregation-based hierarchical authentication scheme. This method provides a strong security and is applicable to the U2IoT architecture. The main idea is to establish backward and forward anonymous data transmission among multiple targets. In addition, various techniques, i.e. directed path descriptors, homomorphism functions, and Chebyshev chaotic maps, are jointly applied for mutual authentication. Later, Hernández-Ramos et al. [13] proposed a framework for lightweight authentication and authorization. This presented framework is based on the reference model proposed by the EU FP7 IoT-A project. Meanwhile, Kawamoto et al. [14] proposed a location-based authentication system, where ambient information from IoT-based sensors are collected and analyzed as the authentication tokens. To pursue high authentication accuracy, the proposed system automatically and continuously adjusts the system parameters according to surrounding environment situation. Next, Cirani et al. [15] proposed an IoT-OAS architecture with the characteristics of flexible, highly configurable, and easy-to-integrate with existing services. The authors further provide an authorization platform which can invoke an external OAuth-based authorization service. The evaluation of the proposed architecture is based on Contiki OS-based constrained devices. In 2017, Cha et al. [16] demonstrated a privacy-aware mechanism for secure communication and efficient access-control among BLE-based devices. The proposed mechanism is based on elliptic curve cryptography. In addition, the authors presented a framework for the management of security examination reports of BLE-based applications.

Methods

This section introduces the underlying IoT communication architecture and then presents the proposed nursing-care support system consisting of a registration process and an authentication process.

Targeted IoT communication scenario

In this section, we introduce the underlying IoT communication architecture of our proposed nursing-care support system. Figure 1 demonstrates the scenario we target on, i.e. patient management and rehabilitation, in which fixed environmental sensors and medical sensing devices are deployed on field and on the patient, respectively, to support caregivers (such as nurse) in activities of patient care and rehabilitation. Three important components are existed in the identified IoT communication scenario, i.e. a backend nursing-care server, a mobile gateway (usually handheld by the caregiver), and intelligent devices (such as fixed sensor nodes or medical sensing devices). The intelligent devices are utilized for sensing and collecting environmental parameters and patients' bio-data, while the caregiver will operate a handheld smart device as the mobile gateway to communicate with the intelligent devices. Note that the patient's bio-data are such as electrocardiography, electroencephalography, electromyography and blood pressure retrieved from the patient. After that, with the environmental data and the patient's bio-data, the caregiver can identify patient's need in a faster way. More accurate and timely treatment services will then be able to deliver to the patients.

The IoT-based nursing-care support system

In this section, we present the proposed nursing-care support system in which IoT-based intelligent devices are adopted on the patient and the corresponding environment (e.g., Fig. 2). From Fig. 2a, the nurse first utilizes his/her handheld mobile gateway to retrieve the data from smart bio-objects. All of the retrieved data will be forwarded to the backend nursing-care server. At the backend server, a further data analysis for the mining of the patient's needs will be performed. Then, in Fig. 2b, decision support/assistant information will be derived and delivered to the nurse to support better-quality nursing care services on the patient.

In general, the proposed system consists of two phases, i.e. the registration phase and the authentication phase. In the registration phase, the security credentials will be

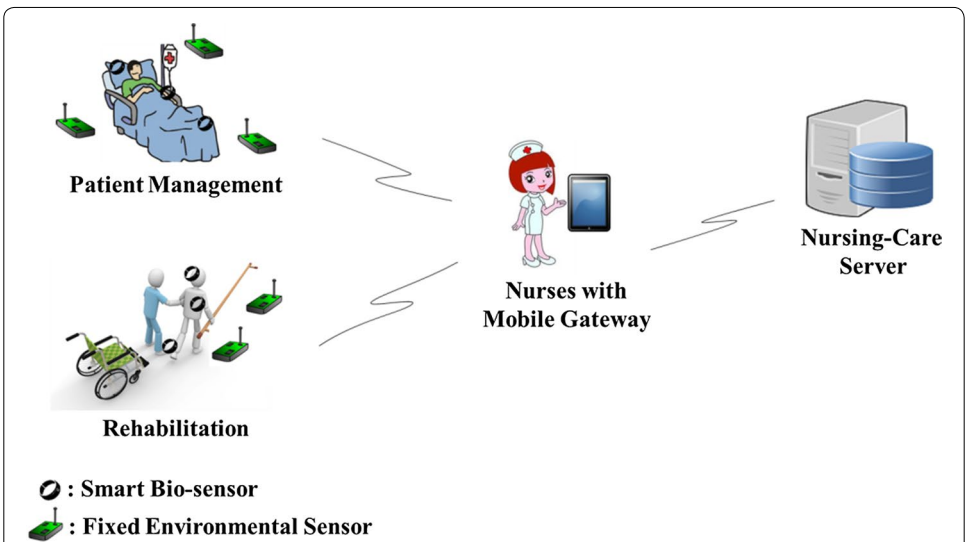

Fig. 1 The targeted IoT communication architecture

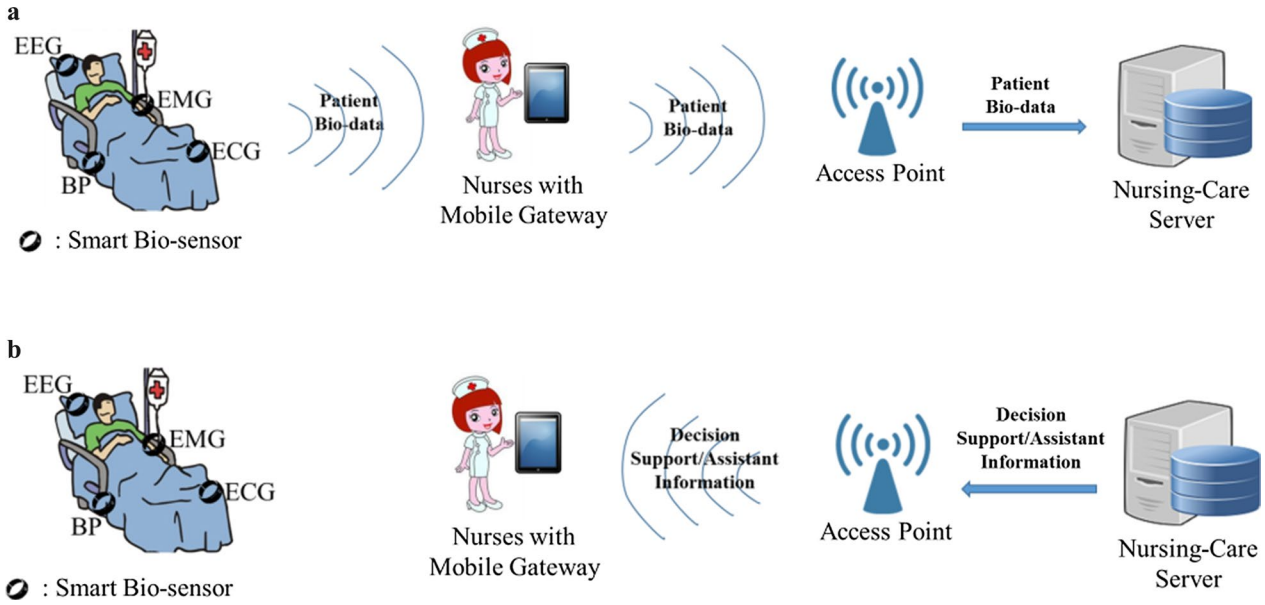

Fig. 2 The proposed IoT-based nursing-care support system

securely agreed and shared among the communication entities, i.e. intelligent devices (smart bio-objects and fixed environmental sensors), the mobile gateway and the nursing-care server, in advance. Next, an authentication phase is operated to secure all of the communication and data exchange among the communication entities. The proposed nursing-care support system is able to achieve the following security requirements: (a) to guarantee mutual authentication among intelligent devices, the mobile gateway and the nursing-care server; (b) to provide anonymity and un-traceability for intelligent devices; (c) to resist against forgery attack and replay attack and (d) to securely establish a robust session key between the mobile gateway and the nursing-care server.

The registration phase of the proposed system

Before introducing our proposed system, we present the symbols and abbreviations throughout this study in Table 1. In the first stage of the registration phase, an intelligent device d_i (i.e. smart bio-sensors or fixed environmental sensors) sends its identity ID_{d_i} to the nursing-care server S as a registration request. On receipt of the request from d_i, the nursing-care server S generates a random number N_{ds} and uses its identity ID_s to compute a secret value $K_{ds} = H\left(ID_s||N_{ds}||ID_{d_i}\right)$. Next, the nursing-care server S calculates a set of un-linkable shadow identities $SID = \{sid_1, sid_2, \ldots\}$ for d_i, where each $sid_j \in SID$ and $sid_j = H\left(ID_{d_i}||N_j||K_{ds}\right)$. Note that N_j is a random number used for deriving each sid_j value. Moreover, a track sequence number Tr_{seq} is generated for fast identification of intelligent device d_i during the authentication process as well as for preventing replay attacks. The Tr_{seq} will be stored and updated at both the nursing-care server S and the device d_i after each authentication session. In that case, the nursing-care server S is able to check the freshness of an incoming request from d_i, and to achieve a fast identification of d_i via Tr_{seq} at the backend database during the authentication session. Finally, the nursing-care server S issues a security credential containing $\left(ID_{d_i}, K_{ds}, SID, Tr_{seq}, H(.)\right)$ to the intelligent device d_i. At the same time, the nursing-care server will maintain a

Table 1 Notations throughout this study

Symbol	Definition
d_i	Intelligent device (i.e. smart bio-sensors or fixed environmental sensors)
g_j	Mobile gateway (operated by the nurse or the doctor)
S	The nursing-care server
ID_{d_i}	Private identity of d_i
ID_s	Public identity of the nursing-care server S
ID_{g_j}	Public identity of the mobile gateway g_j
AID_{d_i}	One-time-alias identity of d_i
SID	A set of un-linkable shadow identities $SID = \{sid_1, sid_2, \ldots\}$
K_{ds}	The secret key shared between d_i and S
K_{gs}	The secret key shared between g_j and S
Tr_{seq}	Track sequence number
$N_{ds}, N_j, N_{gs}, N_d, N_g, m$	Random numbers
$H(.)$	Secure one-way hash function, i.e. SHA-3
$\oplus$	Bitwise exclusive-or operation
$\|\|$	Concatenation operation

record $\left(ID_{d_i}, K_{ds}, SID, Tr_{seq}, H(.)\right)$ corresponding to d_i at the backend database. Note that $H(.)$ denotes a secure one-way hash function such as SHA-3. On the other hand, the registration phase between the mobile gateway g_j and the nursing-care server S are launched in a similar way. The mobile gateway g_j send its identity ID_{g_j} to the nursing-care server as a registration request. Next, the nursing-care server S calculates $K_{gs} = H\left(ID_s||N_{gs}||ID_{g_j}\right)$ with a newly generated random number N_{gs}, and shares a security credential containing the secrets, i.e. ID_{g_j} and K_{gs}, with g_j. The nursing-care server also maintains a tuple $\left(ID_{g_j}, K_{gs}, H(.)\right)$ corresponding to the mobile gateway g_j at the backend database.

The authentication phase of the proposed system

In the authentication phase, we consider that a caregiver (with a mobile gateway) would like to provide on-demand nursing care services to patients via contactless and real-time data collection and analysis mechanisms. Under the insecure IoT communication architecture, an authentication procedure is needed to establish a secure communication channel for data exchange among intelligent devices, the mobile gateway and the nursing-care server. The detailed communication procedures of the authentication phase are as shown in Fig. 3.

- Intelligent Device $d_i \rightarrow$ Mobile Gateway g_j : $M_{A_1} = \left\{AID_{d_i}, N_x, Tr_{seq}(\text{if req.}), ID_{g_j}\right\}$
  First, the intelligent device d_i generates a random number N_d and calculates two values, i.e. $M_x = H\left(K_{ds}||ID_{d_i}\right) \oplus N_d$ and $AID_{d_i} = H\left(ID_{d_i}||K_{ds}||N_d||M_x||ID_{g_j}||Tr_{seq}\right)$. Next, d_i constructs a message $M_{A_1} = \left\{AID_{d_i}, M_x, Tr_{seq}, ID_{g_j}\right\}$ and sends M_{A_1} as an authentication request to the mobile gateway g_j. Note that, if the value Tr_{seq} shared between the intelligent device d_i and the nursing-care server S is out of synchronization, d_i needs to choose a fresh shadow identity sid_j from SID as the value AID_{d_i}. Then, d_i sends $M_{A_1} = \left\{AID_{d_i}, M_x, ID_{g_j}\right\}$ to the mobile gateway g_j as an authentication request.
- Mobile Gateway $g_j \rightarrow$ Nursing-Care Server S: $M_{A_2} = \left\{M_y, V_1, M_{A_1}\right\}$
  Once the mobile gateway g_j receives the authentication request from the intelligent device d_i, g_j first generates a random number N_g and computes $M_y = K_{gs} \oplus N_g$ and $V_1 = H\left(M_{A_1}\left|\right|N_g\left|\right|M_y||K_{gs}\right)$. After that, g_j sends $M_{A_2} = \left\{M_y, V_1, M_{A_1}\right\}$ to the nursing-care server S.
- Nursing-Care Server $S \rightarrow$ Mobile Gateway g_j : $M_{A_3} = \{Tr, ID_s, V_2, V_3\}$
  Upon obtaining the incoming message $M_{A_2} = \left\{M_y, V_1, M_{A_1}\right\}$, the nursing-care server S first checks whether the track sequence number Tr_{seq} is in the request or not. If it is, S performs step (1). If Tr_{seq} is not included in M_{A_2}, S performs step (2).
  - Step (1): Check the validity of Tr_{seq}. If it holds, look for the corresponding tuple via Tr_{seq} from the backend database. Otherwise, terminate the connection. If Tr_{seq} is valid, S derives $N_d = H\left(K_{ds}||ID_{d_i}\right) \oplus M_x$ and $N_g = K_{gs} \oplus M_y$, and then verifies V_1

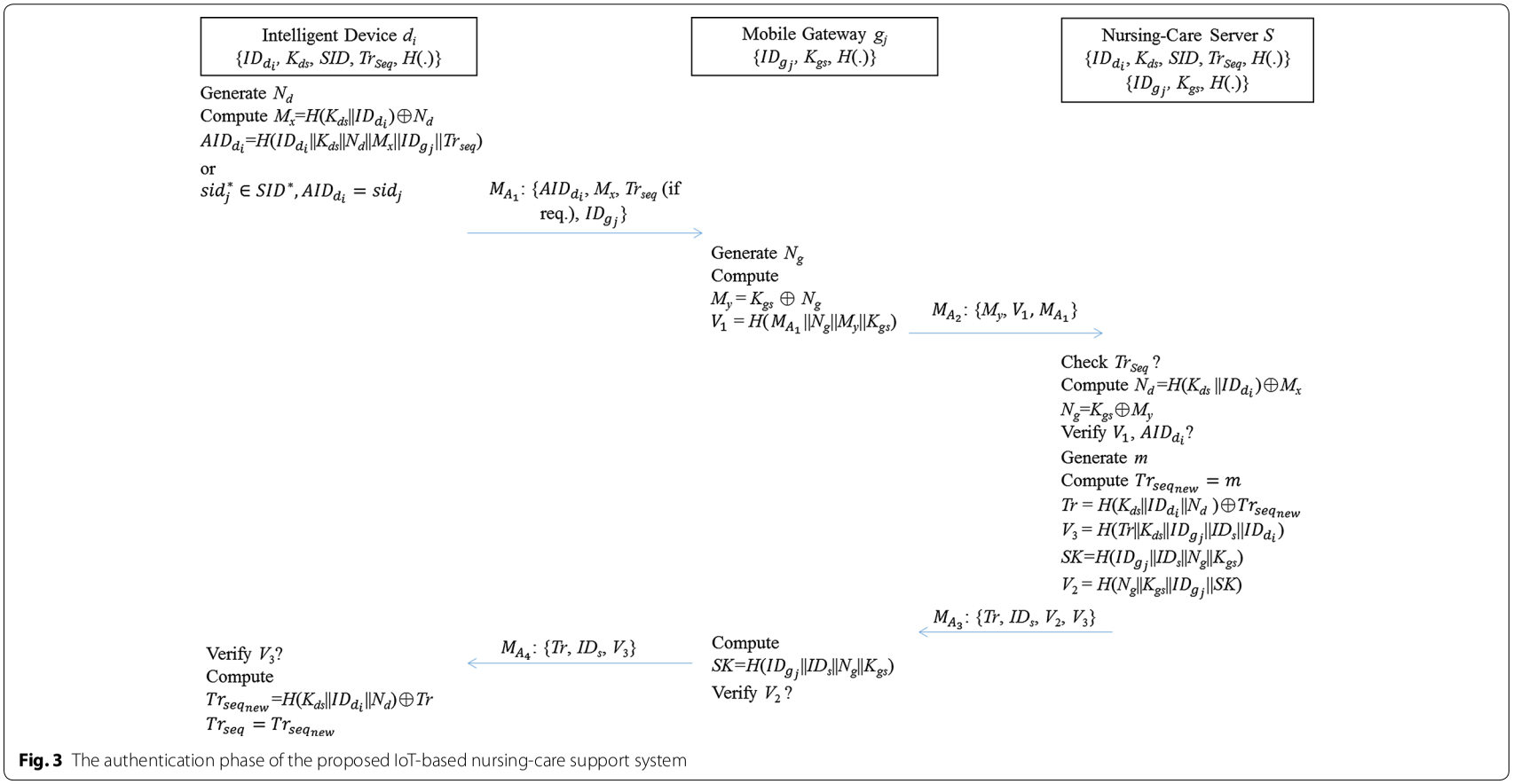

Fig. 3 The authentication phase of the proposed IoT-based nursing-care support system

and AID_{d_i}. That is, S will examine (a) whether the received value V_1 and the computed value $H\left(M_{A_1}||N_g||M_y||K_{gs}\right)$ are equal or not, and (b) whether the received value AID_{d_i} and the computed value $H = \left(ID_{d_i}||K_{ds}||N_d||M_x||ID_{g_j}||Tr_{seq}\right)$ are equal or not. Note that if Tr_{seq} in the request does not match the one maintained in the database, the nursing-care server S will reject the request and terminate the connection. A new request from the device d_i will be asked for in which one of the fresh shadow identities sid_j will be picked up from the list SID as an anonymous identity of d_i. In that case, the step (2) will be launched.

- Step (2): The server S will verify the freshness and validity of $AID_{d_i} = sid_j$. If the nursing-care server S cannot identify the sid_j from the backend database, the server will terminate the connection. Next, the S will request the intelligent device d_i to try with another valid shadow identity sid_j.

If one of the above examinations, i.e. step (1) or (2), is passed, the nursing-care server S will generate a random number m, and set $Tr_{seq_{new}} = m$. After that, S calculates $Tr = H\left(K_{ds}||ID_{d_i}||N_d\right) \oplus Tr_{seq_{new}}$, $V_3 = H\left(Tr||K_{ds}||ID_{g_j}||ID_s||ID_{d_i}\right)$, $SK = H\left(ID_{g_j}||ID_s||N_g||K_{gs}\right)$ and $V_2 = H\left(N_g||K_{gs}||ID_{g_j}||SK\right)$, where SK is a session key utilized for the next secure communication between the mobile gateway g_j and the nursing-care server S. Eventually, S sends $M_{A_3} = \{Tr, ID_s, V_2, V_3\}$ to the mobile gateway g_j.

- Mobile Gateway $g_j \rightarrow$ Intelligent Device d_i: $M_{A_4} = \{Tr, ID_s, V_3\}$
  With the incoming message $M_{A_3} = \{Tr, ID_s, V_2, V_3\}$, the mobile gateway g_j computes $SK' = H\left(ID_{g_j}||ID_s||N_g||K_{gs}\right)$ and $H\left(N_g||K_{gs}||ID_{g_j}||SK'\right)$, and then check if the received V_2 is equal to the computed $H\left(N_g||K_{gs}||ID_{g_j}||SK'\right)$. If it holds, it is obvious that a session key SK is securely agreed by g_j and S. After that, the mobile gateway g_j sends $M_{A_4} = \{Tr, ID_s, V_3\}$ to the intelligent device d_i. With M_{A_4}, the device d_i derives $H\left(Tr||K_{ds}||ID_{g_j}||ID_s||ID_{d_i}\right)$ and compares it with the received V_3. If these two values are identical, d_i computes $Tr_{seq_{new}} = H\left(K_{ds}||ID_{d_i}||N_d\right) \oplus Tr$ and sets $Tr_{seq} = Tr_{seq_{new}}$.

Protocol analysis and discussions

In this section, we present a formal security analysis of the communication procedures of the proposed IoT-based nursing-care support system and discuss whether all the proposed security claims can be achieved or not.

- Claim 1: To achieve mutual authentication among communication entities in the proposed nursing-care support system

The mutual authentication via the proposed communication procedures is proven via BAN logic analysis [17, 18]. Basic constructs and logic postulates for the purpose of analysis are first presented, where the symbols P and Q are defined as principals, X and Y are defined as statements, and K ranges over a long-term secret.

Seven constructs is introduced as follows: (1) P believes X means that the principal P believes that X is true; (2) P sees X means that someone has sent a message containing X to P; (3) P said X denotes that P has actually sent a message including statement X at the current session of the protocol or before; (4) P controls X denotes that P has jurisdiction over X; (5) fresh(X) denotes that X has not been sent in a message; (6) $P \overset{K}{\longleftrightarrow} Q$ means that the secret K is shared between the principals P and Q, and (7) $\{X\}_K$ means that the X is encrypted or protected under the key K. Next, we presented five major rules as logical postulates. First, in the message-meaning rule (referred to rule 1), we believe that if P believes $P \overset{K}{\longleftrightarrow} Q$ and P sees $\{X\}_K$, then we postulate P believes Q said X. Second, the nonce-verification rule (referred to rule 2) denotes that if P believes fresh (X) and P believes Q said X, then we postulate P believes Q believes X. Third, the jurisdiction rule (referred to rule 3) means that if P believes Q controls X and P believes Q believes X, then we postulate P believes X. Fourth, a rule 4 is identified for that if P sees (X, Y) then P sees X. In addition, if P believes $P \overset{K}{\longleftrightarrow} Q$ and P sees $\{X\}_K$, then P sees X. Fifth, the final rule 5 denotes that if one part of a formula is fresh, then the entire formula must also be fresh. If P believes fresh (X), then P believes fresh (X, Y). Finally, we demonstrate seven assumptions of our proposed system in the following.

- Assumption 1: d_i, S believe $d_i \overset{ID_{d_i},K_{ds},SID,Tr_{seq}}{\longleftrightarrow} S$
- Assumption 2: g_j, S believe $g_j \overset{ID_{g_i},K_{gs}}{\longleftrightarrow} S$
- Assumption 3: d_i, S believe fresh(N_d)
- Assumption 4: g_j, S believe fresh(N_g)
- Assumption 5: d_i believes fresh(m)
- Assumption 6: d_i believes S controls N_d
- Assumption 7: g_j believes S controls N_g

Before the security analysis, we conduct the concrete realization of our proposed communication procedures as follows:

Step 1: $d_i \rightarrow g_j : \left\{AID_{d_i}, M_x, Tr_{seq}(\text{if req.}), ID_{g_j}\right\}$, where $AID_{d_i} = H\left(ID_{d_i}||K_{ds}||N_d||M_x||ID_{g_j}||Tr_{seq}\right)$ and $M_x = H\left(K_{ds}||ID_{d_i}\right) \oplus N_d$.

Step 2: $g_j \rightarrow S : \left\{M_y,\ V_1, AID_{d_i}, M_x, Tr_{seq}(\text{if req.}), ID_{g_j}\right\}$, where $M_y = K_{gs} \oplus N_g$ and $V_1 = H\left(M_{A_1}\big|\big|N_g\big|\big|M_y||K_{gs}\right)$.

Step 3: $S \rightarrow g_j : \{Tr, ID_s, V_2, V_3\}$, where $Tr = H\left(K_{ds}||ID_{d_i}||N_d\right) \oplus Tr_{seq_{new}}$, $V_2 = H\left(N_g||K_{gs}||ID_{g_j}||SK\right)$, $V_3 = H\left(Tr||K_{ds}||ID_{g_j}||ID_s||ID_{d_i}\right)$ and $SK = H\left(ID_{g_j}||ID_s\big|\big|N_g\big|\big|K_{gs}\right)$.

Step 4: $g_j \rightarrow d_i : \{Tr, ID_s, V_3\}$, where $Tr = H\left(K_{ds}||ID_{d_i}||N_d\right) \oplus Tr_{seq_{new}}$ and $V_3 = H\left(Tr||K_{ds}||ID_{g_j}||ID_s||ID_{d_i}\right)$.

After that, the following steps show that the formal analysis of the mutual authentication:

1. g_j sees$\{ID_s, V_2\}$ (Step 3).
2. g_j believe $g_j \overset{ID_{g_i},K_{gs}}{\longleftrightarrow} S$(Assumption 2).
3. g_j believes S said $\{ID_s, V_2\}$ [(1) and (2), inferred by Rule 1].

4. g_j believes fresh(N_g) (Assumption 4).
5. g_j believes S believes {ID_s, V_2} [(3) and (4), inferred by Rule 2].
6. g_j believes S controls{N_g} (Assumption 7).
7. g_j believes {ID_s, V_2} [(5) and (6), Inferred by Rule 3].
8. d_i sees {Tr, ID_s, V_3} (Step 4).
9. d_i believes $d_i \overset{ID_{d_i}, K_{ds}, SID, Tr_{seq}}{\longleftrightarrow} S$ (Assumption 1).
10. d_i believes S said {Tr, ID_s, V_3} [(8) and (9), Inferred by Rule 1].
11. d_i believes fresh(N_d), fresh(m) (Assumption 3 and 5).
12. d_i believes S believes {Tr, ID_s, V_3} [(10) and (11), Inferred by Rule 2].
13. d_i believes S controls {N_d} (Assumption 6).
14. d_i believes {Tr, ID_s, V_3} [(12) and (13), inferred by Rule 3].

So far, we obtain the following results.
g_j believes S believes {ID_s, V_2} [From (5)]
g_j believes {ID_s, V_2} [From (7)]
d_i believes S believes {Tr, ID_s, V_3} [From (12)]
d_i believes {Tr, ID_s, V_3} [From (14)]

Based on the assumption of the trustworthiness of S and the four results (5), (7), (12) and (14), both d_i and g_j can authenticate with each other via S.

- Claim 2: To guarantee anonymity and un-traceability for each intelligent device in the proposed nursing-care support system

During the communication procedures of the proposed system, two random numbers N_d and N_g are utilized to randomize the messages, such as $AID_{d_i}, M_x, M_y, V_1, Tr, V_2$ and V_3, transmitted among the intelligent devices d_i, the mobile gateway g_j and the nursing-care server S. The g_j and S cannot obtain the real identity of d_i. In other words, the identity ID_{d_i} is included in a randomized cipher text during each communication session. Therefore, we can claim that our proposed system can provide the anonymity, and the un-traceability can be guaranteed also. On the other hand, the shadow identity scheme in our system is adopted to deal with the condition of loss of synchronization between the intelligent device and the nursing-care server. Since the shadow identity is randomly chosen, it does not provide any clue for malicious attacks due to the un-linkable property of them.

- Claim 3: To resist against forgery attack and replay attack

Adversaries may counterfeit messages to deceive the legal communication entities, i.e. d_i, g_j and S. However, without N_d, N_g, K_{ds} and K_{gs}, it is hard to create a counterfeited but legitimate messages such as $\left\{M_y, V_1, AID_{d_i}, M_x, Tr_{seq}(\text{if req.}), ID_{g_j}\right\}$ and {Tr, ID_s, V_2, V_3} for spoofing. Even if the adversaries launch a replay attack with a previously eavesdropped message, the previously-used message cannot be successfully verified. This is because the random numbers N_d and N_g must be fresh and on-time valid at each session. As a result, we can claim that the resistance to forgery attack and replay attack can be guaranteed in our proposed system.

- Claim 4: To preserve data confidentiality via a secure transmission channel established between the mobile gateway and the nursing-care server

During the transmission of the proposed system, all of the messages $\left\{M_y, V_1, AID_{d_i}, M_x, Tr_{seq}(\text{if req.}), ID_{g_j}\right\}$ and $\{Tr,\ ID_s,\ V_2,\ V_3\}$ are protected through a secure one-way hash function (e.g., SHA-3), and two robust secrets K_{ds} and K_{gs} chosen by S. Without K_{ds} and K_{gs}, it is difficult to retrieve any useful information from transmitted cipher texts owing to the irreversibility of the one-way hash function. The proposed system thus provides data confidentiality. Moreover, according to the analysis of Claim 1, the mutual authentication of g_j and S is achieved via V_2. It is obvious that a session key SK can securely be agreed by g_j and S during our proposed authentication phase, and this session key SK will then be exploited on the verification of V_2. Therefore, we argue that a robust channel will be established between the mobile gateway and the nursing-care server for secure communication.

Performance evaluation and results

To evaluate the practicability of the proposed IoT-based nursing-care support system, we implement a demo system as a proof-of-concept and evaluate it's performance. The implementation was established under the platform shown in Table 2, where the Raspberry PI II platform is simulated as an intelligent device operating with a smartphone (as the mobile gateway) and a desktop computer (as the nursing-care server). Because a performance bottleneck occurring at the intelligent device is always in a high probability when compared to a smartphone and a desktop computer, in this implementation we focus on the performance evaluation of the intelligent device. A secure one-way hash function, i.e. SHA-3 (512 bits), and bitwise exclusive-or operation are adopted. In addition, in our system implementation, "ID_{d_i}, ID_s, ID_{g_j}, K_{ds} and K_{gs}" are set to 96-bits and "SID, Tr_{seq}, N_{ds}, N_j, N_{gs}, N_d, N_g and m" are set to 64-bits. Each time SID contains 100 sid_j values. The experiments are implemented via Oracle Java 8 and Eclipse 3.8, and we implement the SHA-3 hash function with the support of Bouncy Castle Crypto APIs [19].

Table 3 presents the computation cost required in our proposed IoT-based nursing-care support system. During the registration phase, we need to perform $(2+k)$ times of random number generation and $(2+k)$ times of one-way hash function. Note that k is the size of SID and in our implementation we set k as 100. In that case, in the registration phase we have to execute 102 times the random number generation and 102 times that of the one-way hash function, and we found that the total computation

Table 2 Implementation environment

Environment	Description
Raspberry PI II	Broadcom BCM2836 @ 1 GHz Quad-Core ARM Cortex-A7 Architecture, 1 GB DDR2 RAM and SanDisk 16 GB Class 10 SD Card
Operating system	Raspbian 2016/03
Programming IDE	Eclipse 3.8 with Oracle Java 8 ARM
Crypto API	The Bouncy Castle Crypto APIs
Environment	Description

Table 3 Execution time of the proposed IoT-based nursing-care support system

Phase	Computation cost	Execution time (ms)
Registration	$(2+k)$ RN + $(2+k)$ H[a]	14.23 ms (i.e. 102RN + 102H)
Authentication	3RN + 6XOR + 14H (with Tr_{seq})	6.33 ms (i.e. 3RN + 6XOR + 14H)
	3RN + 6XOR + 12H (without Tr_{seq})	5.43 ms (i.e. 3RN + 6XOR + 12H)

RN means random number

XOR means bitwise exclusive-or operation

H means the one-way hash function SHA-3 (512 bits)

[a] k is the size of SID which contains $ksid_j$ values

time is around 14.23 ms. Note that 7.09 ms is needed for 102 RN and 7.14 ms is required for 102 H. Next, in the authentication phase we require the execution time of 6.33 ms and 5.43 ms, respectively, to perform all of the cryptographic modules, such as random number generations, exclusive-or operations and the SHA-3 (512-bits) hash function, during a normal communication session. Our implementation presents that the computation cost will be majorly dominated by the SHA-3 hash function as the execution time of the random number generation and exclusive-or operation are comparatively slight. The execution time to perform all of the SHA-3 functions required in our proposed system takes around 94% of the total computation cost. It is obvious that the SHA-3 function may become a bottleneck in terms of the performance points when the scale of the network becomes larger. Note that, in our system implementation, the input bit sequences of SHA-3 function are 192 bits, 288 bits, 800 bits, 896 bits, 992 bits and 1728 bits.

Conclusions

In this paper, we present an efficient IoT-based nursing-care service system to support the caregiver (such as nurse/doctor/administrator) to provide better quality in nursing care activities. In consideration of the trade-off between system security and computation efficiency, we adopt lightweight cryptographic modules as the major data protection technique in the communication procedures of our proposed nursing-care support system. A demo system is implemented as a proof of concept to show the practicability of the proposed method in which a reasonable and user-acceptable computation cost, i.e. at most 6.33 ms, is presented. Moreover, based on the analysis we conducted, the security robustness of the proposed nursing-care support system is guaranteed. In brief, we argue that our proposed system is very suitable for IoT-based environments and will be a highly competitive candidate for the next generation of nursing-care service systems.

Abbreviations

IoT: Internet-of-Things; BLE: Bluetooth Low Energy; NFC: near-field communication; RFID: radio frequency identification; SHA: Secure Hash Algorithm; 6LoWPAN: IPv6 over Low-Power Wireless Personal Area Networks; ASSET: adaptive security for smart Internet of Things in e-health; BSN: body sensor networks.

Declarations

Authors' contributions

CFC and KHY wrote the paper; KHY and FMH conceived and designed the proposed algorithm. All authors read and approved the final manuscript.

Author details

[1] Department of Information Management, National Dong Hwa University, Hualien 97401, Taiwan, ROC. [2] Physical Education Center, National Dong Hwa University, Hualien 97401, Taiwan, ROC.

Acknowledgements

Not applicable

Competing interests

The authors declare that they have no competing interests.

Availability of data and materials

The datasets used and/or analysed during the current study are available from the corresponding author on reasonable request.

Consent for publication

Not applicable

Ethics approval and consent to participate

Not applicable

Funding

Publication of this article was support in part by the Academia Sinica, in part by the Taiwan Information Security Center, and in part by the Ministry of Science and Technology, Taiwan under Grants MOST 105-2221-E-259-014-MY3, MOST 105-2221-E-011-070-MY3, MOST 105-2923-E-182-001-MY3, and MOST 107-2218-E-011-012.

About this supplement

This article has been published as part of BioMedical Engineering OnLine Volume 17 Supplement 2, 2018: Proceedings of the International Conference on Biomedical Engineering Innovation (ICBEI) 2016. The full contents of the supplement are available online at https://biomedical-engineering-online.biomedcentral.com/articles/supplements/volume-17-supplement-2.

Publisher's Note

Published: 6 November 2018

References

1. Dang QH. Secure Hash Standard (SHS). NIST FIPS 180-4; 2015. https://csrc.nist.gov/csrc/media/publications/fips/180/4/final/documents/fips180-4-draft-aug2014.pdf. Accessed 11 Apr 2018.
2. Dworkin MJ. SHA-3 standard: permutation-based hash and extendable-output functions. NIST FIPS-202; 2015. https://csrc.nist.gov/csrc/media/publications/fips/202/final/documents/fips_202_draft.pdf. Accessed 11 Apr 2018.
3. Jara AJ, Zamora MA, Skarmeta AF. Knowledge acquisition and management architecture for mobile and personal Health environments based on the Internet of Things. In: Proceeding of the 11th IEEE international conference on trust, security and privacy in computing and communications; 2012. p. 1811–8.
4. Berhanu Y, Abie H, Hamdi M A test bed for adaptive security for IoT in eHealth. In: Proceeding of the international workshop on adaptive security; 2013. Article No. 5.
5. ASSET—Adaptive security for smart internet of things in eHealth. http://asset.nr.no/asset/index.php/ASSET_-_Adaptive_Security_for_Smart_Internet_of_Things_in_eHealth. Accessed 11 Apr 2018.
6. Torjusen AB, Abie H, Paintsil E, Trcek D, Skomedal Å. Towards run-time verification of adaptive security for IOT in eHealth. In: Proceeding of the 2014 European conference on software architecture workshops; 2014. Article No. 4.
7. Bello O, Zeadally S. Intelligent device-to-device communication in the internet of things. IEEE Syst J. 2016;10(3):1172–82.
8. Gope P, Hwang T. BSN-care: a secure IoT-based modern healthcare system using body sensor network. IEEE Sens J. 2016;16(5):1368–76.
9. Gope P, Hwang T. Untraceable sensor movement in distributed IoT infrastructure. IEEE Sens J. 2015;15(9):5340–8.
10. Yao X, Han X, Du X, Zhou X. A lightweight multicast authentication mechanism for small scale IoT applications. IEEE Sens J. 2013;13(10):3693–701.
11. Nyberg K. Fast accumulated hashing. In: Proceeding of the 3rd fast software encryption workshop; 1996. p. 83–7.
12. Ning H, Liu H, Yang LT. Aggregated-proof based hierarchical authentication scheme for the internet of things. IEEE Trans Parallel Distrib Syst. 2015;26(3):657–67.
13. Hernández-Ramos JL, Pawlowski MP, Jara AJ, Skarmeta AF, Ladid L. Toward a lightweight authentication and authorization framework for smart objects. IEEE J Sel Areas Commun. 2015;33(4):690–702.
14. Kawamoto Y, Nishiyama H, Kato N, Shimizu Y, Takahara A, Jiang T. Effectively collecting data for the location-based authentication in internet of things. IEEE Sens J. 2017;11(3):1403–11.

15. Cirani S, Picone M, Gonizzi P, Veltri L, Ferrari G. IoT-OAS: an OAuth-based authorization service architecture for secure services in IoT scenarios. IEEE Sens J. 2015;15(2):1224–34.
16. Cha SC, Yeh KH, Chen JF. Toward a Robust Security Paradigm for Bluetooth Low Energy-Based Smart Objects in the Internet-of-Things. Sensors. 2017. https://doi.org/10.3390/s17102348.
17. Burrows M, Abadi M, Needham R. A logic of authentication. ACM Trans Comput Syst. 1990;8(1):18–36.
18. Yeh KH, Tsai KY, Hou JL. Analysis and design of a smart card based authentication protocol. J Zhejiang Univ Sci C. 2013;14(12):909–17.
19. The Bouncy Castle Crypto APIs. https://www.bouncycastle.org/. Accessed 11th Apr 2018.