Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2015, Article ID 183659, 9 pages
http://dx.doi.org/10.1155/2015/183659

Research Article

Novel Authentication Schemes for IoT Based Healthcare Systems

Jia-Li Hou and Kuo-Hui Yeh

Department of Information Management, National Dong Hwa University, Hualien 97401, Taiwan

Correspondence should be addressed to Kuo-Hui Yeh; khyeh@mail.ndhu.edu.tw

Received 16 June 2015; Accepted 20 August 2015

Academic Editor: Sk Md Mizanur Rahman

With the advancement of information communication technologies, the evolution of the Internet has given rise to a ubiquitous network consisting of interconnected objects (or things), called the Internet of Things (IoT). Recently, the academic community has made great strides in researching and developing security for IoT based applications, focusing, in particular, on healthcare systems based on IoT networks. In this paper, we propose a sensor (or sensor tags) based communication architecture for future IoT based healthcare service systems. A secure single sign-on based authentication scheme and a robust coexistence proof protocol for IoT based healthcare systems are proposed. With the formal security analysis, the robustness of the two proposed schemes is guaranteed under the adversary model.

1. Introduction

The rapid growth of population in cities calls for adequate provision of services and infrastructure to meet the needs of urban inhabitants. Various information and communications technologies (ICTs), such as Bluetooth, WiFi, 3G/4G, and NFC/RFID, go a long way to achieving this objective and create the possibility of smart cities where human based services and city monitoring are more aware, interactive, and efficient. Following this trend, the comprehensive evolution of the traditional Internet has given rise to a ubiquitous network consisting of interconnected objects (or things), called the Internet of Things (IoT). In IoT based environments, information sensing and human interaction with the physical world are fundamental concepts for the provision of human value-added services. Among these services, in particular, IoT oriented healthcare support systems are among the most promising and important directions for development and are therefore a major focus of government and industry.

Cyber attackers generally exploit security vulnerabilities in computer hardware, software, and communications protocols to target the IoT ecosystems within enterprise, industrial, and government systems. The confidentiality, integrity, and availability of these systems are thus undermined, and serious attacks (e.g., ones resulting in financial losses, property damage, etc.) may be launched on IoT based environments. It is known that the IoT brings with it a broad array of new security challenges for the research community with respect to general system security, network security, and application security. We present the following observations:

(i) Securing IoT-networked devices requires implementation of secure cryptographic primitives on the devices. However, the limited computational resources of low-power-consuming and low-cost IoT based devices make the design of security components for such devices difficult. As it stands, some devices cannot even execute the currently existing encryption schemes. Hence, we must reconsider the implementation efficiency of security primitives (or cryptocomponents) on IoT-networked devices. In other words, a new lightweight cryptographic technique is urgently needed to meet the critical security and performance requirements of IoT based devices.

(ii) Owing to the level of mutual connectivity between IoT based devices, every time a user turns on an IoT-networked device which is infected by malware or is simply open to unauthorized third-party exploitation, the vulnerability may spread through the network in a short time. In light of these

conditions, devices cannot be seen as stand-alone, as they once were in traditional security settings. In addition, owing to its advantages in terms of computation efficiency and identification accuracy, Bluetooth Low Energy (i.e., BLE) technology has been widely adopted in recent years for smartphones and intelligent wearable-devices such as the Apple Watch, the Sony SmartWatch, and Samsung Gear. For an IoT based application, the user may be an entry point for triggering specific services. Hence, an appropriate authentication scheme for entity verification is indispensable.

(iii) One of the most important goals of IoT is to enrich people's daily lives. Sensor-based objects may be involved with several services at the same time. In that case, to guarantee both communication security and retrieval efficiency during interactions between sensor-based objects, a secure and intelligent access control scheme is promptly required. Moreover, as most IoT based technologies are still in the research stage, the development of a real and practical IoT application has been the focus of industry and business. The feasibility and practicability of proposed IoT based applications must be evaluated via testing scenarios.

(iv) In an IoT-wide universe, a mechanism capable of proving a group of tagged objects (or sensor tags) existing at the same time and the same place can be very useful. For example, a consignment of medication should always be accompanied by a usage leaflet to comply with pharmaceutical safety regulations. If all tablet containers and usage leaflets are labeled with RF tags, a coexistence proof mechanism on RF tags can provide the evidence that each tablet container was associated with an appropriate leaflet during medication distribution. This tag coexistence concept has been widely applied in recent years.

Based on the above analysis, in this paper we would like to present a new IoT based secure healthcare process consisting of a refinement of the traditional authentication scheme, from a performance standpoint. The security components adopted in the proposed authentication scheme have been redesigned to meet the hardware requirements of IoT based devices. The suitability of the proposed authentication scheme as the main protection mechanism for the entry point of an IoT based healthcare system is evaluated. In addition, we introduce a coexistence scheme for proving the correctness of the coexisting medical items for which the ultra low-cost IoT based sensors, such as passive RF tags, are utilized. Medicine error prevention and patient safety can thus be guaranteed.

2. Related Work

The next generation of context-aware mobile applications require the continuous updating of relevant information about a user's surroundings to create low latency notifications and guarantee a high quality of experience. Forsström et al. [1] studied the possibilities of doing so via transmission and monitoring of contextual information from mobile devices and found that the impact of the contextual information was to overload IoT networks. In addition, the authors presented an evaluation model to achieve dynamic control of the information flow without any centralized authority. Recently, the IoT based EPC (Electronic Product Code) system has emerged as a revolutionary new technology for modern logistics management. The IoT can achieve the properties of real-time location returning, object tracking and monitoring, and intelligent recognition. For this type of envisioned scenario, Wang [2] investigated relevant laws and technical standards with a view to increasing government investment and setting up business models for the promotion of future IoT based applications. On the other hand, as the capability to provide personalized healthcare is limited by the data available from patients, which is dynamic and often incomplete, knowledge mining, analysis, and trending are increasingly important. Therefore, Jara et al. [3] presented a knowledge acquisition and management platform relying on IoT based architecture. The platform focused on the management of personal and mobile health and enabled delivery of new services by virtue of its capabilities to predict health anomalies in real-time, offer feedback to patients, and support security and privacy.

In 2011, Zakriti and Guennoun [4] investigated an IoT based model to support interconnectivity and interoperability among smart objects. The proposed method solved various challenges, such as the integration of heterogeneity among devices, the development of diversified protocols, the desired properties of self-manageability and self-organization, and adaptive security and privacy for IoT networks. Then, Tozlu et al. [5] demonstrated three types of sensor-based application scenarios and examined the feasibility of low-power WiFi technology to enable IP connectivity between battery-powered objects. Next, Jin et al. [6] proposed a framework encompassing an urban information system with a view to furthering the realization of smart cities through the concept of the IoT. The introduced framework includes cloud-based integration of respective systems and services and forms a transformational part of the existing cyber systems. This framework can be adapted to enhance the level of interconnectivity and interoperability of important city services. In 2014, Stankovic [7] investigated eight key research topics, that is, massive scaling, architecture and dependencies, creating knowledge and big data, robustness, openness, security, privacy, and human-in-the-loop, to look at how the IoT could change the world, and concluded that the future will see the IoT gradually becoming an increasingly sophisticated utility in terms of sensing, actuation, communications, control, and creating knowledge from vast amounts of data.

In 2013, Hou et al. [8] designed a technique that enables secure initialization of a group of wireless devices, called Chorus, to defend against attack by an adversary. In order to achieve the key authentication property, the authors used Chorus to provide in-band group message authentication and group authenticated key agreement. In addition, two secure protocols are proposed to satisfy minimal hardware requirements and allow for minimal user effort; hence, the

protocols are scalable to a large group of wireless devices. Next, in light of the coupling between diverse IoT sensors, applications, and services, Ukil et al. [9] presented the specific characteristics, visions, and challenges relating to the IoT. Based on the observations and conclusions, the authors developed a privacy preservation framework as a part of an IoT platform, including a data masking tool, for both privacy and utility preservation. After that, since security and privacy are two of the most pressing challenges for the development of IoT applications or architecture, Alqassem [10] specified the essential privacy and security requirements for the IoT and further established an engineering framework as the proof of concept. With the emerging technology brought about by the IoT, the connectivity between objects, such as home appliances and consumer electronics, can be successfully created and applied. On the other hand, as trillions of objects each require their own unique identifications, low-cost RFID technology has begun to attract attention. For this reason, Aggarwal and Das [11] developed a lightweight RFID based protocol to enhance system security while retaining the protocol's efficiency. Later, Torjusen et al. [12] proposed a solution to integrate run-time verification enablers in the feedback adaptation loop of the ASSET [13], that is, an adaptive security framework for the IoT in the eHealth environment, and implemented the framework with colored Petri Nets. The run-time enablers produce machine based formal models of a system's status and context available at run-time. Moreover, the authors presented requirements for verification at run-time as formal specifications and introduced dynamic context monitoring and adaptation.

In recent years, IoT technologies have created an environment characterized by linkage between software systems and the physical world and have catalyzed a movement towards invisible and natural interactions among objects. However, providing efficient and customized personal services requires information about every distinct individual or entity, and this leads to the potential for privacy invasion. Hence, the information flow control and the design of low-cost tags (or, alternatively, small data size) become very important issues. From these observations, Evans and Eyers [14] introduced code templates for two small microcontrollers that make meaningful tagging possible. Later, Skarmeta et al. [15] proposed a capability-based access control mechanism that is built on public key cryptography. The essential ideas are based on the design of a lightweight token used for accessing CoAP (Constrained Application Protocol) resources and a digital signature algorithm inside the smart object. Being based on these two newly proposed techniques, the presented access control mechanism can provide better security and privacy for IoT based networks.

Different wireless communication technologies and network infrastructures are continuously being integrated, such as WSN, RFID systems, 3G technology, WIMAX, PAN, and so forth. In order to solve related security problems, Chen et al. [16] proposed a security architecture for an IoT environment. The proposed system architecture is adaptive to the IoT environment, and, in addition, a security verification mechanism was introduced. Later, Berhanu et al. [17] described a setup for adaptive security for IoT devices in an eHealth environment and discussed the validation of the setup through the study of the impact of antenna orientation on energy consumption. The authors then studied the feasibility of adopting lightweight security solutions as part of the ASSET infrastructure [13]. Next, Ning et al. [18] proposed an authentication scheme for IoT networks. The authors exploited U2IoT architecture to design an aggregated-proof based hierarchical authentication scheme for layered networks. In this authentication mechanism, several concepts, such as anonymous data transmission, mutual authentication, and different access authorities, were incorporated to achieve hierarchical access control. Moreover, Chen [19] proposed a possible solution based on an IBE (identity-based encryption) cryptosystem to efficiently and effectively solve the privacy and security threats encountered in the IoT. The elliptic curve cryptosystem is applied for achieving security in the IoT, and the authors established that essential security problems could be solved without too much resource consumption. After that, Paar [20] developed a concept that took into account both the destructive and constructive aspects embedded in the security of the IoT. The purpose was to examine the efficiency of tradeoffs between the desired security and the lowest possible cost.

Li and Xiong [21] developed a secure scheme for achieving confidentiality, integrity, authentication, and nonrepudiation in a logical single step. The proposed method splits the signcryption into two phases, with an online phase and an offline phase, and allows a sensor node in an identity-based cryptosystem to send a message to an Internet host. Hence, this scheme successfully provides an efficient solution for integrating WSN into IoT. Afterwards, in [22] the author analyzed the security requirements in different layers of the IoT and arrived at two conclusions: (a) the future security issues related to the IoT will mainly involve an open security system, individual privacy protection, and terminal security functionality; and (b) the security of the IoT must be seen from a perspective of integration which mandates the need for a series of policies, laws, and regulations, as well as a perfect security management system for mutual collocation. In 2013, Hummen et al. [23] introduced an IoT oriented authentication scheme which is based on the designs of prevalidation, session resumption, and handshake delegation. The proposed scheme can provide peer authentication and secure data transmission. In the following year, Kantarci and Hussein [24] demonstrated a framework for ensuring public safety in a cloud-centric IoT environment, where smartphones equipped with various types of sensors are deployed. To ensure trustworthiness in the framework, the authors proposed a reputation-based S2aaS scheme, called Trustworthy Sensing for Crowd Management (TSCM), which is able to collect sensing data based on a cloud model. In addition, the authors designed an auction procedure to select mobile devices for particular sensing tasks and to determine the appropriate payments to the users of the mobile devices that provide data. Furthermore, Tilanus et al. [25] discussed the motivations for opening up a given IoT so as to make the "things" it contains part of the global IoT. The proposed method comprises the definition and control of access rights to the discovery and use of virtual objects. It has the potential

to play a central role in the verification of access rights to virtual objects in the deployment of the IoT.

3. The Proposed Schemes

With the advancement of IoT networks, numerous network services and mobile devices have been deployed in pursuit of the betterment of human wellbeing. In general, users may register with the server once and maintain a set of verified data (or parameters) as the login token for system resource and service retrieval. The concept is called the single sign-on (SSO), whereby legal users are allowed to use the unitary token to access different services (or devices). Our proposed authentication scheme is based on the SSO technique, whereby a mobile application allows a user to utilize a mobile device with a unitary token to access multiple services. The techniques of a one-way hash function and random nonce are adopted to simultaneously ensure system efficiency and security robustness. In addition, we present a coexistence mechanism to prove the correctness of the coexisting medical items. With a proof for a group of tagged objects existing at the same time and the same place, medicine error prevention and patient safety can further be enhanced.

3.1. The Proposed Authentication Scheme. In our scheme, three entities, that is, the user U_i or the authentication server AS_j, and a trusted third-party authority TTPA, exist. The server and the trusted authority TTPA do not require the maintenance of any registration table for each registered communication entity. First, the TTPA selects two large primes p and q and computes $N = p \cdot q$. Then, the TTPA determines the key pair (e, d) such that $e \cdot d \equiv 1 \bmod \varphi(N)$, where $\varphi(N) = (p-1)(q-1)$. Next, the TTPA chooses a generator g over the finite field Z_n^*, where n is a large-enough odd prime number. Finally, the TTPA protects the secret d and publishes (e, g, n, N). Note that all the information about the parameters p and q is erased after initialization of the system. Now, both the user and the server need to store only one set of public parameters, that is, $\{e, g, g^a, n, N, h(\cdot)\}$ published by the TTPA, where a is a secret generated by the TTPA and $h(\cdot)$ is a collision-resistant one-way hash function.

Registration Phase. In the registration phase, each user U_i registers a unique and fixed bit-length identity ID_i at the TTPA side and obtains a secret token S_i from the TTPA through a secure channel. The secret token S_i is as $S_i = (ID_i \parallel h(ID_i \parallel b))^d \bmod N$, where b is also a secret generated by the TTPA. Similarly, the server AS_j registers a unique identity ID_j at the TTPA side and obtains a secret token S_j from the TTPA through a secure channel, where $S_j = (h(ID_j \parallel b))^d \bmod N$. Note that ID_j is public for each service request.

User Identification and Verification Phase (Figure 1). If the user U_i wants to request an authentication service from AS_j, the user identification and verification phase is invoked.

(1) U_i computes, $g^{n_1} \bmod N$, $(g^a)^{n_1} \bmod N$, and $A = (S_i \parallel n_1) \oplus h(g^{an_1})$ and sends message $m_1 = \{ID_j, g^{n_1}, A\}$ to AS_j, where n_1 is a random nonce generated by U_i. Upon receiving m_1, AS_j generates a random nonce n_2 to calculate $g^{n_2} \bmod N$, $(g^a)^{n_2} \bmod N$, and $B = (S_j \parallel n_2) \oplus h(g^{an_2})$ and forwards $m_2 = \{ID_j, g^{n_1}, A, g^{n_2}, B\}$ to the TTPA.

(2) After getting m_2, the TTPA computes $(g^{n_1})^a \bmod N$ and $(g^{n_2})^a \bmod N$ and derived $(S_i \parallel n_1)$ and $(S_j \parallel n_2)$ from $A \oplus h(g^{an_1})$ and $B \oplus h(g^{an_2})$. Next, the TTPA verifies S_i and S_j via the following computations:

$$(S_i)^e \bmod N = (ID_i \parallel h(ID_i \parallel b))^{de} \bmod N$$
$$(S_j)^e \bmod N = (h(ID_j \parallel b))^{de} \bmod N.$$

Compute $h(ID_i \parallel b)$ with retrieved value ID_i, and compare the result with retrieved value $h(ID_i \parallel b)$.

Compute $h(ID_i \parallel b)$ with received value ID_j and retrieved value $h(ID_j \parallel b)$?

If the above verification is passed, the TTPA chooses a random nonce n_3 and computes the following values: $(g^{n_1})^{n_3} \bmod N$, $(g^{n_2})^{n_3} \bmod N$, $C = h((g^{n_1})^{n_3} \parallel (g^{n_2})^{n_3} \parallel n_2)$, and $D = h(ID_j \parallel (g^{n_2})^{n_3} \parallel n_1)$. Next, the TTPA sends $m_3 = \{g^{n_1 n_3}, C, g^{n_2 n_3}, D\}$ to AS_j.

(3) Once AS_j obtains m_3, AS_j computes the session key $K_{ij} = (g^{n_1 n_3})^{n_2} \bmod N$ and examines the validity of value C. That is, AS_j calculates $h((g^{n_1})^{n_3} \parallel (g^{n_2})^{n_3} \parallel n_2)$ and compares it with value C. If these values are not equal, the protocol terminates. Otherwise, AS_j calculates $E = h(ID_j \parallel K_{ij})$ and sends $m_4 = \{g^{n_2 n_3}, D, E\}$ to U_i. After that, AS_j believes that U_i is an authorized user.

(4) After receiving m_4, U_i derives the session key $K_{ij} = (g^{n_2 n_3})^{n_1} \bmod N$ and examines the validity of values D and E. In other words, U_i computes $h(ID_j \parallel (g^{n_2})^{n_3} \parallel n_1)$ and $h(ID_j \parallel K_{ij})$ and examines whether the following two equations hold or not.

(a) Is computed $h(ID_j \parallel (g^{n_2})^{n_3} \parallel n_1)$ equal to received D?

(b) Is computed $h(ID_j \parallel K_{ij})$ equal to received E?

If these two examinations hold, U_i believes that AS_j is an authorized service provider with current session key K_{ij}.

3.2. The Proposed Coexistence Mechanism (Figure 2). Recently, the concept of coexistence proof for RF tags has been introduced to prove multiple tagged objects existing at the same time in the same place. Such proofs can be utilized in the application field of inpatient safety and medication management. In the proposed mechanism, each RF tag T_i requires supporting lightweight operations, that is, a 16-bit pseudorandom number generation (PRNG) function and bitwise exclusive OR (XOR) operation, and the backend coexistence server maintains two secret keys X_i and Y_i, an index-pseudonym IDS_i, and a unique identity ID_i for each T_i. In addition, the timestamp scheme and a random one-way permutation function F mapping within range $[1, 2L]$ are

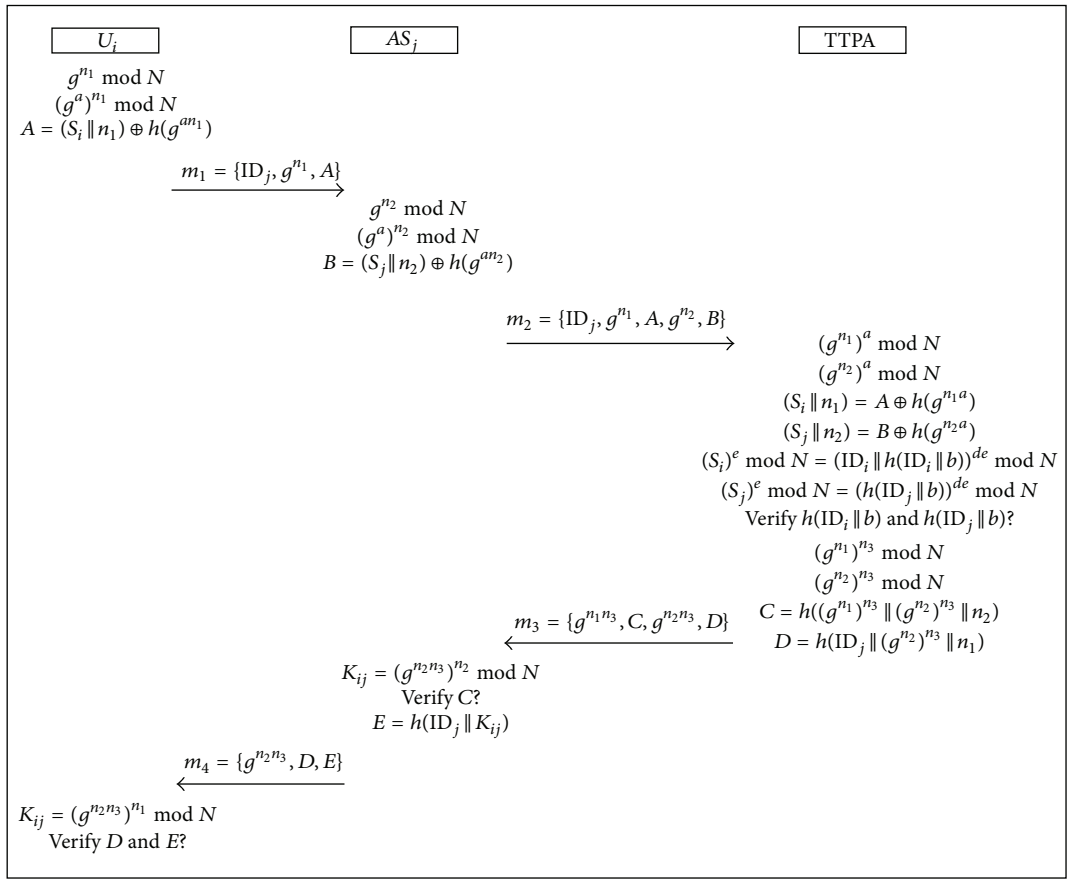

Figure 1: The proposed authentication scheme.

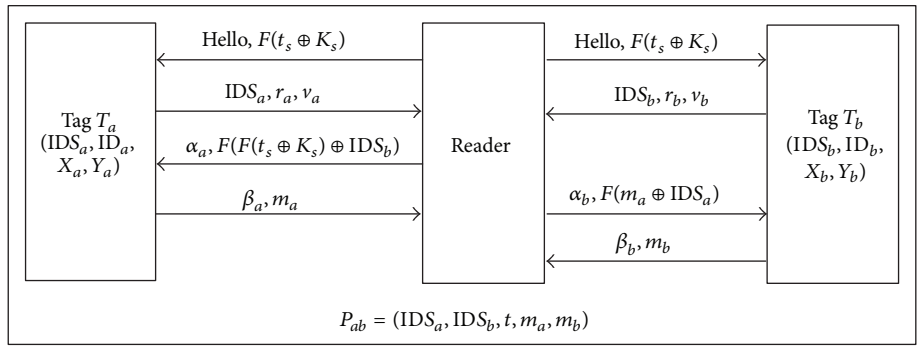

Figure 2: The proposed coexistence mechanism.

adopted in the proposed mechanism, where L is the security parameter. The implementation of F is based on PRNG and XOR to obtain operational efficiency for low-cost RF tags [26].

Step 1. First, the RF reader requests a well-protected timestamp $F(t_s \oplus K_s)$ from the backend server, where K_s is the server's secret key. Note that a corresponding log is created. An initial message $\{\mathrm{Hello}, F(t_s \oplus K_s)\}$ is then issued to T_a and T_b. After T_a and T_b get the incoming message, they both send $\{\mathrm{IDS}_a, r_a, v_a = F(F(Y_a) \oplus F(t_s \oplus K_s) \oplus r_a)\}$ and $\{\mathrm{IDS}_b, r_b, v_b = F(F(Y_b) \oplus F(t_s \oplus K_s) \oplus r_b)\}$ to the reader, respectively. And the reader immediately forwards these two responses with $F(t_s \oplus K_s)$ to the backend server. At the server side, if the verification of $F(t_s \oplus K_s)$ holds, (i.e., the validity of the current process time-period is verified), the server will then verify v_a and v_b. Once the examinations of v_a and v_b hold, the server sends two derived key values, that is, $K_a = F(F(F(Y_a)) \oplus r_a)$ and $K_b = F(F(F(Y_b)) \oplus r_b)$, to the reader and updates $\{Y_a, \mathrm{IDS}_a, Y_b, \mathrm{IDS}_b\}$ with $\{Y_a' = F(Y_a \oplus r_a), \mathrm{IDS}_a' = F(Y_a' \oplus \mathrm{IDS}_a), Y_b' = F(Y_b \oplus r_b), \mathrm{IDS}_b' = F(Y_b' \oplus \mathrm{IDS}_b)\}$.

Step 2. Upon obtaining K_a and K_b, the reader computes $\alpha_a = F(K_a \oplus F(F(t_s \oplus K_s) \oplus \mathrm{IDS}_b))$ and sends $\{\alpha_a, F(F(t_s \oplus K_s) \oplus \mathrm{IDS}_b)\}$ to T_a.

Step 3. After T_a receives $\{\alpha_a, F(F(t_s \oplus K_s) \oplus \mathrm{IDS}_b)\}$, T_a computes $K_a = F(F(F(Y_a)) \oplus r_a)$ with its own secret key Y_a and examines $\alpha_a = F(K_a \oplus F(F(t_s \oplus K_s) \oplus \mathrm{IDS}_b))$. If it holds, T_a will then calculate $m_a = F(\mathrm{IDS}_a \oplus F(F(t_s \oplus K_s) \oplus \mathrm{IDS}_b) \oplus X_a)$ and $\beta_a = F(F(K_a) \oplus m_a)$ and send $\{m_a, \beta_a\}$ to the reader. Then, T_a updates $\{Y_a, \mathrm{IDS}_a\}$ to $\{Y_a' = F(Y_a \oplus r_a), \mathrm{IDS}_a' = F(Y_a' \oplus \mathrm{IDS}_a)\}$.

Step 4. Once the reader gets $\{m_a, \beta_a\}$, it verifies $\beta_a = F(F(K_a) \oplus m_a)$. If the examination passes, the reader sends $\{\alpha_b, F(m_a \oplus \mathrm{IDS}_a)\}$ to T_b, where $\alpha_b = F(K_b \oplus F(m_a \oplus \mathrm{IDS}_a))$.

Step 5. After receiving $\{\alpha_b, F(m_a \oplus \mathrm{IDS}_a)\}$, T_b uses its key Y_b to compute $K_b = F(F(F(Y_b)) \oplus r_b)$ and verify $\alpha_b = F(K_b \oplus F(m_a \oplus \mathrm{IDS}_a))$. If it holds, T_b will send $\{\beta_b, m_b\}$ to the reader in which $m_b = F(\mathrm{IDS}_b \oplus F(m_a \oplus \mathrm{IDS}_a) \oplus X_b)$ and $\beta_b = F(F(K_b) \oplus m_b)$. Next, T_b updates $\{Y_b, \mathrm{IDS}_b\}$ with $\{Y_b' = F(Y_b \oplus r_b), \mathrm{IDS}_b' = F(Y_b' \oplus \mathrm{IDS}_b)\}$.

Step 6. Upon receiving $\{\beta_b, m_b\}$, the reader performs the verification of $\beta_b = F(F(K_b) \oplus m_b)$. If it holds, the reader confirms the coexistence of T_a and T_b with a valid proof $P_{ab} = (\mathrm{IDS}_a, \mathrm{IDS}_b, t, m_a, m_b)$.

4. Security Analyses

In this section, we analyze the security of the proposed authentication scheme for IoT based healthcare systems. We first present the adversary model and then conduct the security analysis of the proposed authentication scheme and the coexistence proof mechanism.

4.1. Adversary Model. In the communication model, we assume that a user U_i intends to establish a session key $SKey_{(i,j)}$ with an authentication server S_j via the help of the trusted third-party authority TTPA. We assume that the adversary can interact with the participants via oracle queries. The following major queries model the capabilities of the adversary. Note that Π_U^i is denoted as the instance i of a participant U.

(i) Send(Π_U^i, m): this query sends a message m to an oracle Π_U^i and gets the corresponding result.

(ii) Reveal(Π_U^i): this query returns the session key of the oracle Π_U^i.

(iii) Corrupt(U): this query returns the long-term secret key of U.

(iv) Execute($\Pi_{U_A}^i, \Pi_{U_B}^i$): this query models passive attacks in which the adversary can obtain the messages exchanged during the honest execution of the protocol between two oracles $\Pi_{U_A}^i$ and $\Pi_{U_B}^i$.

(v) Hash(m): the one-way hash function can be viewed as random functions within the appropriate range in the ideal hash model. Note that if m has never been queried before, it returns a truly random number r to the adversary and stores (r, m) in the hash table. Otherwise, it returns the previously generated result to the adversary.

(vi) Test(Π_U^i): this query models the security of the session key, that is, whether the real session key can be distinguished from a random string or not. For answering this question, an unbiased coin b is flipped by the oracle Π_U^i. When the adversary issues a single Test query to Π_U^i, the adversary obtains either the real session key $SKey_{(i,j)}$ if $b = 1$ or a random string if $b = 0$.

4.2. Security Analysis of the Proposed Authentication Scheme. In this subsection, we present the formal analysis of our proposed authentication scheme based on [27–29].

(i) AKE security (session key security): the adversary tries to guess the hidden bit b involved in a Test query via a guess b'. We say that the adversary wins the game of breaking the session key security of an AKE (Authenticated Key Exchange) protocol P if the adversary issues Test queries to a fresh oracle Π_U^i and guesses the hidden bit b successfully. The probability that the adversary wins the game is $\Pr[b' = b]$. In brief, the advantage of an adversary Eve in attacking protocol P can be defined as $\mathrm{Adv}_P^{\mathrm{AKE}}(\mathrm{Eve}) = |2 \times \Pr[b' = b] - 1|$. In brief, P is AKE-secure if $\mathrm{Adv}_P^{\mathrm{AKE}}(\mathrm{Eve})$ is negligible.

In the following subsection, we formally analyze the security of our proposed authentication protocol. Notations and definitions are presented first, and the formal security analysis is then demonstrated. We define T_{Eve} as the adversary's total running time, and q_s, q_r, q_c, q_e, and q_h are the number of Send, Reveal, Corrupt, Execute, and Hash queries, respectively.

(ii) *Computational Diffie-Hellman (CDH) assumption*: let $G = \langle g \rangle$ be a multiplicative cyclic group of order N, and let two random numbers t and k be chosen in Z_N^*. Given g, g^t, and g^k, the adversary Eve has a negligible success probability $\mathrm{Succ}_G^{\mathrm{CDH}}(\mathrm{Eve})$ of obtaining an element $z \in G$, such that $z = g^{tk}$ within polynomial time.

Theorem 1. *Let Eve be an adversary against the AKE security of our proposed authentication scheme within a time bound T_{Eve}, with less than q_s Send queries with the communication entities, and q_h times Hash queries. Then, $Adv_P^{AKE}(Eve, q_s, q_h) \leq q_h q_s \times Succ_G^{CDH}(T'_{Eve})$, where T'_{Eve} denotes the computational time for $Succ_G^{CDH}$ and $q_s = \sum_{i=1}^{5} q_{s\_i}$ is the sum of the number of $Send_1$, $Send_2$, $Send_3$, $Send_4$, and $Send_5$.*

Proof. Let Eve be an adversary that is able to get an advantage ε to break the AKE-secure protocol within time T_{Eve}. We can

construct a CDH attacker ATT from Eve to respond to all of Eve's queries and deal with the CDH problem, where ATT is given a challenge $\Omega = (g^t, g^k)$ and outputs an element z such that $z = g^{tk}$.

First, when Eve issues a Send_1 query as a start command, ATT responds with $m_1 = \{\text{ID}_j, g^{n_1}, A\}$ to Eve. Second, when Eve issues a Send_2 query, ATT randomly chooses two integers c_1 and c_2 from $[1, q_{s\_2}]$. If $c_1 \neq c_2$, ATT responds with $\{\text{ID}_j, g^{n_1}, A, g^{n_2}, B\}$ to Eve. Otherwise, ATT replaces the corresponding parameters of $m_2 = \{\text{ID}_j, g^{n_1}, A, g^{n_2}, B\}$ with the element g^k from Ω to generate a new and random message m_2' and then responds with the message m_2' to Eve. Third, once ATT receives the Send_3 query from Eve, ATT answers with the message $m_3 = \{g^{n_1 n_3}, C, g^{n_2 n_3}, D\}$ as the protocol. If the input of the query is from Ω, ATT generates a new message m_3' and then responds with m_3' to Eve. Fourth, when Eve issues the Send_4 query, ATT answers with $m_4 = \{g^{n_2 n_3}, D, E\}$ to Eve. Otherwise, a random string m_4' will be generated and sent to Eve. Finally, ATT answers a null string via a Send_5 query and then sets the protocol as being successful (or sets all conditions to true).

In the alternative, when Eve issues a $\text{Reveal}(\Pi_{U_i}^i)$ or a $\text{Reveal}(\Pi_{S_j}^j)$ query, ATT checks whether the oracle has been accepted and is fresh or not. If the result is positive, ATT answers with the session key $SKey_{(i,j)}$ to Eve. Otherwise, if the session key has been constructed from the challenge Ω, ATT terminates. When Eve issues $\text{Corrupt}(U_i)$, $\text{Corrupt}(S_j)$, $\text{Execute}(\Pi_{U_i}^i, \Pi_{S_j}^j)$, $\text{Hash}(m)$ queries, ATT answers in a straightforward way. When Eve issues a Test query, ATT answers in a straightforward way. Otherwise, if the session key has been constructed from the challenge Ω, ATT answers Eve with a random string with the same length as the session key $SKey_{(i,j)}$.

The above simulation is indistinguishable from any execution of the proposed protocol P except for one execution which involves the challenge Ω. The probability γ that ATT correctly guesses the session key, which Eve will make a Test query on, is equal to the probability of $c_1 = c_2$. Hence, we have $\gamma = 1/q_{s\_2} \geq 1/q_s$.

Assume that Eve issues a Test query to output b', where $b' = b$. This means that Eve knows the session key, so there must be at least one Hash query that returns the session key. The probability λ that ATT will choose the Hash query correctly is $\lambda \geq 1/q_h$. The successful probability $\text{Succ}_G^{\text{CDH}}(\text{ATT})$ that ATT will expose g^{kt} from the challenge Ω is thus $\text{Succ}_G^{\text{CDH}}(\text{ATT}) = \varepsilon \times \gamma \times \lambda \geq \varepsilon \times (1/q_s) \times (1/q_h)$. Finally, the advantage of Eve to break the AKE security of the protocol P is derived as follows:

$$\varepsilon = \text{Adv}_P^{\text{AKE}}(\text{Eve}, q_s, q_h) \leq q_h q_s \times \text{Succ}_G^{\text{CDH}}\left(T'_{\text{Eve}}\right). \quad (1)$$

□

4.3. Security Analysis of the Proposed Coexistence Scheme. In this subsection, we present the security claims of our proposed coexistence mechanism, such as data confidentiality and the resistance to proof counterfeit attack and replay attack.

Claim 1. The proposed coexistence mechanism is secure against proof counterfeit attack.

In our proposed coexistence mechanism, the timestamp is generated from the backend server and is well-protected by the server's secret key. This design removes the possibility of creating a legitimate but fake timestamp. Hence, it is impossible to create a counterfeit proof involving fake timestamp for the purpose of deception. In addition, the proposed mechanism is based on the random one-way permutation function F which is an efficient and robust computation component for low-cost RF tags [26]. As all the transmitted information is involved with the function F, it is difficult to derive the information without knowing all the communication entities' secret keys and the corresponding timestamps. Therefore, the proposed scheme can guarantee resistance to proof counterfeit attack. At the same time, system efficiency is delivered by virtue of the lightweight computation cost of the permutation function F.

Claim 2. The proposed coexistence mechanism can provide data confidentiality and resist against replay attack.

We assume that a malicious adversary Eve can intercept all messages communicated between RF tags T_a, T_b, and the reader. Because the adversary Eve cannot derive the private keys, that is, X_i or Y_i for the target tag T_i, from messages transmitted via the public channel, the data involved in the transmitted messages cannot be retrieved. In addition, the one-way property of the function F serves to guarantee the unrecovery of the input data, so that data confidentiality can thus be achieved. Moreover, in each session of our proposed scheme, we exploit random numbers, that is, r_a and r_b, in randomizing transmitted messages. In addition, the timestamp t_s is involved with the construction of the verification message P_{ab}. These random numbers and the timestamp can not only randomize the transmitted messages but can ensure resistance against replay attack.

5. Conclusion

In this paper, we have introduced two secure communication protocols for IoT based healthcare systems, in which a SSO based authentication scheme and a coexistence proof mechanism are proposed. The proposed authentication scheme is appropriate for use as the main protection technique for an IoT based healthcare environment consisting of various types of sensors, such as thin/fat sensors, sensor tags, or tagged items. For IoT network services, the proposed authentication scheme can provide robust entity authentication and secure data communication. In addition, we further present a coexistence proof protocol for proving multiple tagged objects (or sensors and/or sensor tags) existing at the same time and the same place. The generated proofs can be utilized in the application field of inpatient safety and medication

management. Based on the security analysis results we have conducted, we are confident that the feasibility of these two proposed schemes can be guaranteed.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgments

This work was supported by the Taiwan Information Security Center (TWISC) and the Ministry of Science and Technology, Taiwan, under Grants numbered MOST 103-2221-E-259-016-MY2 and MOST 103-2221-E-011-090-MY2.

References

[1] S. Forsström, P. Österberg, and T. Kanter, "Evaluating ubiquitous sensor information sharing on the internet-of-things," in *Proceedings of the 11th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom '12)*, pp. 1454–1460, June 2012.

[2] S. Wang, "Internet of things based on EPC technology and its application in logistics," in *Proceedings of the 2nd International Conference on Artificial Intelligence, Management Science and Electronic Commerce (AIMSEC '11)*, pp. 3077–3080, August 2011.

[3] A. J. Jara, M. A. Zamora, and A. F. Skarmeta, "Knowledge acquisition and management architecture for mobile and personal health environments based on the internet of things," in *Proceedings of the 11th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom '12)*, pp. 1811–1818, June 2012.

[4] A. Zakriti and Z. Guennoun, "Service entities model for the internet of things: a bio-inspired collaborative approach," in *Proceedings of the International Conference on Multimedia Computing and Systems (ICMCS '11)*, pp. 1–5, April 2011.

[5] S. Tozlu, M. Senel, W. Mao, and A. Keshavarzian, "Wi-Fi enabled sensors for internet of things: a practical approach," *IEEE Communications Magazine*, vol. 50, no. 6, pp. 134–143, 2012.

[6] J. Jin, J. Gubbi, S. Marusic, and M. Palaniswami, "An information framework for creating a smart city through internet of things," *IEEE Internet of Things Journal*, vol. 1, no. 2, pp. 112–121, 2014.

[7] J. A. Stankovic, "Research directions for the internet of things," *IEEE Internet of Things Journal*, vol. 1, no. 1, pp. 3–9, 2014.

[8] Y. Hou, M. Li, and J. D. Guttman, "Chorus: scalable in-band trust establishment for multiple constrained devices over the insecure wireless channel," in *Proceedings of the 6th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec '13)*, pp. 167–178, ACM, Budapest, Hungary, April 2013.

[9] A. Ukil, S. Bandyopadhyay, J. Joseph, V. Banahatti, and S. Lodha, "Negotiation-based privacy preservation scheme in internet of things platform," in *Proceedings of the 1st International Conference on Security of Internet of Things (SecurIT '12)*, pp. 75–84, August 2012.

[10] I. Alqassem, "Privacy and security requirements framework for the internet of things (IoT)," in *Proceedings of the 36th International Conference on Software Engineering (ICSE Companion '14)*, pp. 739–741, June 2014.

[11] R. Aggarwal and M. L. Das, "RFID security in the context of internet of things," in *Proceedings of the 1st International Conference on Security of Internet of Things (SecurIT '12)*, pp. 51–56, August 2012.

[12] A. B. Torjusen, H. Abie, E. Paintsil, D. Trcek, and Å. Skomedal, "Towards run-time verification of adaptive security for IoT in eHealth," in *Proceedings of the European Conference on Software Architecture Workshops (ECSAW '14)*, Article no. 4, ACM, Vienna, Austria, August 2014.

[13] ASSET project, *http://asset.nr.no*.

[14] D. Evans and D. M. Eyers, "Efficient data tagging for managing privacy in the internet of things," in *Proceedings of the IEEE International Conference on Green Computing and Communications (GreenCom '12)*, pp. 244–248, IEEE, Besançon, France, November 2012.

[15] A. F. Skarmeta, J. L. Hernández-Ramos, and M. V. Moreno, "A decentralized approach for security and privacy challenges in the Internet of Things," in *Proceedings of the IEEE World Forum on Internet of Things (WF-IoT '14)*, pp. 67–72, March 2014.

[16] D. Chen, G. Chang, L. Jin, X. Ren, J. Li, and F. Li, "A novel secure architecture for the Internet of things," in *Proceedings of the 5th International Conference on Genetic and Evolutionary Computing (ICGEC '11)*, pp. 311–314, IEEE, Xiamen, China, September 2011.

[17] Y. Berhanu, H. Abie, and M. Hamdi, "A testbed for adaptive security for IoT in eHealth," in *Proceedings of the International Workshop on Adaptive Security (ASPI '13)*, article 5, September 2013.

[18] H. Ning, H. Liu, and L. T. Yang, "Aggregated-proof based hierarchical authentication scheme for the internet of things," *IEEE Transactions on Parallel and Distributed Systems*, vol. 26, no. 3, pp. 657–667, 2015.

[19] W. Chen, "An IBE-based security scheme on internet of things," in *Proceedings of the IEEE 2nd International Conference on Cloud Computing and Intelligence Systems (CCIS '12)*, pp. 1046–1049, November 2012.

[20] C. Paar, "Constructive and destructive aspects of embedded security in the internet of things," in *Proceedings of the ACM SIGSAC Conference on Computer & Communications Security (CCS '13)*, pp. 1495–1496, ACM, Berlin, Germany, November 2013.

[21] F. Li and P. Xiong, "Practical secure communication for integrating wireless sensor networks into the internet of things," *IEEE Sensors Journal*, vol. 13, no. 10, pp. 3677–3684, 2013.

[22] L. Lan, "Study on security architecture in the internet of things," in *Proceedings of the International Conference on Measurement, Information and Control (MIC '12)*, pp. 374–377, IEEE, Harbin, China, May 2012.

[23] R. Hummen, J. H. Ziegeldorf, H. Shafagh, S. Raza, and K. Wehrle, "Towards viable certificate-based authentication for the Internet of Things," in *Proceedings of the 2nd ACM Workshop on Hot Topics on Wireless Network Security and Privacy (HotWiSec '13)*, pp. 37–41, April 2013.

[24] B. Kantarci and T. Hussein, "Trustworthy sensing for public safety in cloud-centric internet of things," *IEEE Internet of Things Journal*, vol. 1, no. 4, pp. 360–368, 2014.

[25] P. Tilanus, B. Ran, M. Faeth, D. Kelaidonis, and V. Stavroulaki, "Virtual object access rights to enable multi-party use of sensors," in *Proceedings of the IEEE 14th International Symposium and Workshops on a World of Wireless, Mobile and Multimedia Networks (WoWMoM '13)*, pp. 1–7, June 2013.

[26] S. H. Wu, K. F. Chen, and Y. F. Zhu, "A secure lightweight RFID binding proof protocol for medication errors and patient safety," *Journal of Medical Systems*, vol. 36, no. 5, pp. 2743–2749, 2015.

[27] M. Bellare, D. Pointcheval, and P. Rogaway, "Authenticated key exchange secure against dictionary attacks," in *Advances in Cryptology—EUROCRYPT 2000*, vol. 1807 of *Lecture Notes in Computer Science*, pp. 140–156, Springer, Berlin, Germany, 2000.

[28] M. Bellare and P. Rogaway, "Entity authentication and key distribution," in *Proceedings of the Annual International Cryptology Conference (CRYPTO' 93)*, vol. 773 of *Lecture Notes in Computer Science*, pp. 232–249, 1993.

[29] S. Blake-Wilson, D. Johnson, and A. Menezes, "Key agreement protocols and their security analysis," in *Crytography and Coding: 6th IMA International Conference Cirencester, UK, December 17–19, 1997 Proceedings*, vol. 1355 of *Lecture Notes in Computer Science*, pp. 30–45, Springer, Berlin, Germany, 1997.