Secure Authentication Scheme for Medicine Anti-counterfeiting System in IoT Environment

Mohammad Wazid, *Student Member, IEEE*, Ashok Kumar Das, *Member, IEEE*, Muhammad Khurram Khan*, *Senior Member, IEEE*, Abdulatif Al-Dhawailie Al-Ghaiheb, Neeraj Kumar, *Member, IEEE*, Athanasios V. Vasilakos, *Senior Member, IEEE*

***Abstract*—A counterfeit drug is a medication or pharmaceutical product, which is manufactured and made available on the market to deceptively represent its origin, authenticity and effectiveness, etc, and causes serious threats to the health of a patient. Counterfeited medicines make an adverse effect on the public health and also cause revenue loss to the legitimate manufacturing organizations. In this paper, we propose a new authentication scheme for medicine anti-counterfeiting system in the Internet of Things (IoT) environment which is used for checking the authenticity of pharmaceutical products (dosage forms). The proposed scheme utilizes the near field communication (NFC) and is suitable for mobile environment, which also provides efficient NFC update phase. The security analysis using the widely-accepted Real-Or-Random (ROR) model proves that the proposed scheme provides the session key (SK) security. The proposed scheme also protects other known attacks which are analyzed informally. Furthermore, the formal security verification using the broadly-accepted Automated Validation of Internet Security Protocols and Applications (AVISPA) tool shows that the proposed scheme is secure. The scheme is efficient with respect to computation and communication costs, and also it provides additional functionality features when compared to other existing schemes. Finally, for demonstration of the practicality of the scheme, we evaluate it using the broadly-accepted NS-2 simulation.**

***Index Terms*—Anti-counterfeiting, authentication, AVISPA, NS2 simulation, security.**

I. Introduction

World Health Organization (WHO) defined counterfeit medicine as "one which is deliberately and fraudulently mislabeled with respect to identity and/or source" [1], [2], [3]. Counterfeiting of various products creates problem to different manufacturing industries such as food and beverage, automotive parts, software, cosmetic, jewelery, etc. It causes serious threat to pharmaceuticals products. People, who purchase and use counterfeit medicines, suffer a lot because these medicines do not provide any relief to their diseases. The concern issue threatens the public health and also causes revenue losses to the legitimate manufacturing organizations. The International Chamber of Commerce of Geneva pointed out that the estimation of annual sales of counterfeit products in the world amounted to US$ 650 billion [4].

According to WHO data, there are about 100,000 deaths happened in a year in Africa due to use of counterfeit drugs. The British "International Policy Network" estimated that 700,000 deaths in a year are happened due to the use of counterfeit malaria and tuberculosis drugs. Counterfeiting can be happened with branded as well as generic products. WHO further noticed that more than 30% of medicines on sale are counterfeited in some part of Africa, Asia and Latin America. According to the report of WHO, the commonly counterfeited drugs are antibiotics, anti-malarials, hormones and steroids, and now anticancer and antiviral drugs are also included in the list [1], [2], [3].

At the same time various organizations of different countries are fighting against counterfeiting of medicines. According to Xinhua News Agency of China, China is using "recognition and tracing technology" packaging of medicines in which anti-counterfeit labels are sealed on each medicine package. African countries are also using new technologies to fight against counterfeiting of medicines. A handheld spectrometer, called the TruScan, used at airports and border posts can detect the counterfeiting of medicines by performing the analysis of their chemical compositions. The technologies such as simple and free text messages are also being used to detect counterfeit medicines. The organizations such as mPedigree Network and Sproxil implemented a system in which legitimate drug manufacturing organizations use label on the drug packages with an encrypted code. When a customer/consumer wants to buy that drug, he/she scratches off the label on the drug package and text the code to the system of company which authenticates the drug package without any charge. After authentication of drug package, the system responses with a text message accordingly whether it is fake/actual. Thus, a consumer can easily come to know the authenticity of the drug package very easily and without any cost. However, the drawback with this technique is that it is not fully automated as the consumer first needs to scratch off the label, and then to type the code and send to the system, which requires a lot of users involvement [1], [2], [3].

M. Wazid is with the Center for Security, Theory and Algorithmic Research, International Institute of Information Technology, Hyderabad 500 032, India (E-mail: mohammad.wazid@research.iiit.ac.in).

A. K. Das is with the Center for Security, Theory and Algorithmic Research, International Institute of Information Technology, Hyderabad 500 032, India (E-mail: iitkgp.akdas@gmail.com, ashok.das@iiit.ac.in).

M. K. Khan is with the Center of Excellence in Information Assurance, King Saud University, Riyadh, Kingdom of Saudi Arabia (E-mail: mkhurram@ksu.edu.sa). *(*Corresponding author: Muhammad Khurram Khan)*

A. A. Al-Ghaiheb is with the Clinical Pharmacy Department, College of Pharmacy, King Saud University, Riyadh, Kingdom of Saudi Arabia (E-mail: alatif@ksu.edu.sa).

N. Kumar is with the Department of Computer Science and Engineering, Thapar University, Patiala 147 004, India (e-mail: neeraj.kumar@thapar.edu).

A. V. Vasilakos is with the Department of Computer Science, Electrical and Space Engineering, Lulea University of Technology, Lulea 971 87, Sweden (e-mail: th.vasilakos@gmail.com).

The Radio Frequency Identification (RFID) permits identification of unique items which use radio waves. A RFID reader typically communicates with RFID tags that contain digital information in microchips [5]. RFID based anti-counterfeiting technology has emerged as an effective tool to prevent counterfeiting, because it complements the commonly used anti-counterfeiting methods (for example, colors, shifting inks, fingerprints and chemical markers) [4], [5]. These methods, however, do not use the automatic verification of product authenticity.

Device-to-Device (D2D) communications is a type of technology which enables devices to communicate directly with each other without the involvement of fixed networking infrastructures (for example, access point and base station) [6]. Some typical applications of original D2D communications rely on bluetooth, WiFi-direct and near field communication (NFC). NFC is a short-range high frequency (HF) wireless communication technology, which transfers data (text or numbers) between two NFC-enabled devices over about a 10 cm distance [7], [8]. NFC tags such as $NTAG213$ contains small microchips with little aerials which can store a small amount of data for transferring to another NFC enabled device, such as a mobile devices. NFC technology is an upgradation of the existing RFID technology. Under this technology, the interface of a smartcard and a reader are combined into a single device. Users can easily share data between NFC-enabled devices. It is also used in other various applications such as wireless bill payment, electronic traveling ticket on existing contact-less infrastructure, etc. [7], [8].

In the recent years, several authentication protocols have been proposed for ambient assisted living system and wireless sensor networks [9], [10], [11]. Yan *et al.* [12] presented a new anonymous authentication protocol which has the ability to authenticate both pseudonyms and trust levels in order to support trustworthy pervasive social networking with privacy preservation. Furthermore, several RFID based anti-counterfeiting techniques have been proposed [5], [13], [14], [15], [16], [17]. However, most of the existing RFID based anti-counterfeiting schemes are not secure and have several drawbacks, such as replay, man-in-the-middle and reader impersonation attacks. In addition, some of them are not suitable for mobile environment, and they do not also have efficient RFID update phase and even they are not user-friendly. The NFC based anti-counterfeiting techniques are very useful for mobile environment in which no card reader is required, user only requires a NFC-enabled mobile device that reads the data stored in the NFC tag and sends to the server.

The Internet of Things (IoT) refers to the network of physical objects which have Internet Protocol address (IP address) for Internet connectivity [18]. All these physical devices can communicate over the Internet.

This paper presents a new authentication scheme for medicine anti-counterfeiting system in IoT Environment. The proposed scheme has the ability to authenticate medicine dosage forms online by the help of mobile device. The proposed scheme is also capable to prevent the counterfeiting of medicine dosage forms. It further provides secure mutual authentication between the NFC tag placed on a dosage form and the server. In the proposed scheme a NFC enabled mobile device acts as an interface between the NFC tag and the server, which reads the information stored in the NFC tag and sends the information to the server. The server verifies the authenticity of the dosage forms and sends response to the NFC enabled mobile device user. On the basis of the response received from the server, the customer (patient) can take his/her decision whether to purchase that medicine or not.

A. System architecture of medicine anti-counterfeiting in IoT environment

Fig. 1 shows the system architecture of medicine anti-counterfeiting in IoT environment. As we know in Internet of Things (IoT) every physical objects such as servers, mobile device users have an IP address for Internet connectivity, all these devices communicate to each other using the Internet. In the given architecture we have three different types of servers: 1) information server (IS_i), 2) authentication server (AS_j) and 3) database server (DS_k). Apart from that we have mobile device user at the manufacturer site and a customer who wants to buy the medicine's dosage forms. Both user at the manufacturer site and customer can communicate with the servers. Note that all users have near field (NFC) enabled mobile device and all servers are able to communicate with each other. Initially, each manufacturer at the manufacturer site registers the details of dosage forms (package) to the information server using their NFC enabled mobile device. After the successful registration (IS_i) sends this information to AS_j and DS_k. This considered architecture is different from the existing architecture [5]. In this architecture AS_j has the complete information which is required to check the authenticity of the dosage forms. Therefore we are not using any pedigree server which is available in the current architectures [5]. During the authentication process some screened records are generated at AS_j which are then sent to DS_k for storage. These records will be then used for the future authentication. The steps involved in dosage forms anti-counterfeiting process are given in Section I-B

The roles of various servers are described below:

Information server (IS_i): The initial registration of each dosage form is done at IS_i. In addition, IS_i sends the registration information of dosage forms to AS_j and DS_k.

Authentication server (AS_j): It is used for the authentication of the dosage form. It authenticates the dosage form on the basis of the information provided by the IS_i. It also sends the authentication response (whether fake or real) to the customer/patient and also to the DS_k.

Database server (DS_k): It stores the information provided by the IS_i and AS_j. The screened records generated during the authentication process are stored in DS_k. In the proposed scheme, a NFC tag is updated after each successful authentication process. This server maintains these records. If there are n number of sites between the manufacturing organization and a customer (consumer), the NFC tag needs to be updated at these sites. These information are also stored at this server. By seeing these records, the authority (i.e., database administrator) can observe who, when and where the NFC tag was updated,

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2017.2706752, IEEE Internet of Things Journal

and it will be useful in cross checking whether the NFC tag is updated by a legal intermediate party. It is not desirable to maintain all these records at the AS_j, because we want to dedicate authentication process solely on the AS_j. Due to this reason, the role of DS_k is essential.

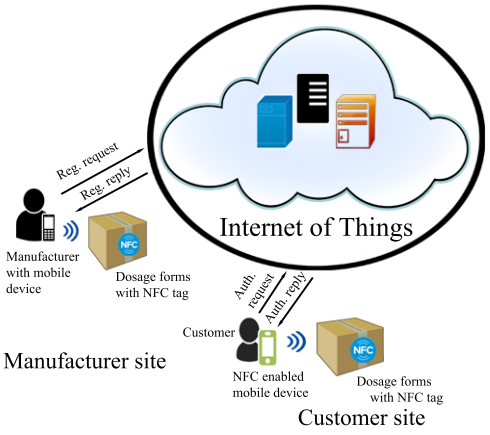

Fig. 1. System architecture of medicine anti-counterfeiting

1) Implementation site: The proposed medicine anti-counterfeiting system in IoT environment is efficient and has more usability as it suits the mobile environment. As far as implementation is concerned the pharmaceutical companies can also implement this type of anti-counterfeiting system in their information technology (IT) department. But this act will not be fully trusted by the customers/ patients. So, it would be better if a trusted third party, say digital anti-counterfeiting party, can implement this type of system.

2) Usability of the proposed system: Our scheme is secure as well as user friendly. A customer (patient) just needs the NFC enabled mobile device with the Internet connectivity to check authenticity of medicine package. So, the user can perform anti-counterfeiting process anywhere, anytime in any part of the world.

B. Steps involved in medicine anti-counterfeiting process

The steps involved in dosage forms anti-counterfeiting process are given in Fig. 2 and also discussed below:

- In the first step the user at the manufacturer site registers the medicine's dosage forms to the information server (IS_i). IS_i then computes some information which is required for the authentication process and sends this to the NFC tag of the dosage forms for storage.
- The IS_i shares the dosage forms complete information with the database server (DS_k) and the limited information which is only used for the authentication to the authentication server (AS_j).
- To check the authenticity of the dosage forms the customer/patient sends authentication request to ASj, then AS_j checks the authenticity of the dosage forms and response to the patient accordingly. AS_j also shares authentication response with DS_k. DS_k stores all screened records which can be used in the future authentications/transactions process.

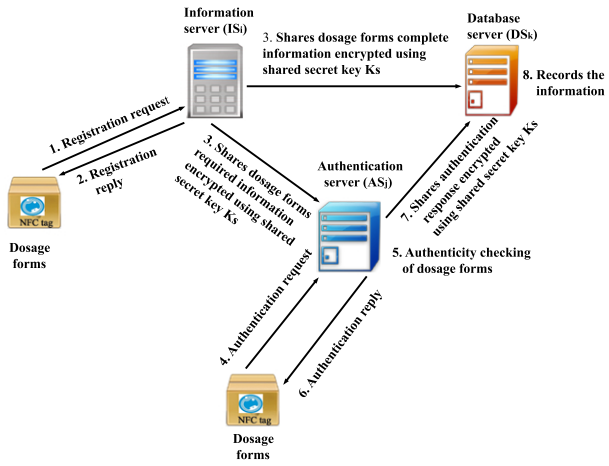

Fig. 2. Steps involved in dosage forms anti-counterfeiting process

Each medicine package has a NFC tag, which contains various information related to the product. It consists of an electronic product code (EPC) [19]. An EPC is a universal identifier that provides unique identity of some physical object and it can be easily stored in NFC tag [20]. Two identical products can be distinguished by the EPC. EPC contains several information such as product's manufacturing date, its origin, batch number, etc. The basic format of the EPC is given in Fig. 3. It contains the following fields: 1) header, 2) EPC manager number, 3) object class (OC), and 4) serial number (SN). The header field identifies the length, type and version of EPC. The EPC manager number maintains the subsequent partitions. The serial number field is a unique serial number for each EPC. The lengths of header, EPC manager number, object class and serial number are 8 bits, 28 bits, 24 bits and 36 bits, respectively. Thus, the total length of EPC is 96 bits.

Header	EPC manager number	Object class (OC)	Serial number (SN)

Fig. 3. Structure of EPC

C. Motivation

The counterfeiting of medicines causes the serious threat to the society. The counterfeited medicines make an adverse effect on the health of the people and also cause revenue loss to the legitimate medicine manufacturing organizations. In the recent years, several anti-counterfeiting techniques have been proposed. However, most of the existing schemes are not secure and have several drawbacks. Various attacks such as replay, man-in-the-middle and reader impersonation attacks are feasible in most of existing schemes. In addition, some of these schemes are not suitable for mobile environment, and they do not have an efficient user-friendly RFID/NFC update phase.

In this paper, we propose a new authentication scheme for medicine anti-counterfeiting system in the IoT environment, which can be used for checking the authenticity of

medicines (dosage forms). The proposed scheme authenticates the medicine dosage forms online by the help of mobile device. There is a NFC enabled mobile device, which acts as an interface between the NFC tag and the authentication server, which reads the information stored in the NFC tag and sends the information to the authentication server. The authentication server verifies the authenticity of the dosage forms and sends response to the NFC enabled mobile device user. The customer (patient) finally receives the response (for example, if the medicine is fake or genuine, or if it is a genuine medicine then which medicine he/she is going to purchase). On the basis of this response, he/she can take decision whether to purchase that medicine or not.

D. Main contributions

The following are the main contributions:

- We present a new medicine anti-counterfeiting scheme to check the authenticity of the medicine's dosage forms in IoT environment.
- With the help of the product authentication & session key establishment phase, after successful mutual authentication between NFC enabled mobile device (NFC tag) and the authentication server, a secret session key is established for future secure communication between them. Our scheme also supports NFC tag update.
- The widely-used ROR model is used formal security analysis to prove the session key security. The informal security analysis also shows that our scheme protects various known attacks.
- Finally, our scheme requires the lightweight symmetric encryption/decryption and one-way hash function computations only. The communication and computation costs of our scheme are also comparable with the related existing schemes.

E. System Models

The following models are considered in this paper.

1) Network Model: The network model is depicted in Fig. 1, in which there is a customer (mobile device user) MU who wants to check the authenticity of dosage forms. To check the authenticity of dosage forms MU scans the NFC tag placed on each dosage form and sends the information to AS_j. The mobile device acts as the bridge between the dosage form and AS_j. The registration process of each dosage form and the authenticity of the dosage form are already discussed in Section I-A.

2) Threat Model: The Dolev-Yao (DY) threat model [21] is followed in the proposed scheme. As per the DY model, two communicating parties communicate over an insecure channel [22]. The same threat model is applied in the proposed scheme, in which the communication channel is public, and the end-point entities (MU and AS_j) are assumed to be not trusted. An intruder can eavesdrop the exchanged messages and also can delete or modify the content of the transmitted messages.

F. Structure of the paper

In Section II, we review the existing anti-counterfeiting techniques. Section III discusses some mathematical preliminaries which are used for describing and analyzing the proposed scheme. Section IV gives the description of various phases related to the proposed scheme. The rigorous security analysis of the proposed scheme is given in Section V. Section VI simulates the proposed scheme for the formal security verification using the broadly-accepted AVISPA tool. Section VII compares the performance of the proposed scheme with related existing schemes. We then make some concluding remarks in Section IX.

II. Related work

Choi *et al.* [5] reviewed several existing RFID based anti-counterfeiting mechanisms, and also gave a RFID-based anti counterfeiting system for product tracking and tracing. Using the proposed system, the consumers can verify the authenticity of the product, which they opt to buy the products.

Kim *et al.* [23] proposed an application-level technique for anti-counterfeiting, which employs a RFID reader available to a consumer's device (for example, PDA and mobile phone). It checks the authenticity of the product.

Kim *et al.* [24] proposed a technique for anti-counterfeiting solution, which is used to track and trace a product through whole life-cycle. It provides the authentication to the product packages having RFID tags. The technique uses location information especially from location based service (LBS) of the consumer devices. On basis of information obtained, the system can take fine-grained decision about the product's authenticity.

Public-key cryptography (PKC) can be used for products anti-counterfeiting, but the main issue is its implementation in RFID tags. Batina *et al.* [14] investigated the PKC (elliptic curve based cryptosystem) implementation feasibility for anti-counterfeiting applications. Jeng *et al.* [25] provided a survey on techniques used for anti-counterfeiting. The RFID tags counterfeiting issue are discussed in this survey. Some methods are also provided to make RFID-tag unclonable. Further, research direction of the anti-counterfeiting domain is also provided in that survey.

Chen *et al.* [15] proposed an anti-counterfeit secure transaction scheme, which is capable to perform the online authentication. Their scheme uses the one-way function and public-key cryptographic operations, such as public-key encryption/decryption, and signature generation and verification. However, their scheme has some security limitations, such as it does not provide strong replay attack protection and also protection against RFID tag cloning attack.

Rau and Hsiao [26] proposed an anti-counterfeiting scheme that provides a novel RFID structure to defend various possible attacks (for example, replay attack, counterfeit attack and forward key security). In their technique, certain parameters including electronic product code (EPC) are hidden by some random numbers in order to provide privacy protection and EPC leaking. However, their scheme is also vulnerable to strong replay attack and RFID tag cloning attack. In addition, their scheme does not provide the session key security.

Chien and Chen [27] analyzed the weaknesses of some EPC Class 1 GEN-2-conformed security protocols, and then proposed a protocol, which provides better security level as compared to the analyzed protocols, and also it conforms to the EPC Class 1 GEN-2 standards. Similar to the schemes of Chen *et al.* [15] and Rau-Hsiao [26], their scheme does not also provide strong replay and RFID tag cloning attacks protection. Furthermore, their scheme does not provide the session key security.

Choi *et al.* [28] proposed an anti-counterfeiting system for apparel products. They also discussed some of the key data management issues such as data synchronization problem, e-pedigree formatting and traceability or visibility controlling. Their system supports products authentication in the item-level, products anti-lost in pallet-level and products status prediction in batch-level.

Ma *et al.* [16] proposed an anti-counterfeiting system for cosmetic brands. Their system analyzes the distribution channels and sales methods to provide the anti-counterfeiting to cosmetic brands. Staake *et al.* [17] proposed a mechanism for products authentication. The proposed system has the functionality to handle tags, which support strong cryptography and use for anti-counterfeiting process.

Cheung *et al.* [4] presented a track-and-trace system for RFID-based anti-counterfeiting. They pointed out various possible implementation aspects of the system. These include selection of a tag, product tagging, programming of tag and its locking. Choi *et al.* [13] presented another anti-counterfeiting system for a tag data processing and synchronization (TDPS) to generate initial e-pedigrees for various products. RFID-enabled apparel packaging line is also implemented for performance validation of TDPS.

Blass *et al.* [29] proposed a scheme, which allows object genuineness verification in RFID-based supply chains. Zanetti *et al.* [30] also proposed a technique to detect the cloned RFID tags in supply chains in which the tag cloning is detected by a centralized detector. Tuyls *et al.* [31] investigated the techniques that restrict the cloning of RFID-tags, which are used in anti-counterfeiting system.

III. Mathematical foundation

This section briefly discusses the collision-resistant one-way hash function [32], [33], [34] and the indistinguishability of encryption under chosen plaintext attack (IND-CPA) [35].

Definition 1 (Collision-resistant hash function)**.** *Let h: $\{0,1\}^* \rightarrow \{0,1\}^l$ be a one-way hash function. It is a deterministic algorithm, which produces a fixed-length, say l-bit binary string $h(a) \in \{0,1\}^l$ as output for an arbitrary-length binary input string $a \in \{0,1\}^*$ as input. If $Adv_{\mathcal{A}}^{HASH}(t)$ indicates the advantage of an adversary $\mathcal{A}$ to find a collision in execution time t, we have, $Adv_{\mathcal{A}}^{HASH}(t) = Pr[(a,a') \leftarrow_R \mathcal{A}$: $a \neq a'$, $h(a) = h(a')]$. Here $Pr[X]$ is the probability of an event X and $(a,b) \leftarrow_R \mathcal{A}$ is a pair (a,b) which is randomly chosen by $\mathcal{A}$. $\mathcal{A}$ is also allowed to be probabilistic and $Adv_{\mathcal{A}}^{HASH}(t)$ is calculated over the random choices. By an (η,t)-adversary $\mathcal{A}$ attacking the collision resistance of $h(\cdot)$, we mean that the runtime of $\mathcal{A}$ is at most t and that $Adv_{(A)}^{HASH}(t) \leq \eta$.*

Definition 2 (IND-CPA)**.** *Suppose SE/ME denotes the single/multiple eavesdropper, respectively. Let OR_{sk_1}, OR_{sk_2}, …, OR_{sk_N} be N different independent encryption oracles associated with encryption keys $sk_1, sk_2, \ldots, sk_N$, respectively. The advantage functions of SE and ME are given, respectively, as $Adv_{\Omega,SE}^{IND-CPA}(l) = |2Pr[SE \leftarrow OR_{sk_1}; (p_0,p_1 \leftarrow_R SE); \theta \leftarrow_R \{0,1\}; \beta \leftarrow_R OR_{sk_1}(p_\theta) : SE(\beta) = \theta] - 1|$, and $Adv_{\Omega,ME}^{IND-CPA}(l) = 2Pr[ME \leftarrow OR_{sk_1}, \ldots, OR_{sk_N}; (p_0,p_1 \leftarrow_R ME); \theta \leftarrow_R \{0,1\}; \beta_1 \leftarrow_R OR_{sk_1}(p_\theta), \ldots, \beta_N \leftarrow_R OR_{sk_N}(p_\theta) : ME(\beta_1, \ldots, \beta_N) = \theta] - 1$, where Ω is an encryption scheme. Under the single (multiple) eavesdropper setting, Ω is IND-CPA secure if $Adv_{\Omega,SE}^{IND-CPA}(l)$ (respectively, $Adv_{\Omega,ME}^{IND-CPA}(l)$) becomes negligible (in the security parameter l) for any probabilistic, polynomial time (PPT) adversary SE (ME).*

IV. The proposed scheme

The proposed scheme explained in this section consists of three phases: 1) product registration, 2) product authentication & session key agreement, and 3) NFC tag update. In the proposed scheme, the communication channel between the mobile device (smart phone) and the NFC tag is assumed to be secure. We apply the improved version of the NFC-SEC standard to secure the communication channel between mobile device (smart phone) and the NFC tag [36]. The proposed scheme also uses the current timestamps in order to protect the replay attacks. For this purpose, we assume the time synchronization among the entities in the network.

In the proposed network model shown in Fig. 1, there are several IS_is, AS_js and DS_ks in the IoT environment. A trusted authority first selects a leading IS_i among all ISs, a leading AS_j among ASs and also a leading DS_k among DSs. To manage the security associations (SAs) among the servers, during the bootstrapping time using the Internet Key Exchange Protocol Version 2 (IKEv2) protocol [37] all the leading IS_i, AS_j and DS_k will establish a secret key K_s among them. To establish K_s among them, they will use the three-party station-to-station Diffie-Hellman key exchange protocol [38]. After that the key K_s is shared among all ISs by the leading IS_i using a pre-shared secret among them. In a similar fashion, the key K_s is also shared among all ASs and DSs by their respective leading AS_j and DS_k. Note that the key K_s has the most important role in the proposed scheme for security bootstrapping among the protocol entities because all the communication among the IS_is, AS_js and DS_ks are securely performed using K_s only. In addition, the key K_s is also useful during the product and session key agreement phase.

The notations listed in Table I are used in the scheme.

A. Product registration phase

Each medicine's dosage forms has a NFC tag, which contains all product related information. To check the authenticity of the product, the manufacturing organization needs to register it to the information server (IS_i). Then IS_i shares this information with the database server (DS_k) and the only required information for authentication with the authentication

TABLE I
NOTATIONS USED IN OUR SCHEME

Symbol	Description
IS_i	Information server
AS_j	Authentication server
DS_k	Record server
MU	NFC enabled mobile device user
ID_s	Identity of server AS_j
K_s	Shared 1024-bit secret key among IS_i, AS_j and DS_k
$h(\cdot)$	Collision-resistant one-way hash function
T_1, T_3	Current timestamps generated by MU
T_2	Current timestamp generated by AS_j
R_1	Random number generated by MU
R_2	Random number generated by AS_j
ΔT	Maximum transmission delay
SK	Session key between MU and AS_j
$\oplus, \|\|$	Bitwise XOR and concatenation operations

server (AS_j). DS_k stores all the screened records which can be further used in the future authentication. The user (customer/patient) has a NFC enabled mobile device, which acts as the interface between AS_j and the NFC tag. The mobile device of user (MU) reads the information stored in the NFC tag, and then sends it to AS_j to check authenticity of the medicines packages.

The steps of product registration between the NFC tag and IS_i are given below:

Step RG1. Initially, the authorized mobile device user (MU) at the manufacturing organization sends the EPC stored in the NFC tag to IS_i via a secure channel. Note that EPC is also shared with AS_j.

Step RG2. After receiving EPC securely, IS_i computes $A = E_{K_s}(EPC)$, $B = h(K_s|| \ ID_s|| \ SN|| \ PRTS)$, where SN is serial number given in EPC, ID_s is identity of AS_j, $PRTS$ is the product registration timestamp, and K_s is the shared secret key among IS_i, AS_j and DS_k. Then, IS_i sends the registration reply message $\langle A, B, h(\cdot)\rangle$ to MU via secure channel, which further stores $\langle A, B, h(\cdot)\rangle$ in the NFC tag's memory. IS_i also sends the message $\langle A, B, h(\cdot)\rangle$ securely to AS_j. Finally, AS_j stores $\langle A, B, h(\cdot), ID_s, K_s\rangle$ in its database.

B. Product authentication and session key agreement phase

Suppose a mobile device user (a customer, i.e., a patient) MU wants to buy medicines. MU uses his/her mobile device to read the information $\langle A, B, h(\cdot)\rangle$ available in the NFC tag of dosage form, and then the mobile device generates an authentication request message and sends it to AS_j via a public channel. After successful authentication between NFC_{tag}/MU and AS_j, both MU and AS_j agree on a common session key. Note that the authorized intermediate vendors can also follow the same process for the dosage form authentication. We need the following steps to execute this phase:

Step PAKA1. MU generates the current timestamp T_1 and a random nonce R_1, and then computes $C = h(A||B||T_1) \oplus R_1$. After that MU sends the authentication request message $MSG_1 = \langle A, C, T_1\rangle$ to AS_j via public channel.

Step PAKA2. Let the message $MSG_1 = \langle A, C, T_1\rangle$ be received at time T_1^* by AS_j. The first task of AS_j is to check the validity of received timestamp T_1, which is done by verifying the condition $|T_1 - T_1^*| \leq \Delta T$. If timestamp is valid, AS_j decrypts A to retrieve EPC as $EPC' = D_{K_s}(A)$ by using shared secret key K_s. It then computes $B' = h(K_s|| \ ID_s \ ||SN')$, where SN' is serial number of the decrypted EPC. AS_j further checks if $B' = B$. If the condition holds, the product is valid and MU is also authenticated by AS_j. Otherwise, AS_j sends a acknowledgment message to MU that the medicine is counterfeited. AS_j also sends its response (whether medicine's dosage forms is real/fake) to DS_k via securely encrypted using the shared key K_s.

Step PAKA3. AS_j computes $R_1 = C \oplus \ h(A|| \ B'|| \ T_1)$. Then, AS_j generates the current timestamp T_2 and a random nonce R_2, and calculates $D = h(A|| \ B'|| \ T_1|| \ T_2|| \ ID_s) \oplus R_2$, $E = ID_s \oplus \ h(R_1 \ ||A \ ||B')$. Further, AS_j computes the session key $SK = h(ID_s \ ||B' \ ||R_1 \ ||R_2 \ ||T_1 \ ||T_2)$, $G = h(SK|| \ T_2) \oplus OC$ and $SKV = h(SK|| \ T_2|| \ R_1|| \ R_2|| \ OC)$, where OC is the object class containing in the decrypted EPC. AS_j then sends the authentication reply message $MSG_2 = \langle D, E, G, SKV, T_2\rangle$ to MU via public channel.

Step PAKA4. Upon receiving $MSG_2 = \langle D, E, G, SKV, T_2\rangle$, MU validates T_2 by checking the condition $|T_2 - T_2^*| \leq \Delta T$. If it is valid, MU computes $ID_s' = E \oplus \ h(R_1 \ ||A \ ||B)$ and $R_2' = D \oplus \ h(A|| \ B|| \ T_1|| \ T_2 \ ||ID_s')$. It further computes session key $SK' = h(ID_s' \ ||B \ ||R_1 \ ||R_2' \ ||T_1 \ ||T_2)$, $OC' = G \oplus h(SK'||T_2)$ and $SKV' = h(SK'|| \ T_2 \ ||R_1 \ ||R_2' \ ||OC')$. MU then checks the condition $SKV' = SKV$. If it holds, AS_j is authenticated by MU and also MU displays the user which class OC' of the medicine he/she is authenticating with AS_j. After that the computed session key SK ($= SK'$) is stored at both sides MU and AS_j for future secure communication.

The summary of this phase is provided in Fig. 4.

NFC tag (NFC_{tag})/ mobile device (MU)	Authentication server (AS_j)
Generate current timestamp T_1, random number R_1.	
Compute $C = h(A\|\|B\|\|T_1) \oplus R_1$.	
$MSG_1 = \langle A, C, T_1\rangle \xrightarrow{\quad}$ (via a public channel)	
	Check if $\|T_1 - T_1^*\| \leq \Delta T$?
	If so, retrieve $EPC' = D_{K_s}(A)$.
	Compute $B' = h(K_s\|\|ID_s\|\|SN')$.
	Check if $B' = B$?
	If so, product is valid and MU is authenticated by AS_j.
	Generate current timestamp T_2, random number R_2.
	Compute $R_1 = C \oplus h(A\|\|B'\|\|T_1)$,
Check if $\|T_2 - T_2^*\| \leq \Delta T$?	$D = h(A\|\|B'\|\|T_1\|\|T_2\|\|ID_s) \oplus R_2$,
If so, compute $ID_s' = E \oplus h(R_1\|\|A\|\|B)$,	$E = ID_s \oplus h(R_1\|\|A\|\|B')$,
$R_2' = D \oplus h(A\|\| \ B\|\| \ T_1\|\| \ T_2 \ \|\|ID_s')$.	session key $SK = h(ID_s\|\|B'\|\|$
Computes session key $SK' = h(ID_s'$	$R_1\|\|R_2\|\|T_1\|\|T_2)$,
$\|\|B\|\|R_1\|\|R_2'\|\|T_1\|\|T_2)$,	$G = h(SK\|\| \ T_2) \oplus OC$
$OC' = G \oplus h(SK'\|\|T_2)$	$SKV = h(SK\|\|T_2\|\|R_1\|\|R_2\|\|OC)$.
$SKV' = h(SK'\|\|T_2\|\|R_1\|\|R_2'\|\|OC')$.	$MSG_2 = \langle D, E, G, SKV, T_2\rangle \xleftarrow{\quad}$ (via a public channel)
Check if $SKV' = SKV$?	
If so, the product is authenticated by user, and informs user about object class OC of the genuine medicine.	
Both MU and AS_j share the same session key SK ($= SK'$).	

Fig. 4. Product authentication and session key agreement phase

Remark 1. *To provide the strong replay attack protection, the techniques in [39], [40] are adopted along with the timestamp. AS_j can store the tuple (EPC, B, T_1) in its database. Next time, when AS_j receives another authentication request*

message, say $MSG_1' = \langle A', C', T_1' \rangle$, it verifies the timeliness of T_1'. If it is valid, AS_j continues to decrypt A' using K_s to retrieve $EPC' = D_{K_s}(A')$. AS_j further calculates $B' = h(K_s \,||ID_s\, ||SN')$, where SN' is the serial number of the extracted EPC', and checks if $B' = B$ and $T_1' = T_1$ hold simultaneously. If these hold simultaneously, MSG_1' is obviously a replay message. On the other hand, AS_j treats MSG_1' as a fresh authentication request message and replaces (EPC, B, T_1) with (EPC', B', T_1') in its database.

Remark 2. *Consider the following threat associated with the NFC applications. Suppose the information $(A, B, h(\cdot))$ stored in the NFC tag (on the bottle of the genuine medicine) is read and then written to the other NFC tag (on the bottle of potassium cyanide) by an attacker $\mathcal{A}$. In such a scenario, in Step PAKA4, the MU computes session key $SK' = h(ID_s' \,||B\, ||R_1\, ||R_2'\, ||T_1\, ||T_2)$, the object class of the EPC as $OC' = G \oplus h(SK'||T_2)$ and $SKV' = h(SK'||\, T_2\, ||R_1\, ||R_2'\, ||OC')$. Though the condition $SKV' = SKV$ is satisfied, the MU displays the user which class OC' of the medicine he/she is authenticating with AS_j. Thus, the user will be able to know whether the medicine is genuine or fake or which medicine the user wants to purchase with the help of the OC containing in the EPC of the medicine package's NFC tag.*

C. NFC tag update phase

To overcome NFC tag cloning, we provide an important feature in our scheme in which after each successful product authentication, AS_j can update the information EPC available in the NFC tag by using secure session key established between MU and AS_j. Note that this phase is basically performed by the authorized intermediate vendors. The following steps are performed in this update process:

Step TU1. AS_j chooses a new EPC, say EPC_{new} and generates the current timestamp T_3. AS_j computes $A' = E_{K_s}(EPC_{new})$, $B' = h(K_s||\, ID_s||\, SN_{new})$, where SN_{new} is the new serial number present in EPC_{new}. Furthermore, AS_j computes $F = E_{SK}(A',\, B',\, T_3)$ using the already established session key SK. AS_j then sends the update request $MSG_3 = \langle F \rangle$ to MU at the intermediate vendor's site via open channel.

Step TU2. Upon receiving $MSG_3 = \langle F \rangle$, MU first decrypts F using the already established session key SK' $(= SK)$ during the product authentication & session key agreement phase to retrieve A, B and T_3 as $(A',\, B',\, T_3') = D_{SK'}(F)$. If the validity of the decrypted timestamp T_3' holds, that is, $|T_3' - T_3^*| \leq \Delta T$ holds, where T_3^* is the time when MU received the message MSG_3, MU updates (A, B) with (A', B') in the NFC tag, respectively.

Step TU3. Finally, AS_j updates (A, B) with (A', B') in its database.

V. Security analysis

This section analyzes the security of our scheme.

A. Security analysis using Real-Or-Random model

We apply the Real-Or-Random (ROR) model [41], [42] for our formal security analysis. Two entities are involved in the product authentication & session key agreement phase: NFC enabled mobile device MU and authentication server AS_j.

Participants. Assume that $INS_{AS_j}^t$ and INS_{MU}^r are the instances t and r of AS_j and MU, respectively. $INS_{AS_j}^t$ and INS_{MU}^r are called the *oracles*.

Accept state. Upon receiving last expected protocol message, if an instance INS^t goes to an accept state, INS^t is said to be in accepted state. The session identification (sid) is formed by the ordered concatenation of all communicated messages by INS^t.

Partnering. Two instances INS_{MU}^r of MU and $INS_{AS_j}^t$ of AS_j are known to be partnered if the three simultaneous conditions between them are fulfilled: 1) both are in accepted state, (2) both mutually authenticate each other and share the same sid and 3) they are mutual partners of each other.

Freshness. We say $INS_{AS_j}^t$ or INS_{MU}^r is fresh, if the session key SK is not revealed to an attacker, say $\mathcal{A}$ using the reveal query $RVL(INS^t)$ given below.

Adversary. An adversary $\mathcal{A}$ will have full control over all communications. In addition, $\mathcal{A}$ can access the following queries:

$EXE(INS^t, INS^r)$: In order to obtain the messages exchanged between two honest participants in the network, $\mathcal{A}$ can apply this query. It can be modeled as an eavesdropping attack.

$RVL(INS^t)$: This query reveals the current session key SK generated by INS^t (and its partner) to an adversary $\mathcal{A}$.

$SND(INS^t, msg)$: It is modeled as an active attack. $\mathcal{A}$ can send a message msg to a participant instance INS^t. In reply, a response message is received by $\mathcal{A}$.

$TST(INS^t)$: This corresponds to the semantic security of the session key SK between MU and AS_j, which follows the indistinguishability in the ROR model [41]. In this case, before the game starts, an unbiased coin b is tossed, and then $\mathcal{A}$ retains the result as secret to take decision about the output of this query. If $\mathcal{A}$ executes $TST(INS^t)$ query and the established SK is fresh, INS^t will return SK if $b = 1$. Otherwise, it returns a random number in the same domain when $b = 0$. On the other hand, it produces null result $(\perp)$.

Semantic security of the session key. In this security, the challenge of an adversary $\mathcal{A}$ is to differentiate the real session key SK from a random key. $\mathcal{A}$ can query many TST queries to either $INS_{AS_j}^t$ and INS_{MU}^r. The outcome result of TST query needs to be consistent with respect to b. After the experiment is over, $\mathcal{A}$ returns a guessed bit b'. $\mathcal{A}$ wins the game when the condition $b' = b$ is met. Let $SUCC$ be the event where $\mathcal{A}$ wins the game. The advantage of $\mathcal{A}$ to break the semantic security of the proposed authenticated key agreement (AKE) scheme, say $\mathcal{P}$ is then $Adv_{\mathcal{P}}^{AKE} = |2.Pr[SUCC] - 1|$. $\mathcal{P}$ is secure in the ROR sense, if $Adv_{\mathcal{P}}^{AKE} \leq \psi$, for any sufficiently small $\psi > 0$.

Random oracle. A one-way hash function $h(\cdot)$ is available to all the participants including $\mathcal{A}$. We model $h(\cdot)$ as a random oracle, say $Hash$ oracle as in [42].

Theorem 1. *Let $\mathcal{A}$ be an attacker that run in the polynomial time t against our proposed scheme $\mathcal{P}$ in the ROR model. Then, the probability of breaking the session-*

key security (SK-security) of $\mathcal{P}$ by $\mathcal{A}$ is $Adv_{\mathcal{P}}^{AKE} \leq q_h^2/|Hash| + 2Adv_{\Omega}^{IND-CPA}(l)$, where $Adv_{\Omega,SE}^{IND-CPA}(l)$ $/Adv_{\Omega,ME}^{IND-CPA}(l)$, q_h, $|Hash|$ and l are the advantage of $\mathcal{A}$ of breaking the IND-CPA secure symmetric cipher Ω (provided in Definition 2), the number of $Hash$ queries, the range space of the hash function $h(\cdot)$ and the security parameter, respectively, and $Adv_{\Omega}^{IND-CPA}(l) = Adv_{\Omega,SE}^{IND-CPA}(l)$ or $Adv_{\Omega,ME}^{IND-CPA}(l)$.

Proof. We have four different games $Game_i$ $(i = 0, 1, 2, 3)$. Let ES_i be an event wherein $\mathcal{A}$ can successfully guess the bit b in $Game_i$ and also win the game. We start with $Game_0$, where the real attack against our protocol is considered, and then end with $Game_3$, where $\mathcal{A}$ has negligible advantage in breaking the SK-security of $\mathcal{P}$. The proof contains the following games:

$Game_0$: In this game, the bit b is selected at the beginning of $Game_0$. Therefore, by definition,

$$Adv_{\mathcal{P}}^{AKE} = |2.Pr[ES_0] - 1|. \quad (1)$$

$Game_1$: We transfer $Game_0$ into $Game_1$ by adding simulation of $\mathcal{A}$'s eavesdropping attacks, where $\mathcal{A}$ can make $EXE(INS^t, INS^r)$ query. At the end of the game, $\mathcal{A}$ can make the TST query. $\mathcal{A}$ needs to take decision if the result of the TST oracle is SK or a random number. Note that SK is computed by AS_j as $SK = h(ID_s||B'||R_1||R_2||T_1||T_2)$, which is computed by MU as $SK' = h(ID_s'||B||R_1||R_2'||T_1||T_2)$, where $SK = SK'$. Computation of $SK(= SK')$ requires the permanent secrets ID_s, K_s and $B = h(K_s||\ ID_s||\ SN)$ and temporary secrets R_1 and R_2. Without these secrets, $\mathcal{A}$ can not compute SK $(= SK')$. It is then clear that $\mathcal{A}$'s winning probability of the game is not increased by eavesdropping of messages. In other words, $Game_0$ is equivalent to $Game_1$, and we have,

$$Pr[ES_0] = Pr[ES_1]. \quad (2)$$

$Game_2$: $Game_1$ is transferred into $Game_2$ using the simulation of the SND and $Hash$ oracles, which is modeled an active attack. $\mathcal{A}$ then decides if a party accepts a fake or modified message. $\mathcal{A}$ is allowed to many $Hash$ queries to check whether any collision occurs or not. The messages $MSG_1 = \langle A,\ C,\ T_1\rangle$ and $MSG_2 = \langle D,\ E,\ G,\ SKV,\ T_2\rangle$ involve the permanent secrets ID_s, K_s and $B = h(K_s||\ ID_s||\ SN)$, temporary secrets R_1 and R_2 and current timestamps T_1, T_2 and T_3. Note that R_1 and R_2 are random numbers. Hence, there will be no collision even if $\mathcal{A}$ make the SND query. With the results from the birthday paradox [43], it follows that

$$|Pr[ES_1] - Pr[ES_2]| \leq q_h^2/(2.|Hash|). \quad (3)$$

$Game_3$: Finally, this game models also an attack which is transformed from $Game_2$. In this case, $\mathcal{A}$ needs to calculate SK $(= SK')$, which uses ID_s, B, R_1, R_2, T_1 and T_2 from the eavesdropping messages MSG_1 and MSG_2. To compute B, $\mathcal{A}$ needs the secret key K_s, ID_s and the serial number SN in EPC. To know SN, $\mathcal{A}$ needs to decrypt $A = E_{K_s}(EPC)$ using the key K_s, which is unknown to $\mathcal{A}$. Therefore, we have

$$|Pr[ES_2] - Pr[ES_3]| \leq Adv_{\Omega}^{IND-CPA}(l). \quad (4)$$

Note that all the established session keys between MU and AS_j are random and independent. Hence, no information about b is leaked to $\mathcal{A}$. As a result, we have

$$Pr[ES_3] = 1/2. \quad (5)$$

From Equation (1), we have

$$\frac{1}{2}.Adv_{\mathcal{P}}^{AKE} = |Pr[ES_0] - \frac{1}{2}|. \quad (6)$$

Using the triangular inequality, we have

$$\begin{aligned} |Pr[ES_1] - Pr[ES_3]| &\leq |Pr[ES_1] - Pr[ES_2]| + \\ &\quad |Pr[ES_2] - Pr[ES_3]| \\ &\leq \frac{q_h^2}{2.|Hash|} + Adv_{\Omega}^{IND-CPA}(l). \end{aligned} \quad (7)$$

Using Equations (2), (5) and (7), we have

$$|Pr[ES_0] - \frac{1}{2}| \leq \frac{q_h^2}{2.|Hash|} + Adv_{\Omega}^{IND-CPA}(l). \quad (8)$$

Finally, from Equations (6) and (8), we obtain:

$$Adv_{\mathcal{P}}^{AKE} \leq q_h^2/|Hash| + 2Adv_{\Omega}^{IND-CPA}(l).$$

□

B. Informal security analysis

1) Replay attack: This attack occurs when an attacker tries to be a legitimate user by using the previously eavesdropped information. An attacker can then record the exchanged messages and further retransmit them. From Remark 1, it follows that the proposed scheme provides strong replay attack protection against an attacker.

2) Man-in-the-middle attack: Suppose an adversary $\mathcal{A}$ intercepts the authentication request $MSG_1 = \langle A,\ C,\ T_1\rangle$ and tries to create a valid message $MSG_1' = \langle A',\ C',\ T_1'\rangle$, where T_1' and R_1' are the current timestamp and random nonce, respectively, generated by $\mathcal{A}$, $A' = A$, $C' = h(A||\ B||\ T_1')$ $\oplus R_1'$. To modify C to C', $\mathcal{A}$ needs B, where $B = h(K_s||\ ID_s\ ||SN)$ and $A = E_{K_s}(EPC)$. To calculate B, $\mathcal{A}$ needs the secret key K_s, ID_s and serial number SN of EPC, which are unknown to $\mathcal{A}$. Therefore, $\mathcal{A}$ can not modify $MSG_1 = \langle A,\ C,\ T_1\rangle$. In a similar way, $\mathcal{A}$ can not also modify the authentication response message $MSG_2 = \langle D,\ E,\ G,\ SKV,\ T_2\rangle$. Therefore, the man-in-the-middle attack from both sides MU and AS_j is not possible on our scheme.

3) Protection against tag cloning: To make a clone of NFC tag, its serial number SN (which is inside EPC) is required. The NFC tag stores only the information $\{A, B, h(\cdot)\}$ in its memory. The values of A and B are $A = E_{K_s}(EPC)$ and $B = h(K_s||\ ID_s\ ||SN)$, respectively, where K_s is a shared key among the different servers only known to them and ID_s is the authentication server's ID_s only known to itself. To decrypt $A = E_{K_s}(EPC)$, the shared key K_s is required, which is not known to the attacker. However, the collision resistance property of $h(\cdot)$ puts it very difficult to obtain K_s, ID_s and SN from B. Therefore, our protocol provides protection against the NFC tag cloning.

4) Session key security: During the product authentication & session key agreement phase, AS_j sends $MSG_2 = \langle D, E, G, SKV, T_2 \rangle$ to MU, where $D = h(A|| B'|| T_1|| T_2|| ID_s) \oplus R_2$, $E = ID_s \oplus h(R_1|| A|| B')$, $G = h(SK|| T_2) \oplus OC$ and $SKV = h(SK|| T_2|| R_1|| R_2|| OC)$. Suppose an adversary $\mathcal{A}$ generates timestamps T_1', T_2', and random nonces R_1' and R_2'. Further, $\mathcal{A}$ tries to compute $D' = h(A'|| B'|| T_1' ||T_2' ||ID_s) \oplus R_2'$, $E' = ID_s \oplus h(R_1'|| A'|| B')$ and $G' = h(SK'|| T_2') \oplus OC$. Without knowledge of A', B', OC and ID_s, the computation of D', E' and G' are infeasible. Also the collision resistance property of $h(\cdot)$ puts it also very difficult to obtain SK' from SKV'. Therefore, our protocol provides session key security.

5) User impersonation attack: A valid MU sends product authentication message $MSG_1 = \langle A, C, T_1 \rangle$ to AS_j. Suppose an adversary $\mathcal{A}$ tries to impersonate as MU by creating another valid message, say $MSG_1' = \langle A', C', T_1' \rangle$ and then sending it to AS_j instead of MSG_1. To perform this attack, $\mathcal{A}$ requires $A' = E_{K_s}(EPC')$, $C' = h(A'|| B'|| T_1') \oplus R_1'$, where $B' = h(K_s||ID_s||SN')$, and T_1' and R_1' are the timestamp and random number selected by $\mathcal{A}$. $\mathcal{A}$ can not impersonate as MU because he/she can not compute A' without knowing the shared key K_s, which is only known to the servers. $\mathcal{A}$ also tries to compute $C' = h(A'||B'||T_1') \oplus R_1'$. The computation of C' is computationally hard because of the collision resistance property of $h(\cdot)$ as SN, K_s and ID_s are embedded into B. So, $\mathcal{A}$ can not send $MSG_1' = \langle A', C', T_1' \rangle$ on behalf of MU. Thus, this attack is eliminated in our scheme.

6) Server impersonation attack: A legitimate AS_j sends product authentication reply message $MSG_2 = \langle D, E, G, SKV, T_2 \rangle$ to MU. Suppose an adversary $\mathcal{A}$ tries to impersonate as AS_j by creating another valid message, say $MSG_2' = \langle D', E', G', SKV', T_2' \rangle$ and then sending it to MU instead of MSG_2, where R_2' and T_2' are the random number and timestamp chosen by $\mathcal{A}$. In order to perform AS_j impersonation attack, $\mathcal{A}$ requires to compute D', E', G' and SKV'. However, $\mathcal{A}$ can not impersonation as AS_j because he/she can not compute D', E' and G' without knowing A', B', ID_s and OC. Furthermore, to compute $SKV' = h(SK'|| T_2'|| R_1'|| R_2' ||OC)$, $\mathcal{A}$ requires SK. Thus, without knowing SK', he/she can not compute SKV'. So, $\mathcal{A}$ can not send authentication reply message $MSG_2' = \langle D', E', G', SKV', T_2' \rangle$ to MU on behalf of AS_j. This indicates that server impersonation attack is also eliminated.

7) Mutual authentication: During the product authentication and session key agreement phase, the MU sends the authentication request message $MSG_1 = \langle A, C, T_1 \rangle$ to AS_j via public channel. After receiving this message, the AS_j first checks the validity of the received timestamp T_1 and if it is valid, it retrieves EPC as $EPC' = D_{K_s}(A)$ by using shared secret key K_s. It then computes $B' = h(K_s|| ID_s ||SN')$ and checks if $B' = B$. If the condition holds, the product is valid and the product (MU) is authenticated by AS_j. After that AS_j sends the authentication reply message $MSG_2 = \langle D, E, G, SKV, T_2 \rangle$ to MU via public channel. After checking the validity of the received timestamp T_2 in the message, the MU calculates $ID_s' = E \oplus h(R_1 ||A ||B)$, $R_2' = D \oplus h(A|| B|| T_1|| T_2 ||ID_s')$, the session key $SK' = h(ID_s' ||B ||R_1 ||R_2' ||T_1 ||T_2)$, $OC' = G \oplus h(SK'||T_2)$ and $SKV' = h(SK'|| T_2 ||R_1 ||R_2' ||OC')$. MU then verifies the condition $SKV' = SKV$. If it holds, AS_j is authenticated by MU and informs the user about object class OC of the genuine medicine. Only after the mutual authentication between MU and AS_j, the session key SK ($= SK'$) is stored by both MU and AS_j for their future secure communications. As a result, the proposed scheme provides secure mutual authentication between MU and AS_j.

VI. Simulation for formal security verification using AVISPA tool

We simulate the proposed scheme for the formal security verification using the broadly-accepted AVISPA tool [44], [45], [46]. The AVISPA tool only detects if a security protocol is secure against the replay and man-in-the-middle attacks.

A designed security protocol needs to be first implemented using the role-based High Level Protocol Specification Language (HLPSL) of AVISPA tool. The HLPSL is then translated into intermediate form (IF) with the help of the HLPSL2IF translator. The IF is fed into one of four back ends supported by the AVISPA tool. These backends are 1) On-the-fly Model-Checker (OFMC), 2) Constraint-Logic-based Attack Searcher (CL-AtSe), 3) SAT-based Model-Checker (SATMC), and 4) Tree Automata based on Automatic Approximations for the Analysis of Security Protocols (TA4SP). These backends finally produce the output format (OF), which tells whether the tested protocol is safe or unsafe against replay and man-in-the-middle attacks. The detailed description of these backends along with the specification of HLPSL and AVISPA tool can be found in [44], [45], [46], [47], [48].

The roles for the product registration, product authentication & session key agreement, and NFC update phases of the proposed scheme are implemented in HLPSL. Apart from these basic roles, two mandatory roles: session and environment need to be implemented in HLPSL.

The proposed scheme is tested using the widely-used OFMC and CL-AtSe backends. The executability check on non-trivial HLPSL specification, replay attack check and Dolev-Yao model check are verified in our scheme. The detailed descriptions of these verifications are given in [45], [46]. The simulated results using the OFMC and CL-AtSe backends given in Fig. 5 clearly indicate that the replay and man-in-the-middle attacks are protected by the proposed scheme.

VII. Comparative study

This section compares the performance of our scheme with existing schemes of Chien-Chen [27], Chen *et al.* [15], Rau-Hsiao [26] for computation and communication overheads for the product authentication & session key agreement and NFC update phases. The functionality features of these schemes and our scheme are also compared. The product registration is only needed for one-time. Due to this, we have ignored it in the comparative study. We have included the NFC update phase in the comparative study as it happens after each successful authentication.

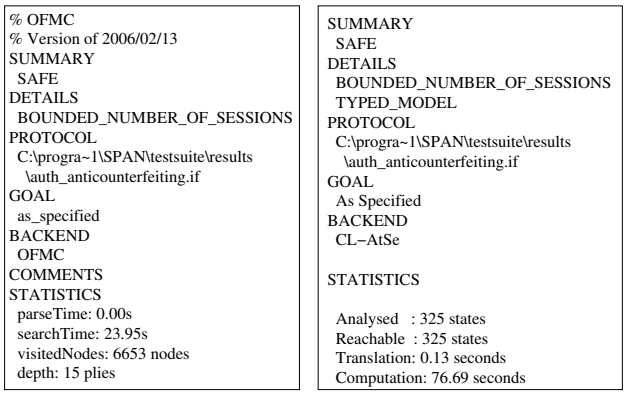

Fig. 5. Simulation results using OFMC and CL-AtSe backends

A. Computation cost comparison

Table II compares the computation cost of our scheme with existing schemes [15], [26], [27]. We have used the following notations: T_{PRNG}, T_h, T_{PENC}/T_{PDEC}, T_{SENC}/T_{SDEC} denote computational time for a pseudo random number generator, a cryptographic one-way hash function $h(\cdot)$, a public-key encryption/decryption (if we apply RSA algorithm) and a symmetric encryption/decryption (for example, if AES algorithm is used). Since the bitwise XOR operation is negligible, it is neglected. It is well-known that T_{PENC}/T_{PDEC} is much higher than that for T_h, T_{PRNG}, and T_{SENC}/T_{SDEC}. The results reported in Table II depict that computation time of our scheme is less than the scheme of Chen *et al.* [15]. Though our scheme takes more computation time than the schemes of Chien-Chen [27] and Rau-Hsiao [26], it is justified since more functionality features are supported in the proposed scheme as compared to those for their schemes.

TABLE II
COMPUTATION COST: A COMPARATIVE ANALYSIS

Scheme	Computation cost
Chien-Chen [27]	$4T_h + 4T_{PRNG}$
Chen *et al.* [15]	$19T_h + 25T_{PENC}/T_{PDEC}$
Rau-Hsiao [26]	$3T_h + 6T_{PRNG}$
Our	$14T_h + 4T_{SENC}/T_{SDEC}$

B. Communication cost comparison

The comparison of the communication costs among our scheme and other schemes [15], [26], [27] is given in Table III. EPC is of length 96 bits (as shown in Fig. 3). It is known that the security of 160-bit elliptic curve cryptography is equivalent to that for 1024-bit RSA security [49]. We further assume that the random number, timestamp, symmetric encryption/decryption using AES algorithm, hash digest using SHA-1 [50] are 128 bits, 32 bits, 128 bits and 160 bits. The communication costs for the schemes of Chien-Chen [27], Chen *et al.* [15], Rau-Hsiao [26] and our scheme are 640, 12288, 800 and 1216 bits, respectively. The proposed scheme uses two messages in the product authentication & key agreement phase: $MSG_1 = \langle A, C, T_1 \rangle$ and $MSG_2 = \langle D, E, G, SKV, T_2 \rangle$, which take 320 and 672 bits, respectively. In the NFC update phase, the message $MSG_3 = \langle F \rangle$ needs $(\lceil \frac{128+160+32}{128} \rceil \times 128) = 384$ bits. As a result, the total communication cost in our scheme during these phases is $(320 + 672 + 384) = 1376$ bits. The results given in Table III depict that the communication cost of our scheme is less than Chen *et al.*'s scheme [15]. Though our scheme takes more communication time than the schemes of Chien-Chen [27] and Rau-Hsiao [26], it is also justified since more functionality features are supported in the proposed scheme as compared to those for their schemes.

TABLE III
COMMUNICATION COST: A COMPARATIVE ANALYSIS

Scheme	No. of bits	No. of messages
Chien-Chen [27]	640	2
Chen *et al.* [15]	12,288	6
Rau-Hsiao [26]	800	2
Our	1376	3

TABLE IV
FUNCTIONALITY FEATURES: A COMPARATIVE ANALYSIS

Functionality feature	[27]	[15]	[26]	Our
AF_1	×	×	×	✓
AF_2	✓	✓	✓	✓
AF_3	✓	✓	✓	✓
AF_4	×	×	×	✓
AF_5	✓	✓	✓	✓
AF_6	✓	✓	✓	✓
AF_7	×	✓	×	✓
AF_8	×	×	×	✓

Note: AF_1 : strong replay attack protection; AF_2 : man-in-the-middle attack protection; AF_3 : protection against RFID/NFC tag cloning; AF_4 : efficient RFID/NFC update phase; AF_5 : protection against user (MU) impersonation attack; AF_6 : protection against server (AS_j) impersonation attack; AF_7 : session key security; AF_8 : provides security under ROR model.
✓: a scheme is secure or it supports that feature; ×: a scheme is insecure or it does not support that feature.

C. Functionality features comparison

Finally, from Table IV, it is noted that Chien-Chen [27], Chen *et al.* [15] and Rau-Hsiao [26] do not provide protection against strong replay attack. Our schemes uses timestamps along with random nonces at both MU and AS_j. So, our scheme provides protection against strong replay attack. The schemes of Chien *et al.* [27], Chen *et al.* [15] and Rau-Hsiao [26] do not support RFID/NFC update phase, whereas our scheme is capable to update the RFID/NFC after each successful authentication. The schemes of Chien-Chen [27] and Rau-Hsiao [26] do not provide session key security, whereas our scheme provides this feature. All other schemes except our scheme do not provide formal security under the broadly-accepted ROR model. In summary, our scheme provides better security and functionality features as compared to other related existing schemes.

VIII. Practical Perspective: NS2 Simulation Study

In this section, we have simulated the proposed scheme for various network parameters using the broadly-accepted NS2 2.35 simulator [51].

A. Simulation parameters

The proposed scheme is simulated on a Ubuntu 14.04 LTS platform using the NS2 2.35 simulator [51]. Various network parameters used in the simulation are listed in Table V. The network is simulated for 1800 seconds (i.e., 30 minutes). The following network scenarios are considered during the simulation:

- *Scenario 1*: It consists of 10 MUs and 10 AS_js.
- *Scenario 2*: It consists of 20 MUs and 10 AS_js.
- *Scenario 3*: It consists of 30 MUs and 10 AS_js.

In each scenario, we have three product authentication and NFC tag update messages, which are $MSG_1 = \{A, C, T_1\}$ (from MU to AS_j), $MSG_2 = \{D, E, G, SKV, T_2\}$ (from AS_j to MU) and $MSG_3 = \{F\}$ (from AS_j to MU), which are of sizes 320 bits, 672 bits and 384 bits, respectively.

TABLE V
Parameters used in simulation

Parameter	Description
Platform	Ubuntu 14.04 LTS
Tool used	NS2 2.35
Number of AS_j	10 (for scenarios 1, 2, 3)
Number of MU	10 (for Scenario 1)
	20 (for Scenario 2)
	30 (for Scenario 3)
Simulation time	1800 seconds
Initial energy e_i at each AS_j	$500J$

B. Analysis of simulation results

The values of throughput (in bps), energy consumption (mW), packet delivery ratio and load (in bps) are calculated and analyzed during the simulation for all three scenarios.

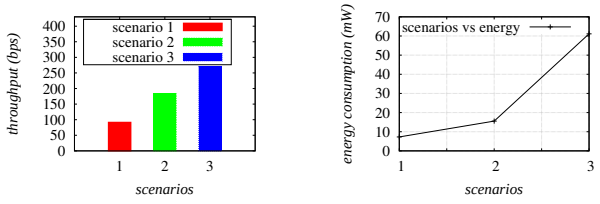

Fig. 6. (a) Throughput (in bps) (b) Energy consumption (mW)

1) Impact on throughput: Throughput is a network parameter which is calculated as the number of bits transmitted per unit time. Thus, throughput can be formulated as $\frac{n_r \times n_{pkt}}{T_d}$, where T_d is total time (in seconds), n_{pkt} the bit size of a packet, and n_r the total number of received packets. Throughput (in bps) of the proposed scheme under different network scenarios is provided in Fig. 6(a). The throughput values are 91.82, 183.38 and 270.40 bps for scenarios 1, 2 and 3, respectively. Throughput increases with increment in number of MUs, because more number of MUs interact with the authentication server. Thus, it further increases the number of exchanged messages, and as a result, throughput becomes high from scenarios 1 to 2, and also from scenarios 2 to 3.

2) Impact on energy consumption: Finally, we have simulated energy consumption (E_{con}) at authentication server AS_j. E_{con} is calculated as $E_{con} = \frac{e_i - e_r}{T_d}$, where T_d is total time (in seconds), e_i is the initial energy and e_r is the remaining energy (in Jules) at S_j. In the proposed scheme, we have calculated the average energy consumption for all authentication servers. E_{con}s (in mW) for different network scenarios are provided in Fig. 6(b). E_{con} values of the proposed scheme are 7.28, 15.56 and 61.13 mW for scenarios 1, 2 and 3, respectively. The energy consumption increases when the number of MUs are increased because more number of MUs interact with the authentication servers. It is expected that the number of exchanged messages is high in scenarios 2 and 3 that further increases the energy consumption from scenarios 1 to 2, and also from scenarios 2 to 3.

3) Impact on packet delivery ratio: Packet delivery ratio (PDR) for a scheme can be calculated as the ratio of the total packets sent to the total packets received. PDRs of the proposed scheme under the considered network scenarios are provided in Fig. 7(a). For scenarios 1, 2 and 3, the PDR values of the proposed scheme are 0.970, 0.968 and 0.953, respectively. Note that PDR decreases with increment in MUs from scenarios 1 to 2, and also from scenarios 2 to 3. As the proposed scheme is lightweight and it uses small packet size, so PDR decrement is less in the scheme.

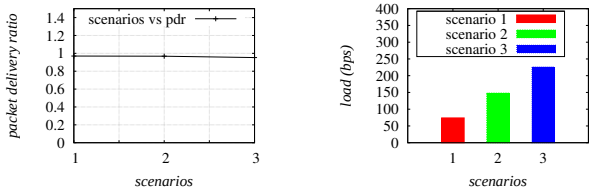

Fig. 7. (a) Throughput (in bps) (b) Energy consumption (mW) (c) Packet delivery ratio

4) Impact on load: In the simulation, we have calculated the load for each authentication server AS_j. The load is calculated as $\frac{(n_s + n_r) \times n_{pkt}}{T_d}$, where T_d is total time (in seconds), n_s are the total packets sent, n_r are the total packets received, and n_{pkt} is the bit size of packet. In the proposed scheme, the average load of the total loads for all authentication servers is calculated. The loads (in bps) for different network scenarios are provided in Fig. 7(b). The load values of the proposed scheme are 74.04, 147.82 and 226.13 bps for scenarios 1, 2 and 3, respectively. The load increases with increment in MUs as more number of MUs interact with the authentication server. It is expected that the number of exchanged messages is high from scenarios 2 and 3, which further increases the load from scenarios 1 to 2 and also from scenarios 2 to 3.

IX. Conclusion

A new authentication scheme for medicine anti-counterfeiting system in IoT environment is put forward for medicine's dosage forms. The proposed scheme is shown to be secure against various known attacks. Furthermore, the formal security verification using the powerful and broadly used AVIPSA tool shows that the proposed scheme is secure. Our scheme is comparable in terms of computation and communication costs, and also provides additional functionality features as compared to other existing schemes. In addition, we have implemented the proposed scheme using the widely-accepted NS2 simulator and the simulation results demonstrate the practicability of the scheme. Overall, better trade-off among security, additional functionality features and efficiency shows that the proposed scheme is appropriate for the anti-counterfeiting of medicine's dosage forms.

Acknowledgments

The authors would like to acknowledge the helpful suggestions of the anonymous reviewers and the Editor. The authors extend their appreciation to the Deanship of Scientific Research at King Saud University for funding this work through Research Group no. RGP-VPP-288.

References

[1] C. Taskforce, "WHO launches taskforce to fight counterfeit drugs," *Bulletin of the World Health Organization*, vol. 84, no. 9, pp. 689–694, 2006.

[2] "Counterfeit drugs raise Africa's temperature," available at http://www.who.int/mediacentre/factsheets/fs275/en/. Accessed on March 2016.

[3] "Substandard, spurious, falsely labelled, falsified and counterfeit (SSFFC) medical products," available at http://www.un.org/africarenewal/magazine/may-2013/counterfeit-drugs-raise-africa's-temperature. Accessed on March 2016.

[4] H. Cheung and S. Choi, "Implementation issues in RFID-based anti-counterfeiting systems," *Computers in Industry*, vol. 62, no. 7, pp. 708–718, 2011.

[5] S. H. Choi and C. H. Poon, "An RFID-based anti-counterfeiting system," *IAENG International Journal of Computer Science*, vol. 35, no. 1, pp. 1–12, 2008.

[6] M. Wang and Z. Yan, "A Survey on Security in D2D Communications," *Mobile Networks and Applications*, vol. 22, no. 2, pp. 195–208, 2017.

[7] A. Bodhani, "New ways to pay [communications near field]," *IET, Engineering & Technology*, vol. 8, no. 7, pp. 32–35, August 2013.

[8] "NFC Tags Explained," available at http://kimtag.com/s/nfc _tags. Accessed on March 2016.

[9] D. He and S. Zeadally, "Authentication protocol for an ambient assisted living system," *IEEE Communications Magazine*, vol. 53, no. 1, pp. 71–77, January 2015.

[10] D. He, S. Zeadally, N. Kumar, and J. H. Lee, "Anonymous Authentication for Wireless Body Area Networks With Provable Security," *IEEE Systems Journal*, 2016, DOI: 10.1109/JSYST.2016.2544805.

[11] D. He, N. Kumar, and N. K. Chilamkurti, "A secure temporal-credential-based mutual authentication and key agreement scheme with pseudo identity for wireless sensor networks," *Information Sciences*, vol. 321, pp. 263–277, 2015.

[12] Z. Yan, W. Feng, and P. Wang, "Anonymous Authentication for Trustworthy Pervasive Social Networking," *IEEE Transactions on Computational Social Systems*, vol. 2, no. 3, pp. 88–98, 2015.

[13] S. Choi, B. Yang, H. Cheung, and Y. Yang, "RFID tag data processing in manufacturing for track-and-trace anti-counterfeiting," *Computers in Industry*, vol. 68, pp. 148 – 161, 2015.

[14] L. Batina, J. Guajardo, T. Kerins, N. Mentens, P. Tuyls, and I. Verbauwhede, "Public-Key Cryptography for RFID-Tags," in *Fifth Annual IEEE International Conference on Pervasive Computing and Communications Workshops*, New York, USA, 2007, pp. 217–222.

[15] C. L. Chen, Y. Y. Chen, T. F. Shih, and T. M. Kuo, "An RFID Authentication and Anti-counterfeit Transaction Protocol," in *International Symposium on Computer, Consumer and Control*, Taichung, Taiwan, 2012, pp. 419–422.

[16] T. Ma, H. Zhang, J. Qian, S. Liu, X. Zhang, and X. Ma, "The Design of Brand Cosmetics Anti-counterfeiting System Based on RFID Technology," in *International Conference on Network and Information Systems for Computers*, Wuhan, China, 2015, pp. 184–189.

[17] T. Staake, F. Thiesse, and E. Fleisch, "Extending the EPC Network: The Potential of RFID in Anti-counterfeiting," in *ACM Symposium on Applied Computing*, Santa Fe, USA, 2005, pp. 1607–1612.

[18] Z. Yan, P. Zhang, and A. V. Vasilakos, "A survey on trust management for Internet of Things," *Journal of Network and Computer Applications*, vol. 42, pp. 120–134, 2014.

[19] "How does RFID system work?" http://www.impinj.com /resources /about-rfid /how-do-rfid-systems-work/. Accessed on February 2016.

[20] F. Resatsch, "Developing and evaluating near field communication applications," in *Ubiquitous Computing*. Springer Gabler Verlag, 2010, ch. 7, pp. XXV–274.

[21] D. Dolev and A. Yao, "On the security of public key protocols," *IEEE Transactions on Information Theory*, vol. 29, no. 2, pp. 198–208, 1983.

[22] M. L. Das, "Two-factor user authentication in wireless sensor networks," *IEEE Transactions on Wireless Communications*, vol. 8, no. 3, pp. 1086–1090, 2009.

[23] J. Kim and H. Kim, "A wireless service for product authentication in mobile RFID environment," in *1st International Symposium on Wireless Pervasive Computing*, Phuket, Thailand, 2006.

[24] J. Kim, D. Choi, I. Kim, and H. Kim, "Product Authentication Service of Consumer's mobile RFID Device," in *10th IEEE International Symposium on Consumer Electronics (ISCE)*, St. Petersburg, USA, 2006, pp. 1–6.

[25] A. B. Jeng, L. C. Chang, and T. E. Wei, "Survey and remedy of the technologies used for RFID tags against counterfeiting," in *International Conference on Machine Learning and Cybernetics*, Baoding, China, 2009, pp. 2975–2981.

[26] C. C. Rau and C. S. Hsiao, "Constructing a security-mechanism RFID system," in *International Conference on Anti-Counterfeiting, Security and Identification*, Taipei, Taiwan, 2012, pp. 1–3.

[27] H.-Y. Chien and C. H. Chen, "Mutual authentication protocol for RFID conforming to EPC Class 1 Generation 2 standards," *Computer Standards & Interfaces*, vol. 29, no. 2, pp. 254 – 259, 2007.

[28] S. Choi, B. Yang, H. Cheung, and Y. Yang, "Data management of RFID-based track-and-trace anti-counterfeiting in apparel supply chain," in *8th International Conference for Internet Technology and Secured Transactions*, London, UK, 2013, pp. 265–269.

[29] E. o. Blass, K. Elkhiyaoui, and R. Molva, "Tracker: security and privacy for RFID-based supply chains," in *18th Annual Network and Distributed System Security Symposium*, San Diego, USA, 2011, pp. 1–20.

[30] D. Zanetti, S. Capkun, and A. Juels, "Tailing RFID Tags for Clone Detection," in *20th Annual Network and Distributed System Security Symposium*, San Diego, USA, 2013.

[31] P. Tuyls and L. Batina, "RFID-Tags for Anti-counterfeiting," in *Topics in Cryptology- CT-RSA*. San Jose, USA: Springer, 2006, pp. 115–131.

[32] V. Odelu, A. K. Das, and A. Goswami, "An efficient ECC-based privacy-preserving client authentication protocol with key agreement using smart card," *Journal of Information Security and Applications*, vol. 21, pp. 1–19, 2015.

[33] P. Sarkar, "A Simple and Generic Construction of Authenticated Encryption with Associated Data," *ACM Transactions on Information and System Security*, vol. 13, no. 4, p. 33, 2010.

[34] D. R. Stinson, "Some Observations on the Theory of Cryptographic Hash Functions," *Designs, Codes and Cryptography*, vol. 38, no. 2, pp. 259–277, 2006.

[35] S. Wu and K. Chen, "An Efficient Key-Management Scheme for Hierarchical Access Control in E-Medicine System," *Journal of Medical Systems*, vol. 36, no. 4, pp. 2325–2337, 2012.

[36] M. Hamze, F. Peyrard, and E. Conchon, "An Improvement of NFC-SEC with Signed Exchanges for an e-Prescription-Based Application," in *Proceedings of 5th International Conference on Mobile Computing, Applications, and Services (MobiCASE 2013)*. Paris, France: Springer International Publishing, 2014, pp. 166–183.

[37] C. Kaufman, P. Hoffman, Y. Nir, and P. Eronen, "Internet Key Exchange Protocol Version 2 (IKEv2)," http://tools.ietf.org/html/rfc5996. Accessed on March 2017.

[38] W. Diffie, P. C. Van Oorschot, and M. J. Wiener, "Authentication and authenticated key exchanges," *Designs, Codes and Cryptography*, vol. 2, no. 2, pp. 107–125, 1992.

[39] X. Li, J.-W. Niu, J. Ma, W.-D. Wang, and C.-L. Liu, "Cryptanalysis and improvement of a biometrics-based remote user authentication scheme using smart cards," *Journal of Network and Computer Applications*, vol. 34, no. 1, pp. 73–79, 2011.
[40] A. K. Das, "Analysis and improvement on an efficient biometric-based remote user authentication scheme using smart cards," *IET Information Security*, vol. 5, no. 3, pp. 145–151, 2011.
[41] M. Abdalla, P. A. Fouque, and D. Pointcheval, "Password-Based Authenticated Key Exchange in the Three-Party Setting," in *8th International Workshop on Theory and Practice in Public Key CryptographyPublic Key Cryptography (PKC 2005)*, ser. Lecture Notes in Computer Science, vol. 3386. Les Diablerets, Switzerland: Springer Berlin Heidelberg, 2005, pp. 65–84.
[42] C. C. Chang and H. D. Le, "A Provably Secure, Efficient, and Flexible Authentication Scheme for Ad hoc Wireless Sensor Networks," *IEEE Transactions on Wireless Communications*, vol. 15, no. 1, pp. 357–366, 2016.
[43] V. Boyko, P. MacKenzie, and S. Patel, "Provably Secure Password-Authenticated Key Exchange Using Diffie-Hellman," in *International Conference on the Theory and Application of Cryptographic Techniques-Advances in Cryptology (EUROCRYPT 2000)*, ser. Lecture Notes in Computer Science. Bruges, Belgium: Springer Berlin Heidelberg, 2000, vol. 1807, pp. 156–171.
[44] AVISPA, "Automated Validation of Internet Security Protocols and Applications," http://www.avispa-project.org/. Accessed on March 2016.
[45] V. Odelu, A. K. Das, and A. Goswami, "A secure biometrics-based multi-server authentication protocol using smart cards," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 9, pp. 1953–1966, 2015.
[46] ——, "SEAP: Secure and efficient authentication protocol for NFC applications using pseudonyms," *IEEE Transactions on Consumer Electronics*, vol. 62, no. 1, pp. 30–38, 2016.
[47] A. K. Das, "A secure and effective biometric-based user authentication scheme for wireless sensor networks using smart card and fuzzy extractor," *International Journal of Communication Systems*, vol. 30, no. 1, pp. 1–25, 2017.
[48] A. Armando et al., "The AVISPA Tool for the Automated Validation of Internet Security Protocols and Applications," in *17th International Conference on Computer Aided Verification (CAV 2005), Lecture Notes in Computer Science (LNCS), Springer-Verlag*, vol. 3576, Edinburgh, Scotland, 2005, pp. 281–285.
[49] S. Vanstone, "Responses to NIST's proposal," *Communications of the ACM*, vol. 35, no. 7, pp. 50–52, 1992.
[50] "Secure Hash Standard," FIPS PUB 180-1, National Institute of Standards and Technology (NIST), U.S. Department of Commerce, April 1995. Available at http://csrc.nist.gov/publications/fips/fips180-4/fips-180-4.pdf. Accessed on March 2016.
[51] "The Network Simulator-ns-2," http://www.isi.edu/nsnam/ns/. Accessed on April 2016.

Mohammad Wazid received the M.Tech. degree in computer network engineering from Graphic Era University, Dehradun, India. He is currently pursuing the Ph.D. degree with IIIT Hyderabad, India. His current research interests include security, remote user authentication, IoT and cloud computing. He has published more than 40 papers in international journals and conferences in the above areas. He was a recipient of the University Gold Medal and the Young Scientist Award by UCOST, Department of Science and Technology, Government of Uttarakhand, India.

Ashok Kumar Das (M'17) received the Ph.D. degree in computer science and engineering, the M.Tech. degree in computer science and data processing, and the M.Sc. degree in mathematics from IIT Kharagpur, India. He is currently an Assistant Professor with the Center for Security, Theory and Algorithmic Research, International Institute of Information Technology, Hyderabad, India. His current research interests include cryptography, wireless sensor network security, security in vehicular ad hoc networks, smart grid, IoT and cloud computing, and remote user authentication. He has authored over 130 papers in international journals and conferences in the above areas. He was a recipient of the Institute Silver Medal from IIT Kharagpur. He is in the editorial board of KSII Transactions on Internet and Information Systems, and the International Journal of Internet Technology and Secured Transactions (Inderscience), and a Guest Editor for the Computers & Electrical Engineering (Elsevier) for the special issue on Big data and IoT in e-healthcare, and has served as a Program Committee Member in many international conferences.

Muhammad Khurram Khan (M'07-SM'12) is currently working as a full professor at the Center of Excellence in Information Assurance, King Saud University, Saudi Arabia. He has edited seven books and proceedings published by Springer-Verlag and IEEE. He has published more than 300 papers in international journals and conferences and he is an inventor of several U.S./PCT patents. Dr. Khan is the Editor-in-Chief of a well-reputed journal 'Telecommunication Systems' (Springer). He is also on the editorial boards of several International journals, including the Journal of Network and Computer Applications (Elsevier), IEEE Communications Magazine and IEEE Access. His current research interests include Cybersecurity, biometrics, multimedia security, and digital authentication. He is a Fellow of the IET (UK), Fellow of the BCS (UK), Fellow of the FTRA (Korea), senior member of the IEEE (USA), a member of the IEEE Technical Committee on Security & Privacy, and a member of the IEEE Cybersecurity community.

Abdulatif Al-Dhawailie Al-Ghaiheb is currently a full professor of Clinical Pharmacy, College of Pharmacy, King Saud University, Saudi Arabia. He received the Ph.D. in the area of Clinical Pharmacy (Pharmacokinetic/dynamic) and M.Sc. in Clinical Pharmacy from the Queen's University of Belfast, Northern Ireland, U.K. His current research interests include information security and cloud computing.

Neeraj Kumar (M'16) received the Ph.D. degree in computer science and engineering from Shri Mata Vaishno Devi University, Katra (J&K), India, in 2009. He was a Post-Doctoral Research Fellow at Coventry University, Coventry, U.K. He is currently an Associate Professor with the Department of Computer Science and Engineering, Thapar University, Patiala, India. He has authored more than 160 technical research papers published in leading journals and conferences from the IEEE, Elsevier, Springer, John Wiley, etc. Some of his research findings are published in top cited journals such as the IEEE Transactions on Industrial Electronics, IEEE Transactions on Dependable and Secure Computing, IEEE Transactions on Intelligent Transportation Systems, IEEE Transactions on Consumer Electronics, IEEE Network, IEEE Communications, IEEE Wireless Communications, IEEE Internet of Things Journal and IEEE Systems Journal. He has guided many research scholars leading to Ph.D. and M.E./M.Tech.

Athanasios V. Vasilakos is recently Professor with the Lulea University of Technology, Sweden. He served or is serving as an Editor for many technical journals, such as the IEEE Transactions on Network and Service management, IEEE Transactions on Cloud Computing, IEEE Transactions on Information Forensics and Security, IEEE Transactions on Cybernetics, IEEE Transactions on Nanobioscience, IEEE Transactions on Information Technology in Biomedicine, IEEE Transactions on Cloud Computing, IEEE Communication Magazine, ACM Transactions on Autonomous and Adaptive Systems, IEEE Journal on Selected Areas in Communications, ACM Transactions on Autonomous and Adaptive Systems, etc. He has published over 500 technical research papers in leading journals and conferences in his areas of research. He is also General Chair of the European Alliances for Innovation (http://www.eai.eu).