IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received April 6, 2020, accepted April 16, 2020, date of publication April 21, 2020, date of current version May 6, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2989305

Lightweight Authentication Protocol for NFC Based Anti-Counterfeiting System in IoT Infrastructure

BANDER A. ALZAHRANI[1], KHALID MAHMOOD[2], AND SARU KUMARI[3]
[1]Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah, Saudi Arabia
[2]Department of Computer Science, COMSATS University Islamabad, Sahiwal Campus, Sahiwal 57000, Pakistan
[3]Department of Mathematics, Chaudhary Charan Singh University, Meerut 250004, India

Corresponding authors: Bander A. Alzahrani (baalzahrani@kau.edu.sa) and Saru Kumari (saryusiirohi@gmail.com)

This project was funded by the Deanship of Scientific Research (DSR) at King Abdulaziz University, Jeddah, under grant No. (D-156-611-1440). The authors, therefore, gratefully acknowledge the DSR technical and financial support.

ABSTRACT Counterfeit medications are known as the medications that were manufactured for the purpose of deceptively representing as authentic, effective and original in the market. Such medications cause severe health issues for patients. Counterfeited drugs have an inimical effect on the human health. The legal manufacturing companies also face threats to their revenue loss due to these counterfeited medicines. In this paper, we introduce a novel authentication protocol for anti-counterfeited drugs systems based on Internet of Things (IoT) to help checking the validity of drugs ''unit dosage''. Our protocol uses the near-field communication (NFC) as it is convenient for mobile environment. The protocol also offers reliable update phase for NFC. Furthermore, our scheme is complemented with performance evaluation along with the use of random oracle model for formal security analysis. We also evaluate our protocol broadly using Py-Charm tool. Results show that proposed protocol resists most of common related flaws almost in equal computing cost with more added security features.

INDEX TERMS Authentication protocols, near-field communication, anti-counterfeiting, counterfeit medicines, radio frequency identification.

I. INTRODUCTION

The broad majority of business extensively utilizes the innovative technology of Internet of Things which is persuading almost every facet of the world. However, the nature of public communication over the Internet makes the objects and devices of IoT vulnerable to numerous cyber-attacks. Moreover, various standard solutions of security developed for enterprise systems are not efficient and implementable to IoT devices. This becomes even more serious in the case of sensitive and critical systems such as anti-counterfeiting which is constructed by the use of IoT infrastructure. As a result, the critical systems of IoT based anti-counterfeiting face various protection and security challenges. Therefore, it is crucial to observe IoT specific security attacks and develop a reliable, scalable, and secure mechanisms of security.

The associate editor coordinating the review of this manuscript and approving it for publication was Weizhi Meng.

Counterfeit medicines are defined by World Health Organization (WHO) as those are fraudulently and deliberately unlabeled with identity [1]–[3]. Various products that are counterfeited, cause problems to various manufacturing companies such as automotive parts, jewelry, cosmetic, software food and beverage etc. Pharmaceutical products have serious threats from it. The counterfeit medicines do not offer any countermeasure to diseases, that is why the people, who use these medicines, suffer a lot. The legal manufacturing organizations are threatened by this problem because it causes loss in their revenue. Worldwide, the annual sale of counterfeit products is estimated as US$ 650 billion by the International Chamber of Commerce of Geneva [4].

WHO also estimated that the utilization of counterfeit products has caused almost 100,000 deaths in Africa in a year. According to the British ''International Policy Network', there were almost 700,000 death cases in a year due to utilization of tuberculosis and malarial medicines. Counterfeiting can happen with local as well as branded products. In some area of Latin America, Africa and Asia, the sale of

counterfeited medicines are more than 30%, as noticed by WHO. It has been also reported that anti-malarial, steroids, hormones, anti-viral, anti-biotic and anti-cancer are general counterfeited medicines [1]–[3].

At the same instant, different organizations of various countries are trying to overcome the problem of counterfeited drugs. According to Xinhua News Agency of China, China is utilizing the technology in which each medicine package that is sealed with anti-counterfeit labels are traced and recognized. The border posts and airports in African countries use hand-held spectrometer, known as Tru-Scan, for the detection of counterfeit drugs with the help of their chemical composition analysis. Counterfeit drugs are also being detected by the simple and free-text message technologies. Companies such as Sproxil and mPedigree Network developed a system in which the labels on medicine packages with an encrypted code is used by the legal medicine manufacturing companies. The label on the drug package is scratched-off by the user who wants to buy that drug and send the code to the company's system which checks the authenticity of medicine packet without any cost. After the verification of medicine packet, the system sends the response message to that user, whether the drug is fake or actual. Therefore, the drug package is known to authentic easily by the customer without any cost. But, the issue is that, this technique needs a lot involvement of user as it is not automated because users are required to remove the label and then to write the code and sending to the system [1]–[3].

Radio Frequency Identification (RFID) allows the identification of different items that use radio waves. A RFID reader usually communicates with RFID tags which have microchips containing the digital information [5]. To prevent counterfeiting, the anti-counterfeiting technology based on RFID has evolved as a powerful tool, because it has generally used anti-counterfeited approach (for example, chemical markers, finger-prints, shifting-inks, and colors). However, the automatic validation of authentic products are not used by these methods.

The technology that enables different devices for communicating directly with each other without any use of central infrastructure networking (i.e. base station and access point) is known as Device-to-Device (D2D) communication [6]. Some common applications of D2D communications depend on Wi-Fi direct, blue-tooth and near field communication. NFC is a high frequency short-range wire-less communication technology, in which NFC enabled devices can communicate with each other up-to 10cm distance. The small amount of data is stored in microchips of NFC tags for transmitting to another NFC supported devices, like mobile devices. The technology of NFC is an enhanced version of the current RFID technology. Such technology provides facility to single device for containing both the interface of a reader and smart card. The data can easily be shared between NFC-based devices [7]–[9].

Recently, numerous authentication schemes have been developed for the networks of wireless sensor and ambient-assisted living system [10]–[17]. A new anonymous authentication scheme is presented by Yan *et al.* [18] in which trust levels and pseudonyms are authenticated in order to provide reliable social networking with secured privacy. Afterwards, various anti-counterfeiting techniques based on RFID have been proposed [5], [19]–[23]. But, the most existed anti-counterfeiting protocols based on RFID are insecure and having various flaws, like main-in-the middle, replay and reader impersonation threats. Some of them do not have sufficient capability for the mobile environment, also do not have adequate RFID changing phase with non user friendly environment. The anti-counterfeiting methods based on NFC are very helpful for mobility environment which have no requirement of card reader as customers just need a mobile device with enabled NFC to interpret the information saved in NFC-tag and transmits to the service provider.

In our protocol, after every successful transaction or process of verification, the NFC tag record is updated in the repository. If there is a number of repositories between the user and the manufacturing company, then at every repository, the transaction of each NFC tag is required to be updated. These records are maintained at distributed database servers. These updated records can be observed by the respective database administration that where, when, and who updates the NFC tag. It also check whether a legal party updates the NFC tag or not.

A new authentication protocol for the system of drug anti-counterfeiting in IoT environment is presented in this paper. Our protocol has the capability for the validation of online drug dosage forms with the help of mobile device. The counterfeiting of drug dosage forms are prevented by the proposed scheme. The protocol offers a secure and robust mechanism of mutual-authentication between the server and NFC tag attached to the form of drug dosage. In the proposed protocol, the NFC operated on mobile devices is used as an interface between the server and the NFC tag that helps in reading the stored information in NFC-tag and transmits this info to the server. Then, drug dosage forms are authenticated by the server and the response message is sent to the user of NFC enabled mobile device. At the end, the customer can easily take his decision after receiving the response from the server whether the drug is able to purchase or not.

Section II explains the underlying system, its workflow and it integration with proposed authentication protocol. Section III exhibits commonly utilized notations and preliminaries. Section IV explains the scheme's related work. Whereas, Section V describes the details of the devised protocol. The rigid security analysis of our proposed protocol is given in Section VI. The performance comparison and analysis of the proposed protocol against related protocols is carried out in Section VII. Section VIII concludes the work with sated remarks.

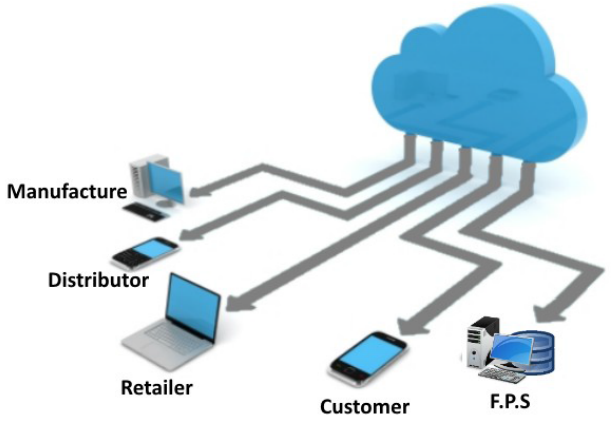

FIGURE 1. Generic architecture of the anti-counterfeiting system.

II. ANTI-COUNTERFEIT SYSTEM

This section presents the underlying system's architecture, its workflow and its integration with a proposed authentication procedure. The details is delineated as follows:

A. SYSTEM ARCHITECTURE AND DESCRIPTION

The interconnection of different objects and devices through the Internet is known as Internet of Things.

The cloud and IoT based systems for anti-counterfeit are realised by developing a portal for anti-counterfeit. Such system design is shown in Fig. 1. The existence of the portal ensures to customers that the drug that they are about to purchase are legitimate and not injurious to health. The system is used by the manufacturers, retailers, distributors, and customers. The interaction and working of these users are elaborated as follows.

1) ADMINISTRATOR

The policies of the mechanism of anti-counterfeit is described by the administrator. The privileges are set by him to get access to the system. The system of code generation is maintained by the administrator and also the web services are provided to end users and clients by only him. The database of user's information and the data which helps to enable the authentication of product, is maintained by the administrator. The description of the product given by the manufacturer are also certified by the administrator so that fake drug products can easily be identified by the customers by scanning the purchased product. Moreover, the service or system updates can be offered by the administrator.

2) MANUFACTURER

The drug products are registered and the related details are entered in database by the web services. The system engenders a particular code for each drug product. Only corresponding manufacturer can access that unique code. That code is printed on related drug item in order to facilitate the authentication of each drug product using database that is maintained on the main server at the manufacturer end.

3) ULTIMATE USERS

Retailers, customers and distributors are assumed as ultimate users and the role of these end users are elaborated as follows:

1) **Retailers and distributors:**
From manufacturers to customers, the process of drug tracking and delivering is the responsibility of retailers and distributors. The received product is authenticated by them and the tracking record of drug products are also updated by them on the database using APP or text message through an Internet browser or mobile device. If the tracking record is maintained at each level, then in the future, it can help to trace that at which level it is counterfeited.
2) **Consumer:**
The originality of drug product using APP or text message can be checked by consumers with the help of computer or mobile. To verify the validity of the drug product by the anti-counterfeit system, the uncommon NFC tag is provided by customers. If the product is successfully authenticated then the condition of status in database is set as sold automatically, in order to prevent counterfeit. So, in this way, they can claim for the counterfeited product, if the status is already set to sold or authentication of product is not valid. Furthermore, the product feedback can be directly provided by the consumer to the manufacturer.

B. ANTI-COUNTERFEIT SYSTEM WORKFLOW

The working of the system of anti-counterfeit is described as follows:

Anti-counterfeit portal helps the end users such as distributors, retailers and consumers to check the authenticity of the drug packet through computer or mobile device. The status of the product with particular tag can be verified by the customers. If the product with particular tag is not already sold then the customer is intimated through message that the product is genuine. This successful verification proceed and the product purchase status is set to sold with the that particular tag. However, if the sold status is already found set then customer is immediately intimated that the product you are going to purchase is fake or tempered. Instantly an alert message is also sent towards the manufacturer about this event. The authentication process is facilitated by a unique NFC tag which is placed on each product. These properties help the customers to check whether the status of the product is set as sold in early or not. If the status is set earlier then obviously the drug product is counterfeited so in this way the system gives the warning to the manufacturer and the user. The information about the original product in the system must have to be maintained by manufacturer, so that the authentication is facilitated. Then the system engenders a unique NFC for each item. The specific database of concerned system is used to keep the product related information. There are two important function in anti-counterfeiting (1) Authentication

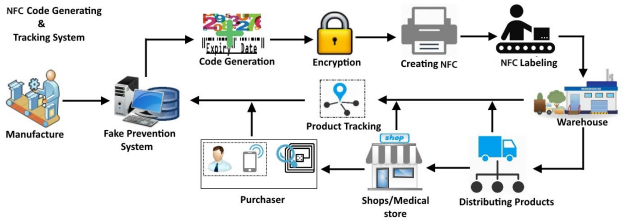

FIGURE 2. Architecture of tracking and code generation.

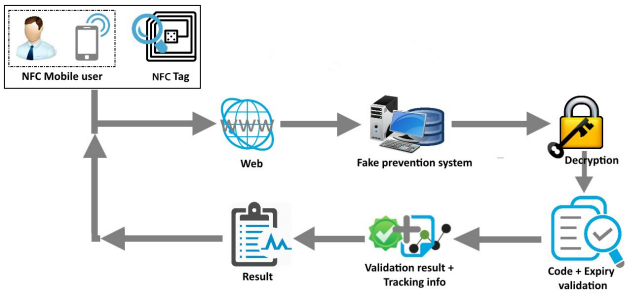

FIGURE 3. Authentication procedure.

method (2) NFC code tracking and generation. These functions are described as follows:

1) TRACKING AND CODE GENERATION OF NFC

The blueprint of NFC tracking and code generation is given in Fig. 2, with the following details:

Step 1: The anti-counterfeiting web services is accessed by manufacturers for their product registration by giving the relevant information. After providing the information, the approval request is sent to administrator to ensure the product registration.

Step 2: The received information upon approval request, is verified by the administration in order to register the products. Then, a request to system of code generation is sent after successful verification, otherwise manufacturer approval request is canceled.

Step 3: A unique code is generated by the system for each product item according to some standard algorithm of code generation. This manufacturer is notified by this engendered code and the database is also updated with this code. The product is assigned as a sold status which remains unset until the item is sold.

2) CODE GENERATION

There are various methods for code generation [24] discussed in the literature for preventing the medicine from counterfeiting. Basically, generated codes are used to check the legitimacy of medicine. The mechanism of code generation must be economical, fast and reliable. These codes should be easy for layman to check and robust enough to counterfeit. It is hard to design a perfect mechanism for code generation with all these discussed properties [25]. It is stated by the Food and Drug Administration (FDA) that almost all mechanisms for anti-counterfeiting are susceptible [26]. Here, a modified mechanism for code generation is described on the basis on the mechanism described in [27]. The next subsection is the brief description of the introduced code generation method.

3) ALPHANUMERIC TOKEN (AT)

Following are the entities involved in AT:

1) Product IDs: A unique identity is designated to each item which is tagged on its packing. Each layer of packing has different length of code. Secondary packing is tagged with 4 characters, 2 letters with 2 digits. 3 characters are assigned to tertiary packing in which first is a letter and remaining 2 are digit. 6 characters are contained by primary packing, where first 3 are literals and remaining 3 are numeric values.
2) Secure database: The unique IDs of product is maintained by utilizing secure database.
3) Mobile application: Mobile application facilitates the ultimate users (retailers, distributors or consumer) in order to check the originality of drug.
4) Users participation: The mobile application also facilitates the users to give direct response to manufacturer.

4) PSEUDO RANDOM SELECTION RULES OF PRODUCT ID

- There should be unique ID of product within packing of tertiary layer. Same IDs can be of different cottons.
- ID should not be a predictable serial number but should be pseudo arbitrary.
- Each packing ID should be followed by specific format.
- The possible number of IDs should be 1500 times more than the item which is hold by tertiary container.

C. AUTHENTICATION PROCEDURE

The authentication procedure shown in Fig. 3 allows retailers, distributors and consumers to validate the legitimacy of specific product and the product tracking record can also be updated by retailers and distributors. Following is the briefly description of this procedure.

Step 1: When the anti-counterfeit system is accessed with the help of computer or mobile device by the end users then this procedure launches.

Step 2: The product NFC is provided by the end users. This NFC is decrypted by the system of anti-counterfeit.

Step 3: The information about expiry date and specific code of the product is recovered and authenticated after decrypting the NFC.

Step 4: The results can be recovered and viewed by the end users with the help of specific product code.

Step 5: At the last step of authentication method, the ultimate user is checked by the system, then the sold status of product is checked by the system if he is customer.

Step 6: The product item is set as sold status after authenticating the product successfully in order to identify the same product whether it is counterfeit or original.

Step 7: The product track record is updated by the system, if distributors and retailers are the end users. And in this case the sold status of product is not set by the system.

III. PRELIMINARIES

The hash functions, elliptic curve cryptography, and adversarial model that are used in this paper are described in this section.

A. HASH FUNCTIONS

By taking an input string $O = H(String)$ of random size, a fixed size output is generated by hash. Generated output is called hash code. Any change in the value of string can cause a huge difference. A secure one way hash operation has following specification:

- If the string is described, it is effortless to obtain $O = H(String)$.
- If $O = H(String)$ is described, it is impossible to find out the string.
- It is mundane task to distinguish input of $String_1$ and $String_2$ so that $H(String_1) = H(String_2)$. This property is called collision resistance.

1) DEFINITION 1 (CHARACTERISTICS OF COLLISION RESISTANCE)

Secure hash function H(.) is predetermined for collision resistance. The possibility that an attacker $\mathcal{A}_{Adv}$ can find a pair $(String_1 \neq String_2)$ as $H(String_1) = H(String_2)$ is separated as $Adv^{HASH}_{\mathcal{A}_{Adv}}(t) = Prb[(String_1, String_2) \Leftarrow_r \mathcal{A}_{Adv} : (String_1 \neq String_2), H(String_1) = H(String_2)]$, where attacker is allowed to select a pair $(String_1, String_2)$ randomly. Attacker's pair is calculated against the randomly selections taken up with-in polynomial time (t). The resistance of collision conclude that $Adv^{HASH}_{\mathcal{A}_{Adv}}(t) \leq \in$, whereas $\in > 0$, is an enough tiny value.

B. ELLIPTIC CURVE Cryptography(ECC)

The Elliptic curve equation is defined in the form $E_p(e, f)$: $c^2 = d^3 + ed + f$ over a prime finite field $(d, c) \in W_P^* \times W_P, e, f$ and $4e^3 + 27f^2 \neq 0$ (mod P). Where P is a selected huge prime number, the size of P is ≥ 160 bits. Scalar product is gained by repeated addition e.g. $nt = t + t + t + \cdots + t(ntimes)$, over a determined t a point on $E_P(e, f)$ and the multiplier n. The variables (e, f, t, P, n) should be a part of limited field F_P. E is supposed to be the abelian group. Whereas O, is stated as the ID's infinity point.

1) DEFINITION 2 (LOGARITHMIC ISSUES IN ECDLP)

ECDLP: is given two specified points over $R, V \in E_P(e, f)$, calculate n a scalar so that $R = nV$. The chances that $\mathcal{A}_{Adv}$ can determine n in polynomial time(T) are described as $Adv^{ECDLP}_X(T) = prb[(X(R, V) = x : xx \in W_P)]$. ECDLP assumption concludes that $\mathcal{A}^{ECDLP}_{Adv_x}(T) \leq \in$.

C. THREAT MODEL

The familiar attacker model is deliberated in this article, as declared in [28] and [29]. Where the following considerations are followed as per the expertise of the attacker $\mathcal{A}_{Adv}$:

1) $\mathcal{A}_{Adv}$ has full control over the open communication channel. $\mathcal{A}_{Adv}$ is adept to eliminate, amend, rerun, interrupt or can transmit a new replicated message.
2) The confidential information saved in the smart card can be excerpted by $\mathcal{A}_{Adv}$, by doing power analysis.
3) $\mathcal{A}_{Adv}$ can be a deceitful or intruder user or service provider of the system.
4) The identities of registered servers and users are not secret but familiar to insiders.
5) The attack on server cannot be launched by $\mathcal{A}_{Adv}$ because the server is assumed to be secured.

IV. RELATED WORK

Chio *et al.* [5] presents an anti-counterfeiting method for products tracing & tracking and also studies numerous related RFID based anti-counterfeiting systems. The customer can authenticate the originality of the products which he selects to buy the products by the contributed system.

Kim *et al.* [30] presents an application level system for anti-counterfeiting, which engages a RFID reader accessible to a customer's device and ensures originality of products. Kim *et al.'s* [31] proposed system is utilized to trace and track a product for entire life cycle using RFID tags, which authenticates product packages. This system utilizes location information system and on the basis of obtained information, can take right decision about the authenticity of product.

Public key cryptography can be utilized in the systems of anti-counterfeiting for product authenticity but key factor is its implementation in RFID tags. Batina *et al.* [20] studies Public-key cryptography anti-counterfeiting system for implementation feasibility. Jang *et al.* provides survey on methods used in this system and to make RFID tags also discuss in this survey. Furthermore, this survey provides research direction in anti-counterfeiting systems.

Chen *et al.* [21] introduces anti-counterfeiting secure transaction protocol, which able to do online authentication. This protocol uses one-way hash function, public key cryptographic functions, signature creation, and verification. Conversely, this protocol has some security boundaries, such as it does not offer RFID tag cloning and strong replay attacks protection.

Anti-counterfeiting protocol is presented by Rau and Hsiao [32] in which a new RFID approach is used to prevent different flaws, for example counterfeit, replay and forward key security attack. Conversely, this protocol has some security boundaries, such as it does not offer RFID-tag replication and strong replay attacks protection. Also, session key security is not provided by this protocol. Blass *et al.* [33] and Zanetti *et al.* [34] introduced a protocol, which allows object Authenticity in supply chains based

TABLE 1. Notations used in this article.

Notations	Description
$\mathcal{MU}_u$	Mobile user of the System
$\mathcal{S}_{Auth}$	Authentication server
$\mathcal{NFC}$	Nearest frequency code
$\mathcal{EPC}$	Electronic product code
P_{pub}	Public key
x	Secrete key of server
a_1	Arbitrary nonce generated by MU_u
a_2	Arbitrary number engendered by S_{auth}
SK	Shared Session key
$\oplus$	XoR operator
$h(.)$	One-way operation of hashing

on RFID. In [34], replication of tag is observed from a central detector. Tuyls *et al.* [35] reviews the methods that define the replication of RFID-tags, which is also used in anti-counterfeiting applications.

V. PROPOSED SCHEME

This section discusses the proposed scheme for anti-counterfeiting which consists of two stages: Registration, Login and Authentication stages. Each stage is described below in detail and as demonstrated in Fig. 4.

A. REGISTRATION STAGE

In order to register a product, the manufacturer sends $\mathcal{EPC}$ to the server $\mathcal{S}_{Auth}$ and performs the following subsequent steps:

REG 1: The manufacturer generates $\mathcal{EPC}$ and sends it to the server S_{Auth} through private channel.

REG 2: After getting the information, the server calculates $\mathcal{NFC}$ in which private key of the server is concatenated with $\mathcal{EPC}$ and a one-way hash function is applied on it.

$$\mathcal{NFC} = h_1(x, \mathcal{EPC})P \tag{1}$$

REG 3: At the end the server S_{Auth} stores $\{\mathcal{NFC}, \mathcal{EPC}, Flag = 0\}$ to his database, and sends the $\mathcal{NFC}$ back to the manufacturer to engraved on the tag.

B. LOGIN AND AUTHENTICATION STAGE

Once the $\mathcal{EPC}$ of product is registered to the server $\mathcal{S}_{Auth}$ successfully, $\mathcal{NFC}$ is generated and provided to the manufacturer. Now the user $\mathcal{U}_p$ can scan it by $\mathcal{NFC}$ scanners to get the detail about the product by follows:

Step AP1: Firstly mobile user scans $\mathcal{NFC}$ and selects the random number a_1 to calculate the following:

$$B_1 = a_1 P, \quad \overline{B_1} = a_1 P_{pub} \tag{2}$$

$$DID_u = \mathcal{EPC} \oplus h_2(B_1, \overline{B_1}) \tag{3}$$

$$A_u = h_3(\mathcal{EPC}, B_1, \overline{B_1}, \mathcal{NFC}) \tag{4}$$

and send the request message $\{DID_u, B_1, A_u\}$ to the server.

Step AP2: On obtaining the request message $\{DID_u, B_1, A_u\}$ from $\mathcal{MU}_u$, the server calculates the following:

$$\overline{B_1} = xB_1 \tag{5}$$

$$\acute{\mathcal{EPC}} = DID_u \oplus h_2(B_1, \overline{B_2}) \tag{6}$$

After the calculation of $\mathcal{EPC}$ server set flag to 1. Moreover server extract flag from *DB* by corresponding $\mathcal{EPC}$. If the extracted flag is equal to 1, the session is aborted, otherwise the flag is updated to 1 in *DB*.

Step AP3: Using the server's private key x the server $\mathcal{S}_{Auth}$ computes:

$$\overline{\mathcal{NFC}} = h_1(x, \mathcal{EPC})P \tag{7}$$

$$A_u = h_3(\acute{\mathcal{EPC}}, B_1, \acute{\overline{B_1}}, \acute{\mathcal{NFC}}) \tag{8}$$

and checks $\acute{A_u} \stackrel{?}{=} A_u$. If it does not match, the session is aborted. Otherwise server engenders an arbitrary nonce a_2 and compute the following:

$$B_2 = a_2 P, \quad \overline{B_2} = a_2 B_1 \tag{9}$$

$$KS_{cs} = a_2 \overline{B_1} \tag{10}$$

$$SK_{cs} = h_5(KS_{cs}, \acute{\overline{B_1}}, B_2) \tag{11}$$

$$AS_{cs} = h_6(\acute{\mathcal{NFC}}, \acute{\overline{B_1}}, B_2, \overline{B_2}) \tag{12}$$

Step AP4: Later, the server sends the challenge message $\{B_2, \overline{B_2}, AS_{cs}\}$ and checks $\acute{AS_{cs}} \stackrel{?}{=} h_6(\mathcal{NFC}, \overline{B_1}, B_2, \overline{B_2})$. If not equal session is aborted, otherwise calculate:

$$KU_u = a_1 \overline{B_2} \tag{13}$$

$$SK_u = h_5(KU_u, \overline{B_1}, B_2) \tag{14}$$

Step AP5: Finally both the $\mathcal{MU}_u$ and the server $\mathcal{S}_{Auth}$ agrees on a shared common session key $\acute{SK} = SK$.

VI. SECURITY ANALYSIS

A. INFORMAL SECURITY ANALYSIS

A complete informal security analysis for Anti-Counterfeiting protocol is described in this section. The following are the major features that the proposed protocol provides and also the major attacks that are prevented by the scheme.

1) MUTUAL AUTHENTICATION

Whenever the mobile user scans $\mathcal{NFC}$ tag for session initiation it sends the request message $\{DID_u, B_1, A_u\}$ to server. On receiving the requested message the server calculates the incoming literals and calculates the reliability of $\mathcal{EPC}$

$$\acute{A_u} = h_3(\mathcal{EPC}, B_1, \acute{\overline{B1}}, \acute{\mathcal{NFC}})$$

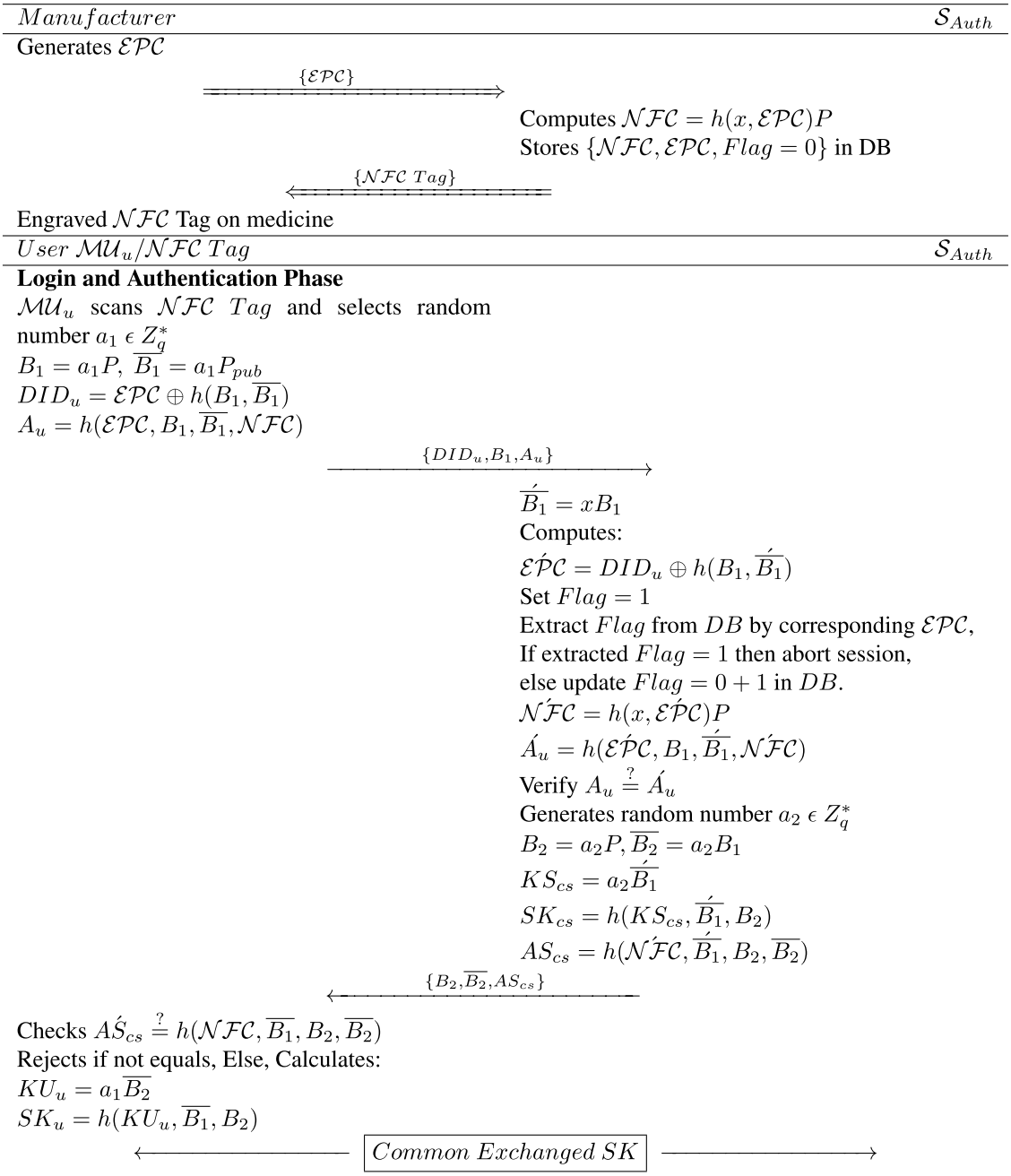

FIGURE 4. The anti-counterfeiting proposed scheme.

Similarly, the server is authenticated by the mobile user by verifying

$$\acute{AS}_{cs} = h_6(\mathcal{NFC}, \overline{B_1}, B_{2,}, \overline{B_2})$$

Where NFC involves the server private key which can only be computed by the legitimate server. So our scheme offers robust mutual authentication.

2) SERVER IMPERSONATION

Adversary cannot impersonate as a legitimate server because the calculation of $\mathcal{NFC}$ involves the server private key. So only the legitimate server can calculate the value of $\mathcal{NFC}$

$$\mathcal{NFC} = h(x, \mathcal{EPC})P$$

Moreover, the calculation of $\mathcal{S}_{Auth}$ signature AS_{cs} also involve $\mathcal{NFC}$

$$AS_{cs} = h(\mathcal{NFC}, \overline{\acute{B_1}}, B_2, \overline{B_2})$$

So the $\mathcal{NFC}$ value can only be calculated by legitimate server. Therefore our scheme resists server impersonation attack.

3) MAN-IN-THE-MIDDLE

Assume that if the attacker $\mathcal{A}_{Adv}$ intercepts the login request information $\{DID_u, B_1, A_u\}$, but the requested message can not be changed by him because the DID_u that is transmitted through the public communication channel is different for each session. Moreover, A_u has $\mathcal{EPC}$ concatenated with $\mathcal{NFC}$ and B_1. $A_u = h_3(\mathcal{EPC}, B_1, \overline{B1}, \mathcal{NFC})$ and for $\mathcal{NFC}$ server private key is required. So, our devised scheme has a robust ability to resist man-in-the-middle attack.

4) REPLAY ATTACK

For each session random variable are generated by both $\mathcal{MU}_u$ and $\mathcal{S}_{Auth}$ if the adversary intercepts the request message, he can not reply it later, because for each session the challenge message against requested message contains different values.

5) PERFECT FORWARD SECRECY

The session key computed by S_{Auth} includes $\overline{\acute{B_1}}$ and B_2 which are user's $\mathcal{MU}_u$ specific & $\mathcal{S}_{Auth}$ specific arbitrary nonce from both sides, respectively. Thus, if $\mathcal{A}_{Adv}$ obtains long term secrete key of any participant, still he will not be able to get the previous session key. Hence the our introduced scheme offers perfect forward secrecy.

6) NO CLOCK SYNCHRONIZATION

Time Stamp is not used in the introduced scheme, instead a random number from each side for each session is generated. So no clock Synchronization is required.

B. FORMAL SECURITY ANALYSIS

For analysis purpose, the following oracles are defined in order to show that the proposed protocol withstands all the major attacks by adversary.

- ***Reveal:*** The oracle yields a string S is output from one way hash function $U = h(S)$
- ***Extract:*** The oracle yields the scalar multiplier X out of a given elliptic curve points $O = XP$ and P.

Theorem 1: The proposed Protocol is unassailable and withstand $\mathcal{A}$ for secrecy of $\mathcal{MU}_u$'s, the server's private key (x) and SK between $\mathcal{MU}_u$ & S_{Auth} under the strict $ECDLP$ supposition and contemplate the protected one-way hash functions as random oracle model.

Proof 1: Let $\mathcal{A}_{Adv}$ with the potential to determine $\mathcal{MU}_u$'s of the system, S_{Auth}'s private key x and SK session key. To achieve such purpose $\mathcal{A}_{Adv}$ implements the algorithmic experiment $EXPE1^{HASH,ECDLP}_{\mathcal{A}_{Adv},PRUAS}$ against the introduced protocol $PRUAS$ by implementing both the $Extract$ and the random oracles $Reveal$. The probability of the experiment is described as $Success_1 = |Prb[EXPR1^{HASH,ECDLP}_{\mathcal{A}_{Adv},PRUAS} = 1] - 1|$. The benefit carried by $\mathcal{A}_{Adv}$ is defined as $Advt1^{HASH,ECDLP}_{\mathcal{A}_{Adv},TFBAMS}(t_e, q_{ext}, q_{rev}) = max_{\mathcal{A}_{Adv}}(Succe_1)$. Where $\mathcal{A}_{Adv}$ can utilize utmost q_{ext} and q_{rev} queries. The experiment indicates that $\mathcal{A}_{Adv}$ can only compute x and SK if and only if $\mathcal{A}_{Adv}$ can (i)reverse secure hash function and (2) find out the ECDLP. However, according to Def III-A.1, it is practically impossible to reverse one-way hash functions, also by Def III-B.1, it is practically infeasible to compute ECDLP. However, we have $Advt1^{ECDLP,HASH}_{\mathcal{A}_{Adv},PRUAS}(t, q_{rv}, q_{ex}) \leq \epsilon$. Therefore, the introduced protocol is withstand an attacker $\mathcal{A}_{Adv}$ to compute $\mathcal{MU}_u$'s of the system, S_{Auth} the server's secret key x and the session key SK.

Algorithm 1 $EXPR1^{ECDLP,HASH}_{\mathcal{A},PRUAS}$

1: Intercept the login request $\{DID_u, B_1, A_u\}$, as $DID_u = \mathcal{EPC} \oplus h(B_1, \overline{B_1})$, $B_1 = a_1P, A_u = h(\mathcal{EPC}, B_1, \overline{B_1}, \mathcal{NFC})$
2: **if** $(\overline{B_1} = xB_1)$ **then**
3: Call *Reveal* oracle on $\mathcal{E\acute{P}C}$ and get $(DID_u \oplus h(B_1, \overline{B_2})) \leftarrow Reveal(\mathcal{EPC})$
4: Set Flag = 1
5: Extract Flag from DB by corresponding $\mathcal{EPC}$
6: **if** Flag = 0 **then**
7: Update the Flag = 0 + 1 in DB
8: Call *Extract* oracle on $\mathcal{NFC}$ to get $h(x, \mathcal{E\acute{P}C})P \leftarrow Extract(\mathcal{N\acute{F}C})$
9: Call *Reveal* oracle on A_u and get $h(\mathcal{E\acute{P}C}, B_1, \overline{B_1}, \mathcal{N\acute{F}C}) \leftarrow Reveal(\acute{A_u})$
10: Verify $(A_u = \acute{A_u})$
11: Compute $KS_{cs} = a_2\overline{B_1}$
12: Compute $SK_{cs} = h(KS_{cs}, \overline{\acute{B_1}}, B_2)$
13: Compute $AS_{cs} = h(\mathcal{N\acute{F}C}, \overline{\acute{B_1}}, B_2, \overline{B_2})$
14: Eavesdrop the response message $(B_2, \overline{B_2}, AS_{cs})$, where $B_2 = a_2P, \overline{B_2} = a_2B_1$
15: Checks $AS_{cs} = h(\mathcal{NFC}, \overline{B_1}, B_2, \overline{B_2})$
16: **if** Equals **then**
17: Compute session key $SK_u = h(KU_u, \overline{B_1}, B_2)$
18: **else**
19: **return** Fail
20: **end if**
21: **else**
22: **return** Fail
23: **end if**
24: **else**
25: **return** Fail
26: **end if**

VII. PERFORMANCE EVALUATION

The comparison between our protocol and various relevant existing schemes [21], [32], [36], [37] in terms of the computation and communication cost of login and authentication

TABLE 2. Comparison of the computation cost.

Protocols	Computation Cost
Ours	$9T_{h(.)} + 8T_{pm} = 0.00007012$ ms
[37]	$14T_{h(.)} + 4T_{senc/sdec} = 0.00251212$ ms
[36]	$4T_{h(.)} + 4T_{PRNG} = 0.00005604$ ms
[32]	$3T_{h(.)} + 6T_{PRNG} = 0.00004206$ ms
[21]	$19T_{h(.)} + 25T_{aenc/adec} = 0.000341$ ms

stage is discussed in this section. The security features of the introduced protocol and existing related schemes have been compared. As the registration phase is considered one time process, it is not covered in this evaluation. The NFC update phase has been used in the performance evaluation of existing schemes, but instead of updating NFC we have used flag value that automatically updates when a product is get purchased. The usage of the flag makes our scheme cost effective as compared to related schemes as shown in Table 2.

A. COMPARISON OF THE COMPUTATION COST

The analysis of computation cost between the proposed and existing schemes [21], [32], [36], [37] is shown in the Table 2. We have considered the following notations that have been used in both the proposed and existing schemes.

- T_{pm}: indicates the running time for the point multiplication
- T_h: indicates the running time for the hash function
- $T_{\oplus}$: shows the running time of the XoR operation
- $T_{\|}$: shows the running time of the concatenation operation
- T_{PRNG}: represents the running time for the pseudo random number generator
- $T_{senc/sdec}$: specifies the time required for the execution of symmetric encryption/decryption
- $T_{aenc/adec}$: refers to the time required for the execution of asymmetric encryption/decryption

The operations ($T_{h(.)}$, $T_{\oplus}$, $T_{\|}$, T_{pm}, T_{PRNG}, $T_{senc/sdec}$, $T_{aenc/adec}$) of the devised and existing protocols have been performed on two different systems with different specifications. The functions that have been utilized on the MU_u / *NFC* Tag side have been implemented using PyCrypto library inside a ubunto 19.04 with 2.60 GHZ processing power and 8 GB RAM on core i5 with the help of Python programming language. The operations ($T_{h(.)}$, T_{pm}, T_{PRNG}) takes 0.000000028, 0.0000000033 and 0.000000047 ms respectively as an execution time. However, the functions that have been utilized on the S_{auth} side are implemented utilizing PyCrypto library inside an ubunto 19.04, with 16 GB RAM and 3.60 GHZ processing power on core i7 with the help of Python programming language. The operations ($T_{h(.)}$, T_{pm}, T_{PRNG}, $T_{senc/sdec}$, $T_{aenc/adec}$) used at S_{auth} side takes 0.000014, 0.00000000095, 0.000000018, 0.000000047, 0.00060 and 0.00007012 ms respectively as an execution/running time. The cryptographic operations ($T_{\|}$ and $T_{\oplus}$) take a insignificant amount of time which as result have been ignored and not included in the calculation of overall computation cost.

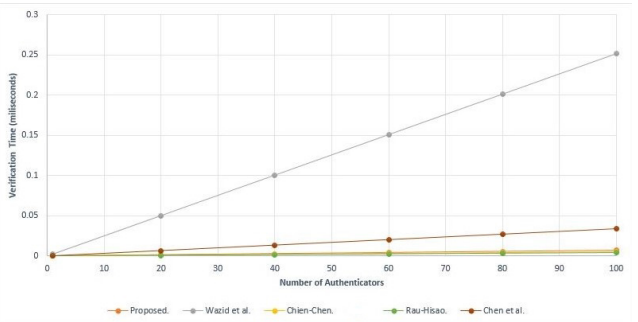

FIGURE 5. Analysis of the computation cost between the devised and the other relevant protocols.

TABLE 3. The comparison of communication overhead.

Protocols	Communication cost	No. of transmitted messages
Ours	960	2
[37]	1376	3
[36]	640	2
[32]	800	2
[21]	12288	6

The comparison of the total computation cost between our devised and the related protocols is displayed in the Fig. 5. The list of all protocols is shown horizontally in the graph and execution time (in ms) of the computation cost is shown vertically. It can be seen that the computation cost of our protocol is far less than most of the existing protocols.

B. COMPARISON OF COMMUNICATION OVERHEAD

The comparison of the number of transmitted messages and communication overhead of our proposed protocol with related schemes [21], [32], [36], [37] is shown in Table 3. The length of *EPC* consists on 96 bits while the large prime number P that is used for the point multiplication consists on 160 bits. Furthermore, the length of randomly generated numbers, timestamps, symmetric encryption/decryption using AES algorithm and the hash function are 128, 32, 128 and 160 bits respectively. Table 3 shows that the required number of communication bits for the proposed scheme are less than the required bits of [21] and [37] while little bit higher than [32] and [36].

Figure 6 shows the communication cost comparison between our protocol and related ones. All the protocols are shown on X axis of the graph, while communication bits are shown vertically. It can noticed that our protocol takes few number of bits as compared to some of the existing protocols, which is evident to the efficiency of our protocol.

C. COMPARISON OF THE SECURITY FEATURES

The proposed scheme have aided security and functionality features as it provides resistance against User impersonation, Server impersonation, Replay and Man-In-Middle attacks.

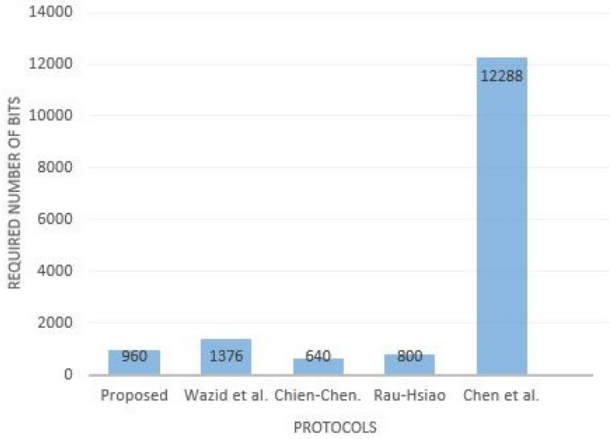

FIGURE 6. Comparison of the communication overhead between the introduced and various existing protocols.

TABLE 4. Comparative analysis of the security features.

Protocols→ Security features↓	[21]	[32]	[36]	[37]	Ours
$SF1$	✓	✓	✓	✓	✓
$SF2$	✗	✗	✗	✗	✓
$SF3$	✓	✓	✓	✓	✓
$SF4$	✗	✗	✗	✗	✓
$SF5$	✓	✓	✓	✓	✓
$SF6$	✗	✗	✗	✗	✓
$SF7$	✗	✗	✗	✗	✓

Furthermore, the proposed scheme provides perfect forward secrecy. As no time stamp is used, there is no clock synchronization in the proposed scheme. Table 4 shows the comparative analysis of security features among the proposed and related protocols [21], [32], [36], [37]. Table 4 indicates that the related protocols are insecure against some attacks, while the proposed protocol is secure against major security attacks.

where the features: $SF1$: resistance against user impersonation MU_u attack; $SF2$: provision of mutual authentication; $SF3$: resistance against server impersonation S_{auth} attack; $SF4$: replay attack protection; $SF5$: Man-In-Middle attack resilience; $SF6$: provision of perfect forward secrecy; $SF7$: no clock synchronization.
✓: indicates that a scheme is secure against that feature; ✗: indicates that a protocol is insecure or does not provide against that feature.

At the end, after considering Table 2, 3 and 4 it can be said that our proposed protocol takes far less computation and communication cost compared to many of the existing protocols. The proposed protocol also provides aided security features that existing protocols do not offer.

VIII. CONCLUSION

We introduced a novel authentication protocol for anti-counterfeited drugs systems based on Internet of Things. The scheme helps to check the validity of the drugs. It has been demonstrated that our proposed protocol is able to resist all the known attacks while preserving the novel approaches and functionalities. Furthermore, the security analysis shows that proposed protocol offers a better security and thus protect against most common attacks. The analysis of performance evaluation and formal security indicates that our protocol is also comparably better in term of computation cost and communication overhead. Additionally, the protocol has been evaluated using Py-Charm tool. In general, proposed scheme can be considered suitable for the anti-counterfeited medicines for added security features it provides.

ACKNOWLEDGMENT

This project was funded by the Deanship of Scientific Research (DSR) at King Abdulaziz University, Jeddah, under grant No. (D-156-611-1440). The authors, therefore, gratefully acknowledge the DSR technical and financial support.

REFERENCES

[1] W. Burns, "WHO launches taskforce to fight counterfeit drugs," in *Bulletin of the World Health Organization*, vol. 84. 2006, pp. 689–690.
[2] J. Sambira, "Counterfeit drugs raise Africa's temperature," *Afr. Renewal*, vol. 27, no. 1, pp. 5–7, May 2013.
[3] *Substandard, Spurious, Falsely Labelled, Falsified and Counterfeit (SSFFC) Medical Products*, WHO, Geneva, Switzerland, 2016.
[4] H. H. Cheung and S. H. Choi, "Implementation issues in RFID-based anti-counterfeiting systems," *Comput. Ind.*, vol. 62, no. 7, pp. 708–718, Sep. 2011.
[5] S. Choi and C. Poon, "An RFID-based Anti-counterfeiting System," *IAENG Int. J. Comput. Sci.*, vol. 35, no. 1, pp. 1–12, 2008.
[6] M. Wang and Z. Yan, "A survey on security in D2D communications," *Mobile Netw. Appl.*, vol. 22, no. 2, pp. 195–208, Apr. 2017.
[7] A. Bodhani, "New ways to pay," *Eng. Technol.*, vol. 8, no. 7, pp. 32–35, Aug. 2013.
[8] N. M. Smith and C. Cahill, "Continuous multi-factor authentication," U.S. Patent 9 705 869, Jul. 11, 2017.
[9] Q. Z. Sheng, S. Zeadally, A. Mitrokotsa, and Z. Maamar, "RFID technology, systems, and applications," *J. Netw. Comput. Appl.*, vol. 34, no. 3, pp. 797–798, 2011.
[10] D. He and S. Zeadally, "Authentication protocol for an ambient assisted living system," *IEEE Commun. Mag.*, vol. 53, no. 1, pp. 71–77, Jan. 2015.
[11] D. He, S. Zeadally, N. Kumar, and J.-H. Lee, "Anonymous authentication for wireless body area networks with provable security," *IEEE Syst. J.*, vol. 11, no. 4, pp. 2590–2601, Dec. 2017.
[12] D. He, N. Kumar, and N. Chilamkurti, "A secure temporal-credential-based mutual authentication and key agreement scheme with pseudo identity for wireless sensor networks," *Inf. Sci.*, vol. 321, pp. 263–277, Nov. 2015.
[13] X. Li, J. Niu, S. Kumari, F. Wu, A. K. Sangaiah, and K.-K.-R. Choo, "A three-factor anonymous authentication scheme for wireless sensor networks in Internet of Things environments," *J. Netw. Comput. Appl.*, vol. 103, pp. 194–204, Feb. 2018.
[14] F. Wu, L. Xu, S. Kumari, X. Li, J. Shen, K.-K.-R. Choo, M. Wazid, and A. K. Das, "An efficient authentication and key agreement scheme for multi-gateway wireless sensor networks in IoT deployment," *J. Netw. Comput. Appl.*, vol. 89, pp. 72–85, Jul. 2017.
[15] J. Li, W. Zhang, V. Dabra, K.-K.-R. Choo, S. Kumari, and D. Hogrefe, "AEP-PPA: An anonymous, efficient and provably-secure privacy-preserving authentication protocol for mobile services in smart cities," *J. Netw. Comput. Appl.*, vol. 134, pp. 52–61, May 2019.
[16] S. Kumari, P. Chaudhary, C.-M. Chen, and M. K. Khan, "Questioning key compromise attack on Ostad-Sharif et al.'s authentication and session key generation scheme for healthcare applications," *IEEE Access*, vol. 7, pp. 39717–39720, 2019.
[17] J. H. Kong, L.-M. Ang, and K. P. Seng, "A comprehensive survey of modern symmetric cryptographic solutions for resource constrained environments," *J. Netw. Comput. Appl.*, vol. 49, pp. 15–50, Mar. 2015.

[18] Z. Yan, W. Feng, and P. Wang, "Anonymous authentication for trustworthy pervasive social networking," *IEEE Trans. Comput. Social Syst.*, vol. 2, no. 3, pp. 88–98, Sep. 2015.
[19] S. H. Choi, B. Yang, H. H. Cheung, and Y. X. Yang, "RFID tag data processing in manufacturing for track-and-trace anti-counterfeiting," *Comput. Ind.*, vol. 68, pp. 148–161, Apr. 2015.
[20] L. Batina, J. Guajardo, T. Kerins, N. Mentens, P. Tuyls, and I. Verbauwhede, "Public-key cryptography for RFID-tags," in *Proc. 5th Annu. IEEE Int. Conf. Pervas. Comput. Commun. Workshops (PerComW)*, Mar. 2007, pp. 217–222.
[21] C.-L. Chen, Y.-Y. Chen, T.-F. Shih, and T.-M. Kuo, "An RFID authentication and anti-counterfeit transaction protocol," in *Proc. Int. Symp. Comput., Consum. Control*, Jun. 2012, pp. 419–422.
[22] 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 *Proc. Int. Conf. Netw. Inf. Syst. Comput.*, Jan. 2015, pp. 184–189.
[23] T. Staake, F. Thiesse, and E. Fleisch, "Extending the EPC network: The potential of RFID in anti-counterfeiting," in *Proc. ACM Symp. Appl. Comput.*, 2005, pp. 1607–1612.
[24] A. Sinha, "Systems engineering perspective of e-pedigree systems," Ph.D. dissertation, MIT Sloan School Manage. Eng. Syst. Division, Massachusetts Inst. Technol., Cambridge, MA, USA, 2009.
[25] R. G. Johnston and A. R. Garcia, "An annotated taxonomy of tag and seal vulnerabilities," *J. Nucl. Mater. Manage.*, vol. 28, no. 3, pp. 23–30, 2000.
[26] T. Lancet, "Combating counterfeit drugs," *Lancet*, vol. 371, no. 9624, p. 1551, May 2008.
[27] R. G. Johnston, "An anticounterfeiting strategy using numeric tokens," *Int. J. Pharmaceutical Med.*, vol. 19, no. 3, pp. 163–171, 2005.
[28] D. Wang, D. He, P. Wang, and C.-H. Chu, "Anonymous two-factor authentication in distributed systems: Certain goals are beyond attainment," *IEEE Trans. Dependable Secure Comput.*, vol. 12, no. 4, pp. 428–442, Jul. 2015.
[29] D. Wang and P. Wang, "Two birds with one stone: Two-factor authentication with security beyond conventional bound," *IEEE Trans. Dependable Secure Comput.*, vol. 15, no. 4, pp. 708–722, Jul./Aug. 2016.
[30] J. Kim and H. Kim, "A wireless service for product authentication in mobile RFID environment," in *Proc. 1st Int. Symp. Wireless Pervas. Comput.*, Jan. 2006, p. 5.
[31] J. Kim, D. Choi, I. Kim, and H. Kim, "Product authentication service of Consumer's mobile RFID device," in *Proc. IEEE Int. Symp. Consum. Electron.*, Jun./Jul. 2007, pp. 1–6.
[32] C.-C. Rau and C.-S. Hsiao, "Constructing a security-mechanism RFID system," in *Proc. Anti-Counterfeiting, Secur., Identificat.*, Aug. 2012, pp. 1–3.
[33] E.-O. Blass, K. Elkhiyaoui, R. Molva, and E. S. Antipolis, "Tracker: Security and privacy for RFID-based supply chains," in *Proc. NDSS 18th Annu. Netw. Distrib. Syst. Secur. Symp.*, Feb. 2011.
[34] D. Zanetti, S. Capkun, and A. Juels, "Tailing RFID tags for clone detection," in *Proc NDSS*, 2013, pp. 1–17.
[35] P. Tuyls and L. Batina, "RFID-tags for anti-counterfeiting," in *Cryptographers' Track RSA Conf.* Springer, 2006, pp. 115–131.
[36] H.-Y. Chien and C.-H. Chen, "Mutual authentication protocol for RFID conforming to EPC class 1 generation 2 standards," *Comput. Standards Interfaces*, vol. 29, no. 2, pp. 254–259, Feb. 2007.
[37] M. Wazid, A. K. Das, M. K. Khan, A. A.-D. Al-Ghaiheb, N. Kumar, and A. V. Vasilakos, "Secure authentication scheme for medicine anti-counterfeiting system in IoT environment," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1634–1646, Oct. 2017.

BANDER A. ALZAHRANI received the M.Sc. degree in computer security and the Ph.D. degree in computer science from Essex University, U.K., in 2010 and 2015, respectively. He is currently an Assistant Professor with King Abdulaziz University, Saudi Arabia. He has published more than 27 research articles in international journals and conferences. His current research interests include wireless sensor networks, information centric networks, Bloom filter data structure and its applications, secure content routing, and authentication protocols in the IoT.

KHALID MAHMOOD received the M.S. degree in computer science from Riphah International University, Islamabad, Pakistan, in 2010, and the Ph.D. degree in computer science from International Islamic University, Islamabad, Pakistan, in 2018. His Ph.D. dissertation is secure authenticated key agreement schemes for smart grid communication in power sector. He is currently with COMSATS University Islamabad, Sahiwal Campus. His research interests include lightweight cryptography, smart grid authentication, authenticated key agreement schemes, and the design and development of lightweight authentication protocols using lightweight cryptographic solutions for diverse infrastructures or systems like vehicular ad hoc networks, smart grid, and Telecare medical information system (TMIS).

SARU KUMARI received the Ph.D. degree in mathematics from Chaudhary Charan Singh University, Meerut, India, in 2012. She is currently an Assistant Professor with the Department of Mathematics, Chaudhary Charan Singh University. She has published more than 133 research articles in reputed international journals and conferences, including 115 publications in SCI-indexed journals. Her current research interests include information security and applied cryptography. She is a Technical Program Committee Member of many international conferences. She is on the Editorial Board of more than 12 journals of international repute including seven SCI journals. She served as the Lead/Guest Editor for four Special Issues in SCI journals of Elsevier, Springer, and Wiley.