Noori et al. EURASIP Journal on Information Security (2020) 2020:13
https://doi.org/10.1186/s13635-020-00114-x

EURASIP Journal on Information Security

RESEARCH Open Access

Scalable, efficient, and secure RFID with elliptic curve cryptosystem for Internet of Things in healthcare environment

Davood Noori[1], Hassan Shakeri[2*] and Masood Niazi Torshiz[2]

Abstract

The rapid development of IoT technology has led to the usage of various devices in our daily life. Along with the ever-increasing rise of the Internet of Things, the use of appropriate methods for establishing secure communications in health care systems is vital. The adoption of high-security optimal mechanisms for this purpose has been more effective regarding the efficiency of medical information systems; hence, many studies are being conducted in this field today. One of the most important components is the RFID cards that can be used for communication between entities in the environment. In healthcare systems, patient information is critical and nobody should have access to this information. Thus, providing security for these networks is essential. Recently, good researches have been done in the area of authentication for medical information systems, using RFID technology, which has a low computational cost. In this paper, we propose a novel method based on elliptic curve cryptography for vital and efficient and scalable authentication between RFID cards, card readers, and servers. This proposed method maintains security and has less computational cost and low elliptic curve point multiplication running time compared to similar recent methods.

Keywords: Elliptic curve cryptography (ECC), Internet of Things (IoT), RFID, Healthcare, Authentication, Key management

1 Introduction

The term "Internet of Things" was first introduced in 1999 [1]. The Internet of Things refers to the precise communication between the physical and digital world [2, 3]. In fact, it provides an extensive infrastructure for providing advanced services, such as sending and receiving information and interconnections using physical and virtual elements [3]. The Internet of Things consists of a set of sensors and radio frequency identification (RFID) technology that communicate through the network with various devices [2]. Technologies such as sensor technology, embedded smart technology, and nanotechnology as well as RFID technology can be widely used in the Internet of Things. In RFID technology, objects can communicate with one another through radio waves and exchange information among themselves [3, 4]. Some advantages of RFID technology in comparison with traditional barcodes are the ability to read and write, lack of direct exposure to the card-reader, simultaneous reading of multiple cards, and non-restrictions of using different barcodes [3, 5]. Considering the above-mentioned reasons, we can use these benefits for health care systems such as hospitals.

The components of RFID technology include servers, card readers, and cards. The cards include various parts including a chip that performs calculations, a memory for data storage, an antenna for transmitting and receiving data, and a special hardware that is used for encryption and decryption operations [6–8].

* Correspondence: shakeri@mshdiau.ac.ir
[2]Department of Computer Engineering, Mashhad Branch, Islamic Azad University, Mashhad, Iran
Full list of author information is available at the end of the article

Cards can communicate with the card reader and transfer encrypted data between themselves. The cards themselves are divided into three categories, including a reactive card that gets the energy necessary to transmit its data through a wireless signal, a semi-active card with a small battery, and the active card that has a radio antenna and a small battery that is directly connected to the card reader [8, 9]. The cards can store and process data and then transfer information to the card reader using their radio transmitter [6, 7].

Card readers have a control unit, a memory unit, and a radio transmitter and receiver; in addition, the capacity of computations in card readers is more than cards, and its main function is to create authentication and exchange messages between the card and the server [8, 10].

A server is a trusted entity and stores all information and ID cards and card readers in its database for proper authentication process, and then the system starts up. The validity of the card can be determined using this information stored in the server [8, 10].

One of the instances that can be implemented by using RFID technology inside the Internet of Things and in healthcare settings is the identification of the newborn and patient [8, 11], tracing and validating the medical treatment of patients [8, 12], patient location and patient management in healthcare centers [8, 13], surgery process management [8, 14], equipment location tracking [5, 8, 15], blood pack tracing, monitoring, and pharmaceutical management.

All messages in healthcare environments are transmitted by using wireless waves through RFID cards in the latter environment. With rapid development and advances of RFID technology in healthcare environments, the need for safe and secure access to sensitive information should be considered, and ultimately, the exchange of this information should be taken into account through the Internet infrastructure of the objects more than before [8]. Transferring information by using RFID technology does not provide any security by itself. Therefore, these healthcare systems are vulnerable to attacks due to the use of RFID. In order to remove these vulnerabilities, various security protocols are provided for secure communication within these networks, some of which are based on symmetric cryptography [16–25], and others are based on asymmetric cryptography [3, 7, 26–28]. Some of these protocols deal with the authentication between the card and the server, in which they confirm each other [3, 7, 26–28] and others have authentication between the card and the reader [16, 17]. In order to ensure that the connection between the card, the card reader, and the server is secure, we need mutual authentication in RFID systems, which will affect the authentication process against various attacks [8].

In this paper, we propose a novel method based on elliptic curve cryptography for vital and efficient and scalable authentication between RFID cards, card readers, and servers. This proposed method maintains security and has less computational cost and low elliptic curve point multiplication running time compared to similar recent methods.

An elliptic curve over $GF(2^m)$ consists of all points $(x, y \in GF(2^m))$ such that it satisfies an elliptic curve equation: $E: y^2 + xy = x^3 + ax^2 + b$ with $a, b \in GF(2^m)$, $b \neq 0$ (let $GF(2^m)$ be a finite field of 2^m elements, where m is an integer). For cryptographic purpose, those over the finite field of F_p and $F2^m$ are most suitable [29].

The addition of two points and doubling a point on an elliptic curve (generally over a set of real numbers) in a geometrical space are illustrated in Figs. 1 and 2. The Group Law is supported by following terms [29]:

- Identity: $P + O = O + P = P$ for all $P = (x, y) \in E$.
- Negativity: Let $P = (x, y) \in E$ and $Q = (x, x + y) \in E$ therefore $P + Q = O$, that is to say, negative of P is Q.
- Point addition: If $P = (x_1, y_1) \in E$ and $Q = (x_2, y_2) \in E$ such that $P \neq \pm Q$, then $P + Q = (x_3, y_3)$ is calculated by following equation:

$$x_3 = \lambda^2 + \lambda + x_1 + x_2 + a, y_3 = \lambda(x_1 + x_3) + x_3 + y_1, \text{with} \lambda = \frac{y_2 + y_2}{x_2 + x_2}$$

- Point doubling: If $P = (x_1, y_1) \in E$ and $P \neq -P$, then $2P = (x_2, y_2)$ is defined by following equation:

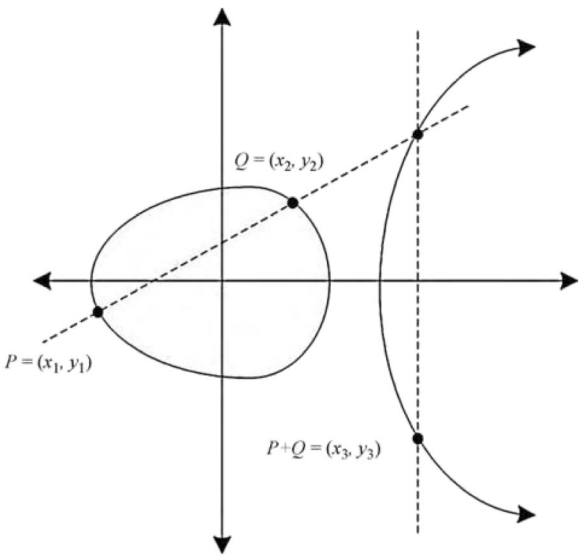

Fig. 1 Addition on elliptic curves

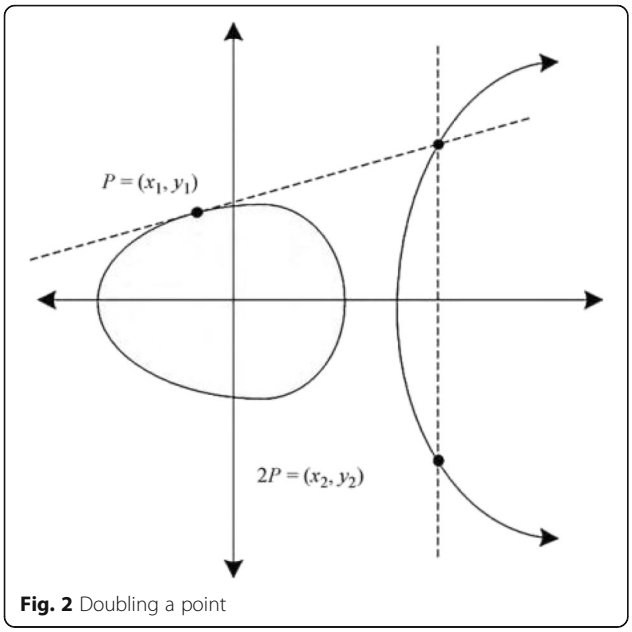

Fig. 2 Doubling a point

$x_2 = \lambda^2 + \lambda + a$, $y_2 = \lambda(x_1 + x_2) + x_2 + y_1$, with $\lambda = x_1 + \frac{y_1}{x_1}$

Scalar multiplication as a fundamental operation in ECC is obtained by performing the elliptic curve addition operation k times: $Q = kP = \underbrace{P + P \ldots + P}_{k}$.

Calculating Q is relatively easy when k and P are given, but it is a hard problem to determine k when Q and P are specified. This problem is called the elliptic curve discrete logarithm problem (ECDLP). Thus, the scalar multiplication on elliptic curves over finite fields is considered as a one-way function which is useful in cryptographic applications [30].

The structure of the paper is organized as follows: Section 2 reviews the related papers; Section 3 describes the proposed solution, including the initializing phase and the authentication phase; Section 4 describes the dynamic key management; in Section 5, the analysis of the proposed solution as well as security and its efficiency has been addressed; and finally, the conclusions are presented in Section 6.

2 Methods and related work

Due to the sensitive information that can be exchanged with RFID technology, security for these networks is critical. RFID technology is one of the most important steps in establishing secure communication in these networks. However, the messages exchanged between the card, the card reader, and the server have always been exposed to a variety of security attacks. In this paper, we use the elliptic curve cryptography to secure the connection between the card and reader. The proposed solution preserves security and computational costs less than the previous methods. Furthermore, key management solutions are presented for dynamic access problems in RFID cards in order to be able to develop scalability healthcare networks

Various research and articles have been conducted for RFID security in a variety of applications, which, in addition to providing effective security schemes, identify and discuss the following security issues [3, 7, 10, 16, 18, 25–28, 31–39]:

2.1 Mutual authentication

In most researches, interconnection between the card, the card reader, and the server is required prior to the initialization of the operation. The relationship between the card and the card reader is insecure and needs to be reciprocally authenticated, while the communication channel between the server and card reader is assumed to be secure.

2.2 Confidentiality

Each secret key of the card, the card reader, or their ID must not be recovered by attackers. If the attacker accesses the card or card reader's secret key, he/she can introduce his/her card or card reader to the server and access sensitive information of the network. To prevent this, data must be encrypted before being transmitted between the card and the card reader.

2.3 Anonymity

An RFID authentication scheme is necessary for anonymity of the card and card reader. If the attacker recognizes the identity of the card or card reader, he can in fact violate their privacy; in order to prevent this issue, the ID of the card and card reader should be encrypted in a mutual authentication process.

2.4 Availability

The RFID authentication process should be implemented accurately over the available lifetime of the card or the card reader. To provide anonymity, for most RFID authentication schemes, the secret keys between the card and the card reader should be updated during the implementation of the authentication process. If the attacker in any way eliminates the process of updating secret keys between the card and the card reader, the authentication scheme will be invalid.

2.5 Forward security

In many authentication schemes, if an attacker can access the secret key, he can get the old location of the card or access the old information of that card, which will result in the violation of the privacy of the owner of

the card. It is therefore necessary to have the forward-looking security within the authentication plan.

2.6 Scalability

An authentication scheme should be able to support the number of cards or card readers in the network. For example, if the number of cards has multiplied or the card has been deleted, added, or its location has changed, or even the location of the card reader has changed, the authentication scheme should be able to maintain and continue to work well and correctly manage the key for the steps listed.

2.7 Resists various attacks

A strong authentication scheme should be able to secure the exchange of information between the card and the card reader against multiple attacks, such as man-in-the-middle attack, replay attack, forging attack, internal attacks, and external attacks.

Various methods are used for the authentication problem in healthcare and health systems based on the Internet of Things that use symmetric and asymmetric cryptography (elliptical curve cryptography) [7, 25, 31, 40–42]. The authors of papers did not use asymmetric cryptographic methods, because the key length is long in asymmetric cryptography and thus the speed is very low, but the implemented elliptical curve cryptography methods [43, 44] have proven less storage space than the SHA3 hashing algorithms [7]. Using elliptic curve cryptography, we can easily expand our network and do not have a scalability problem while being safe against various attacks. In contrast, symmetric encryption always suffers from scalability problem [32, 33, 45–50].

The elliptic curve ciphering identification for RFID technology was presented for the first time in 2006, by Batina and Tuyls [51], and then, various methods were presented by different authors, or the vulnerability of these methods was investigated by other researchers or new protocols have been introduced to improve their cost and security. For example, in Lee's paper [52], works of Batina and Tuyls [51] and Batina et al. [53] were investigated, and the problem of the unidentified card was addressed.

Another article by Zhang and Qi [26] has addressed the problems in Chou's work [34], namely availability of the information inside the card by the attacker, interacting with the server, and card tracking, and aimed to improve Chou's authentication method. A recent paper by Farash et al. [7] has recently been presented in the field of RFID technology using elliptic curve cryptography for health care systems, in which, by reviewing the methods proposed by Zhang and Qi [26] and Zhao [3], first, addresses the security problem of these two methods in insecure sending of the information, and then presents his own security method. Another paper proposed by Yang et al. [10] addresses the problems of the Kaur [54] scheme, being a high computational cost; with changes made to the Kaur scheme, he has presented a new scheme reducing the high cost of computation.

3 Proposed scheme

In our proposed method, the server, the card reader, and the card are all participating; first, the server generates the keys for both the card reader and the card. Then, the server loads the keys on them.

The proposed method has two phases: (1) initializing phase and (2) authentication phase. The details of these two phases are fully described below. The symbols are listed in Table 1.

3.1 Initializing phase

This phase includes the following steps:

Step 1: The server selects the size and type of the Galois field *GF(q)* which can be chosen $p = q$, where p must be a large prime number or $q=2^m$ (this field is usually chosen because the calculations on the $GF(2^m)$ field can be done quickly, and a fast and efficient algorithm has been provided for required calculations on $GF(2^m)$ field); m represents the size of the field.
Step 2: The server uses two parameters $a,b \in F_q$ in order to define the elliptic curve equation E on the field F_q shown in (1):

$$y^2 + xy = x^3 + ax^2 + b \tag{1}$$

Then, the server chooses the basic point (G) for the elliptic curve (basic point means the point on the elliptic curve that has the highest n order) that is $nG = O$.

Table 1 Definition of notations used in the proposed scheme

Notation	Definition
GF(p)	Galois field
E	Elliptic curve defined by the equation
N	Elliptic curve order
G	Elliptic curve base point
a,b	Co-factors of elliptic curve equation "part of the ECC common parameters"
Pr_i	Private key
Pu_i	Public key
$P_{r_i}^{-1}$	Reverse private key
h	Hash function

Step 3: For each card T_i, the server inserts a random integer p_{r_i} from the interval [1, n − 1] as the private key and then calculates and inserts $p_{u_i} = p_{r_i}G$ into the card. Also, the inverted private key p_{ri}^{-1} is inserted into the card. Then, this procedure is repeated for each card reader.

Note: Given the discrete logarithm for the elliptic curve, having p_{u_i} and G, calculation of p_{r_i} is complicated in practice.

Step 4: The server has a one-way hashing function $h(x)$ for converting a point on the elliptic curve E to a number v, where chooses $v \in F_q$.
Step 5: The server selects a random integer l_i from the range [1, n − 1] for each card and then calculates the U_i according to (2).

$$U_i = l_i G \tag{2}$$

Therefore, the secret key for each card is obtained from Eq. (3).

$$SK_i = h(U_i) \tag{3}$$

Step 6: The server specifies the public dots for the reader, as in Eq. (4), in which the parameter j represents the card reader.

$$M_{i,\ j} = l_j\ (p_{U_i}), M_{j,\ i} = l_i\left(p_{U_j}\right) \tag{4}$$

In the end, the server stores the parameters E_q, G, n, h, p_{ri}^{-1}, p_{U_i}, p_{r_i} and l_i for the card and the parameters E_q, G, n, h, p_{rj}^{-1}, p_{U_j}, p_{r_j} and $M_{i,\ j} = l_j\ (p_{U_i})$, $M_{j,\ i} = l_i(p_{U_j})$ for the card reader.

3.2 Authentication phase

In this phase, the card and card reader authenticate each other using the secret key. This phase includes the following steps:

Step 1: To calculate U_j, each card reader is to get its public points and inverted private key already loaded by the server at the initial phase, then U_j is calculated by Eq. (5):

$$U_j = l_j G = p_{rj}^{-1} M_{i,\ j} \tag{5}$$

It should be noted that p_{rj}^{-1} denotes inversion in a finite field, which is an operation required in the digital signature algorithm of the elliptic curve [55].

Step 2: Determining the secret key according to Eq. (6):

$$SK_j = h(U_j) \tag{6}$$

Step 3: In this step, we obtain the value of w according to Eq. (7):

$$w = h(SK_j + SK_j) \tag{7}$$

w is used for two-way authentication. The card reader calculates the value of w, which is hashing of the sum of values SK_j and SK_j. It is used in the symmetric encryption procedure that encrypts the message (m) if the card is able to calculate the value of w, then is able to authenticate the card reader.

In fact, when the card reader communicates with the cards, it can authenticate them, and it is enough to calculate the secret key for the card; also, the card must calculate the value of w in order to authenticate the card reader. The authentication phase is shown in Fig. 3:

For example, Fig. 4 illustrates a cluster with card reader and cards with a certain relationship. In this figure, there are 7 cards and one card reader. There is a bidirectional relationship between each card and card reader, and only the card reader is able to calculate the secret key for the cluster members. The server determines the public parameters $M_{i,\ j}$ and $M_{j,\ i}$ and declares them to the card reader. The set of required public parameters for deriving the secret key by card reader is shown as follows:

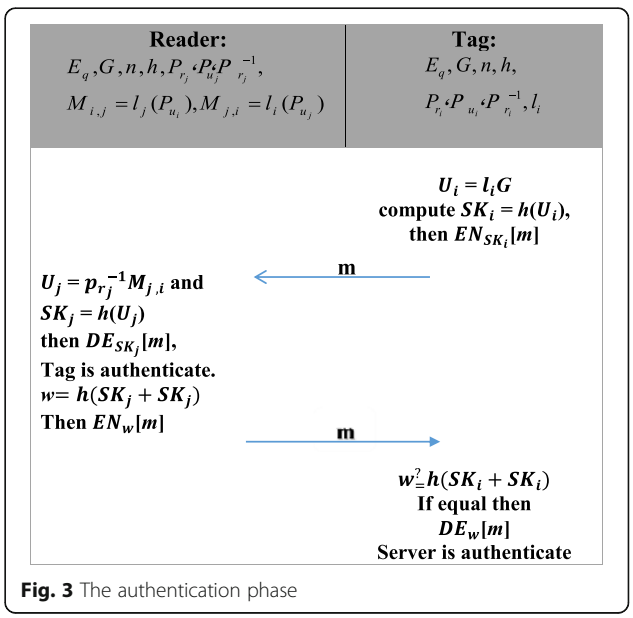

Fig. 3 The authentication phase

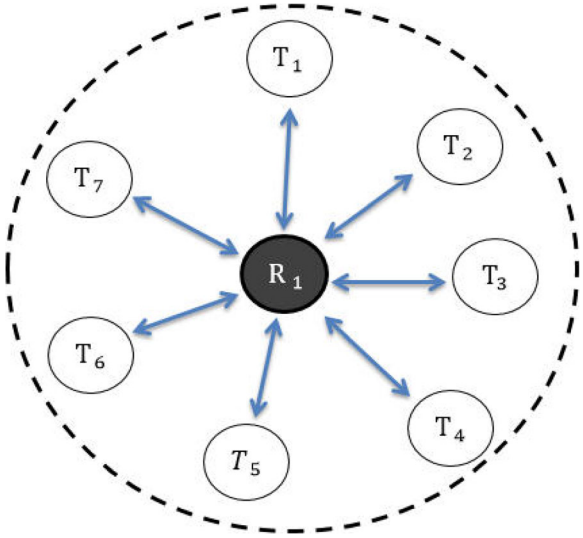

Fig. 4 Communication between cluster members and card reader

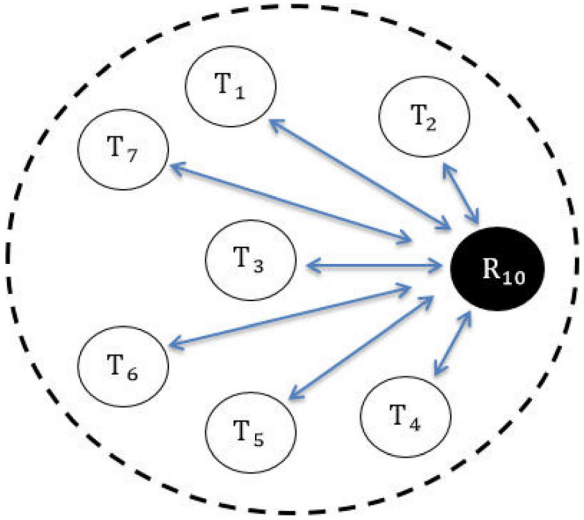

Fig. 5 Switch card reader and communication between cluster members and new card reader

$$\begin{aligned}\text{Reader} : \{&M_{1,1} = l_1(P_{u_1}), M_{1,2} = l_2(P_{u_1}), M_{1,3} \\ &= l_3(P_{u_1}), M_{1,4} = l_4(P_{u_1}), M_{1,5} = l_5(P_{u_1}), M_{1,6} \\ &= l_6(P_{u_1}), M_{1,7} = l_7(P_{u_1}), M_{1,8} = l_8(P_{u_1})\}\end{aligned}$$

Therefore, the card reader in addition to its secret key can derive secret keys of cluster members as follows:

$$\begin{aligned}\text{Reader} = h(U_1) &= h\left(P_{r_1}^{-1} M_{1,1}\right) \\ = h(U_2) &= h\left(P_{r_1}^{-1} M_{1,2}\right) \\ = h(U_3) &= h\left(P_{r_1}^{-1} M_{1,3}\right) \\ = h(U_4) &= h\left(P_{r_1}^{-1} M_{1,4}\right) \\ = h(U_5) &= h\left(P_{r_1}^{-1} M_{1,5}\right) \\ = h(U_6) &= h\left(P_{r_1}^{-1} M_{1,6}\right) \\ = h(U_7) &= h\left(P_{r_1}^{-1} M_{1,7}\right) \\ = h(U_8) &= h\left(P_{r_1}^{-1} M_{1,8}\right)\end{aligned}$$

Note that no card or card reader can operate autonomously unless it has permission from the server, in which case it must receive the required public points from the server.

4 Solution to key management of dynamic access problems

In this section, the concept and problems of dynamic key management for RFID technology in healthcare environments such as adding a new card, removing an existing card, revoking an existing relationship and creating a new relationship (switch card reader), and changing secret keys will be discussed.

4.1 Adding new card

Imagine that a new card T_x is added to Fig. 4. In this case, the private, public keys, and reverse private key will be embedded within new card by the server, then steps 5 to 6 of initializing phase will repeat, and the type of relationship between the card and card reader will be a bi-directional one like the other cards. The details are as follows:

Step 1: Select a random integer P_{r_x} from the interval [1, n − 1] as a secret parameter for each new card T_x by the server; then, the point $P_{u_x} = P_{r_x}G$ is computed as a public parameter, and both of them are embedded in the new card. Moreover, the reverse private key $P_{r_x}^{-1}$ is embedded within the new card too.
Step 2: The server selects a random integer l_x for the new card from interval [1, n − 1]. Thus, the secret key of the card T_x is $SK_x = h(U_x) = h(l_xG)$
Step 3: The server determines the points $M_{i,\ x} = l_x(P_{u_i})$ and $M_{x,\ x} = l_x(P_{u_x})$ to communicate between the card reader and the new card and declares it publicly.

4.2 Removing the existing card

Imagine there is a need for a card to be removed from Fig. 4 for any reason, like the case when cards are captured by an attacker. Under this condition, the server should remove all parameters in contact with the card mentioned above and revoke the access to the card too. In addition, the secret key of the card reader must be changed as follows:

Step 1: The server reselects a random integer l_x^* from the interval [1, n − 1] for card reader. As a result, the new secret key of the card reader is $SK_x^* = h(U_x)$.

4.3 Revoking an existing relationship and creating a new relationship (switch card reader)

Imagine that a new card reader is selected for cluster members (cards), and the previous card reader continues to carry out tasks in another cluster (as shown in Fig. 5).

Then, all communications which the card reader has with cards must be removed. Furthermore, all public parameters and those which connect the cluster members to the card reader and vice versa should also are removed. To build communication between the cluster members and the new card reader, steps 5 to 6 of initializing phase should be executed as follows:

Step 1: The server selects a random integer l_i from interval [1, n − 1] for each card. Therefore, the secret key for each the card is $SK_i = h(U_i) = h(l_i G)$.
Step 2: The server determines the points $M_{j,\ j} = l_j(P_{u_j})$ and $M_{i,\ j} = l_j(P_{u_i})$ for communication between the new card reader and each single card, and declares it publicly.

4.4 Changing secret keys

Sometimes changing a secret key is felt necessary perhaps to ensure higher network security and efficiency. Changing the secret key of a card T_x from SK_x to SK_x^* follows the below procedure:

Step 1: The server selects a random integer l_x^* from interval [1, n − 1]. Therefore, the new secret key of the card T_x is $SK_x^* = h(l_x^* G)$
Step 2: The server determines the points $M_{x,\ \mathrm{x}} = l_x^*$ (P_{u_x}) and $M_{i,\ \mathrm{x}} = l_x^*$ (P_{u_i}) declares it publicly.

Table 3 Definition of some notations used in performance evaluation of the proposed scheme

Notation	Definition
T_H	**Hash computation time**
T_E	**Elliptic curve polynomial computation time**
T_{PA}	**Elliptic curve point addition computation time**
T_{PM}	**Elliptic curve point multiplication computation time**
T_{PR}	**Private key computation time**
T_{PU}	**Public key computation time**

Note: We should be aware that the hash computation cost (T_H) is much less than the private and public keys computation costs (T_{PU} and T_{PR})

5 Security and performance results and discussions

5.1 Security

The following are some of the important attacks and the resistance of the proposed method against them and some security requirements:

5.1.1 Man-in-the-middle attack

In this attack, the attacker is trying to retrieve secret and private keys through intercepting communication channel between the card and card reader. In this case, the attacker cannot extract any useful information. Even if we assume that the attacker retrieves w while the card and card reader are communicating, but based on ECDLP, he cannot get the private key to use it and communicate with the card reader or card.

5.1.2 Forging attack

Identity forging attacks are difficult to detect in these networks because the attacker is trying to forge an authorized card ID in order to get the card's secret key. Now, assume that the attacker is trying to get the card's secret key, which requires solving discrete logarithm for the elliptic curve. Given the resistance of the discrete logarithm for the elliptic curve, as outlined in Johnson et al. [56], the proposed method will be reliable against this attack.

Table 2 Security comparison among related protocols

Item	Proposed scheme	Farash et al. [7]	Alamr et al. [35]	Zhang and Qi [26]	Zhao [3]	Shen et al. [28]	Liao and Hsiao [36]
Confidentiality	Yes	Yes	Yes	Yes	Yes	Yes	No
Avoiding insider attack	Yes	Yes	Yes	Yes	Yes	–	No
Avoiding forgery attack	Yes	Yes	Yes	Yes	Yes	–	No
Mutual authentication	Yes	Yes	Yes	Yes	Yes	Yes	No
Forwards security	Yes	Yes	Yes	No	No	Yes	No
Avoiding replay attack	Yes	Yes	Yes	Yes	Yes	–	Yes
Masquerade attack	Yes	No	No	No	No	No	No
Avoiding man-in-the-middle attack	Yes	Yes	Yes	Yes	Yes	–	Yes

Table 4 Unit conversion of various operations in terms of T_{MUL} [59]

Time complexity of an arithmetic unit	Time complexity in terms of modular multiplication
T_{PM}	$1200T_{MUL}$
T_{PA}	$5T_{MUL}$
T_H	Negligible

5.1.3 Mutual authentication

In the proposed method, if the value of SK_j is equal to SK_i, then the card reader has been able to authenticate the card, and if the card can calculate the value of w, it will authenticate the card reader.

5.1.4 Confidentiality

Based on ECDLP, the attacker cannot retrieve the private key from the messages.

5.1.5 Masquerade attack

There is an extraordinarily important attack whenever a card wants to compute authorized secret keys. Imagine that a malicious card reader masquerades like the server and distributes some planned public parameters $M_{i,\ j}$ and $M_{j,\ i}$. Then, assume some cards use these public parameters to compute secret keys SK_i. If this card uses SK_i as a proper symmetric key and sends it to the card reader encrypted confidential data, then the malicious card reader, with the proper secret key SK_i, can decrypt and access those confidential data. An authentication mechanism such as the proposed scheme in Nikooghadam et al. [57], improved by the changes suggested by the present researchers, is able to stand against this attack. Although a number of overheads are imposed, they are fewer than ECDSA digital signature algorithm [56] used in [58]. Furthermore, suppose a constant and unique private key such as α has been selected by the server, and the resultant public key $Q = \alpha G$ is registered in the server as trusted for all cards and has been registered in the server. In the following, the employment of digital signature is described step by step.

(a) The server prepares special information corresponding to each public parameter $M_{i,\ j}$ and $M_{j,\ i}$, like a digital signature as follows:
   1. Selecting a random integer such as β.
   2. Computing the point $R = \beta G = (x_0, y_0)$ on agreed elliptic curve and assigning $r = x_0 \bmod n$. If $r = 0$, then go to step 1.
   3. Converting all public parameter $M_{i,\ j}$ and $M_{j,\ i}$ into an integer e using a secure one-way hash function as follows: $e = \text{hash}(M_{i,\ j}||M_{j,\ i})$.
   4. Computing $s = (\alpha re + \beta) \bmod n$.
   5. Publishing certain couple information (s,R) along with public parameters $M_{i,\ j}$ and $M_{j,\ i}$ according to Fig. 4.

(b) Each card verifies the validity of public parameters $M_{i,\ j}$ and $M_{j,\ i}$ before using it to compute the assigned secret key as follows:
   1. Converting received $M_{i,\ j}$ and $M_{j,\ i}$ to e by hash function.
   2. Computing $v = sG$.
   3. Computing $s^* = erQ + R$; consider that r is the x-coordinate of the received point R and Q is the reliable public key of the server.
   4. If $v = s^*$, then signature is valid; otherwise, it is rejected.

As an example for card reader, the server signs all public parameter $M_{i,\ j}$ and $M_{j,\ i}$ of the cluster members which have been converted to an integer e by one-way hash function and sends besides the public parameters $(M_{i,\ j}, M_{j,\ i})$ to the card reader. Then, card reader public parameter converts to one integer e and investigates the signature verification following the steps explained above.

Table 2 shows the security comparison between related protocols and the proposed method. This is a comparison between recent research papers such as Farash et al. [7], Alamr et al. [35], Zhang and Qi [26], Zhao [3], Liao and Hsiao [36], Shen et al. [28], and the proposed method in this research.

5.2 Performance

To evaluate the performance, we have compared our proposed method with similar recent research papers such as Farash et al. [7], Alamr et al. [35], Zhang and Qi [26], Zhao [3], Liao and Hsiao [36], Shen et al. [28]. We

Table 5 Performance comparison computation costs among related protocols in the authentication phase

	Time complexity		Time complexity in unit of T_{MUL}.
	Tag	Reader	
Liao and Hsiao [36]	$5T_{PM}$	$5T_{PM}$	$[12000]T_{MUL}$
Alamr et al. [35]	$4T_{PM}$	$5T_{PM}$	$[10800]T_{MUL}$
Zhao [3]	$5T_{PM}$	$5T_{PM}$	$[12000]T_{MUL}$
Shen et al. [28]	$3T_{PM} + 4T_H$	$3T_{PM} + 3T_H$	$[7200]T_{MUL}$
Zhang and Qi [26]	$2T_{PM} + 2T_H$	$1T_{PM} + 2T_H$	$[3600]T_{MUL}$
Farash et al. [7]	$2T_{PM} + 2T_H$	$1T_{PM} + 2T_H$	$[3600]T_{MUL}$
Proposed scheme	$1T_{PM} + 2T_H$	$1T_{PM} + 2T_H$	$[2400]T_{MUL}$

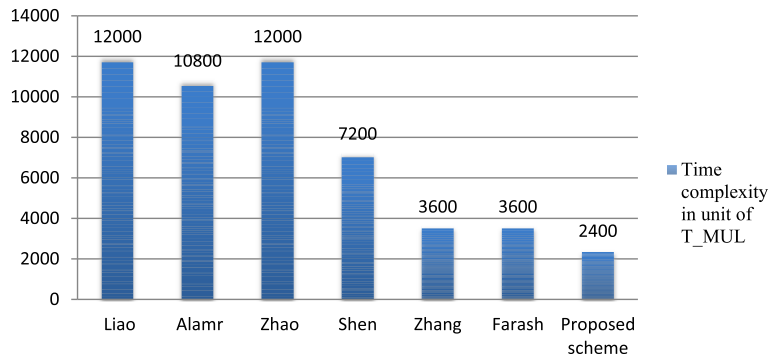

Fig. 6 Performance comparison illustrated in Table 5

estimated the cost of the authentication phase for each of the six methods, for both the card reader and card. In Table 3, we present some of the various symbols used in this section.

On the other hand, according to the method proposed in Nikooghadam et al. [59], the complexity of time for implementation of various operational phases is calculated using modular exponentiation. The results are specified in Table 4.

The comparison between the six methods is shown in Table 5. Since all of the public and private keys and other main parameters are loaded into the card and card reader in the initialization phase, thus, the computational cost of the private and public keys and other parameters is zero. In the authentication phase of our method, the computational cost is $2T_H + 1T_{PM}$ and $2T_H + 1T_{PM}$ for the card and card reader, respectively. Therefore, our proposed method has lower computational cost, when compared to other methods.

It should be noted, due to the fact that time complexity for modular exponentiation in operating unit T_H and T_{PA} is not high, the related values are excluded from Table 5.

As shown in Fig. 6, the performance comparison is illustrated in Table 5.

It is also possible to calculate the execution time of the most complex operations on elliptic curve, that is, the elliptic curve point multiplication in milliseconds. For instance, we assume that all of the related articles use an elliptic curve with an equal key length of 160 bits. The execution time of the elliptical curve point multiplication on 5 MHZ cards equals 0.064 s. The running time of the elliptic curve point multiplication among the related protocols for both the card and the card reader is given in Table 6.

6 Conclusion

Considering the constant developments of the Internet of Things and its applications in fields such as health care systems, where patient information is critical and nobody should have access to this information, then providing security for these networks is essential. Various studies have been done recently to address security and computational cost problems. In this paper, we have proposed an elliptic curve cryptography method that, in addition to maintaining security, has less computational cost compared to similar studies. Furthermore, key management solutions are presented for dynamic access problems in RFID cards in order to be able to develop scalability healthcare networks. For future work, a hardware implementation can also be done in order to evaluate the precise security and computational cost of the proposed method.

Table 6 The running time of the elliptic curve point multiplication among related protocols in authentication phase

	Running time of the elliptic curve point multiplication		Total computational costs
	Tag	Reader	
Liao and Hsiao [36]	$5T_{PM} = 5 \times 64 = 320$	$5T_{PM} = 5 \times 64 = 320$	640(ms)
Alamr et al. [35]	$4T_{PM} = 4 \times 64 = 256$	$5T_{PM} = 5 \times 64 = 320$	576(ms)
Zhao [3]	$5T_{PM} = 5 \times 64 = 320$	$5T_{PM} = 5 \times 64 = 320$	640(ms)
Shen et al. [28]	$3T_{PM} = 3 \times 64 = 192$	$3T_{PM} = 3 \times 64 = 192$	384(ms)
Zhang and Qi [26]	$2T_{PM} = 2 \times 64 = 128$	$1T_{PM} = 1 \times 64 = 64$	192(ms)
Farash et al. [7]	$2T_{PM} = 2 \times 64 = 128$	$1T_{PM} = 1 \times 64 = 64$	192(ms)
Proposed scheme	$1T_{PM} = 1 \times 64 = 64$	$1T_{PM} = 1 \times 64 = 64$	128(ms)

Abbreviations
ECC: Elliptic curve cryptography; IoT: Internet of Things

Authors' contributions
The authors declare no conflict of interest. The authors read and approved the final manuscript.

Funding
Not applicable.

Competing interests
The authors declare that they have no competing interests.

Author details
[1]Department of Computer Engineering, Sabzevar Branch, Islamic Azad University, Sabzevar, Iran. [2]Department of Computer Engineering, Mashhad Branch, Islamic Azad University, Mashhad, Iran.

Received: 24 January 2020 Accepted: 15 July 2020
Published online: 29 July 2020

References

1. H. Sundmaeker, P. Guillemin, P. Friess, S. Woelfflé, Vision and challenges for realising the Internet of Things. *Cluster of European Research Projects on the Internet of Things, European Commision* **3**(3), 34–36 (2010)
2. L. Atzori, A. Iera, G. Morabito, Computer networks: the International Journal of Computer and Telecommunications Networking. *Volume* **54**, 2787–2805 (2010)
3. Z. Zhao, A secure RFID authentication protocol for healthcare environments using elliptic curve cryptosystem. *Journal of medical systems* **38**(5), 46 (2014)
4. A. Juels, RFID security and privacy: a research survey. *IEEE journal on selected areas in communications* **24**(2), 381–394 (2006)
5. D.C. Ranasinghe, M. Sheng, S. Zeadally, *Unique radio innovation for the 21st century: building scalable and global RFID networks* (2010)
6. S. Cai, Y. Li, T. Li, and R. H. Deng, "Attacks and improvements to an RFID mutual authentication protocol and its extensions," in *Proceedings of the second ACM conference on Wireless network security*, 2009, pp. 51-58: ACM.
7. M.S. Farash, O. Nawaz, K. Mahmood, S.A. Chaudhry, M.K. Khan, A provably secure RFID authentication protocol based on elliptic curve for healthcare environments. *Journal of medical systems* **40**(7), 165 (2016)
8. D. He, S. Zeadally, An analysis of RFID authentication schemes for internet of things in healthcare environment using elliptic curve cryptography. *IEEE internet of things journal* **2**(1), 72–83 (2015)
9. Q. Z. Sheng, X. Li, and S. Zeadally, "Enabling next-generation RFID applications: solutions and challenges," *Computer,* vol. 41, no. 9, 2008.
10. X. Yang, X. Yi, Y. Zeng, I. Khalil, X. Huang, and S. Nepal, "An improved lightweight RFID authentication protocol for Internet of Things," in *International Conference on Web Information Systems Engineering*, 2018, pp. 111-126: Springer.
11. Y. Hung, "The study of adopting RFID technology in medical institute with the perspectives of cost benefit," in *International Medical Informatics Symposium in Taiwan, Taiwan*, 2007.
12. J.E. Katz, R.E. Rice, Public views of mobile medical devices and services: a US national survey of consumer sentiments towards RFID healthcare technology. *International journal of medical informatics* **78**(2), 104–114 (2009)
13. J. Leu, *The benefit analysis of RFID use in the health management center—the experience in Shin Kong Wu Ho-Su Memorial Hospital* (*National Taiwan University*, 2010)
14. W. Yao, C.-H. Chu, Z. Li, The adoption and implementation of RFID technologies in healthcare: a literature review. *Journal of medical systems* **36**(6), 3507–3525 (2012)
15. P. Najera, J. Lopez, R. Roman, Real-time location and inpatient care systems based on passive RFID. *Journal of Network and Computer Applications* **34**(3), 980–989 (2011)
16. F. Rahman, M.Z.A. Bhuiyan, S.I. Ahamed, A privacy preserving framework for RFID based healthcare systems. *Future Generation Computer Systems* **72**, 339–352 (2017)
17. J. Kang, Lightweight mutual authentication RFID protocol for secure multi-tag simultaneous authentication in ubiquitous environments. *The Journal of Supercomputing*, 1–14 (2016)
18. L. Gao, L. Zhang, M. Ma, Low cost RFID security protocol based on rabin symmetric encryption algorithm. *Wireless Personal Communications*, 1–14 (2017)
19. M.H. Dehkordi, Y. Farzaneh, Improvement of the hash-based RFID mutual authentication protocol. *Wireless personal communications* **75**(1), 219–232 (2014)
20. M. Safkhani, P. Peris-Lopez, J.C. Hernandez-Castro, N. Bagheri, Cryptanalysis of the Cho et al. protocol: a hash-based RFID tag mutual authentication protocol. *Journal of Computational and Applied Mathematics* **259**, 571–577 (2014)
21. M.R. Alagheband, M.R. Aref, Simulation-based traceability analysis of RFID authentication protocols. *Wireless Personal Communications* **77**(2), 1019–1038 (2014)
22. C.L. Chen, Y.C. Huang, T.F. Shih, A novel mutual authentication scheme for RFID conforming EPCglobal class 1 generation 2 standards. *Information Technology And Control* **41**(3), 220–228 (2012)
23. W.C. Kuo, B.-L. Chen, L.-C. Wuu, Secure indefinite-index RFID authentication scheme with challenge-response strategy. *Information Technology And Control* **42**(2), 124–130 (2013)
24. M.R. Alagheband, M.R. Aref, Unified privacy analysis of new-found RFID authentication protocols. *Security and Communication Networks* **6**(8), 999–1009 (2013)
25. M.S. Farash, Cryptanalysis and improvement of an efficient mutual authentication RFID scheme based on elliptic curve cryptography. *The Journal of Supercomputing* **70**(2), 987–1001 (2014)
26. Z. Zhang, Q. Qi, An efficient RFID authentication protocol to enhance patient medication safety using elliptic curve cryptography. *Journal of medical systems* **38**(5), 47 (2014)
27. H.-Y. Chien, Elliptic curve cryptography-based RFID authentication resisting active tracking. *Wireless Personal Communications* **94**(4), 2925–2936 (2017)
28. H. Shen, J. Shen, M.K. Khan, J.-H. Lee, Efficient RFID authentication using elliptic curve cryptography for the internet of things. *Wireless Personal Communications* **96**(4), 5253–5266 (2017)
29. D. Hankerson, S. Vanstone, A. Menezes, *Guide to elliptic curve cryptography, Springer-Verlag* (*New York*, 2004)
30. P. Deepthi, P. Sathidevi, New stream ciphers based on elliptic curve point multiplication. *Computer Communications* **32**(1), 25–33 (2009)
31. M.S. Farash, Cryptanalysis and improvement of 'an improved authentication with key agreement scheme on elliptic curve cryptosystem for global mobility networks'. *International Journal of Network Management* **25**(1), 31–51 (2015)
32. C.-T. Li, C.-Y. Weng, C.-C. Lee, A secure RFID tag authentication protocol with privacy preserving in telecare medicine information system. *Journal of medical systems* **39**(8), 77 (2015)
33. K. Srivastava, A.K. Awasthi, S.D. Kaul, R. Mittal, A hash based mutual RFID tag authentication protocol in telecare medicine information system. *Journal of medical systems* **39**(1), 153 (2015)
34. J. Chou, "A secure RFID authentication protocol to enhance patient medication safety using elliptic curve cryptography," *J. Supercomput,* 2014.
35. A.A. Alamr, F. Kausar, J. Kim, C. Seo, A secure ECC-based RFID mutual authentication protocol for internet of things. *The Journal of Supercomputing*, 1–14 (2016)
36. Y.-P. Liao and C.-M. Hsiao, "A secure ECC-based RFID authentication scheme using hybrid protocols," in *Advances in Intelligent Systems and Applications-Volume 2*: Springer, 2013, pp. 1-13.
37. S. Amendola, R. Lodato, S. Manzari, C. Occhiuzzi, G. Marrocco, RFID technology for IoT-based personal healthcare in smart spaces. *IEEE Internet of things journal* **1**(2), 144–152 (2014)
38. C. Lai, H. Li, X. Liang, R. Lu, K. Zhang, X. Shen, CPAL: a conditional privacy-preserving authentication with access linkability for roaming service. *IEEE Internet of Things Journal* **1**(1), 46–57 (2014)
39. Y.-P. Liao, C.-M. Hsiao, A secure ECC-based RFID authentication scheme integrated with ID-verifier transfer protocol. *Ad Hoc Networks* **18**, 133–146 (2014)
40. H. Shen, C. Gao, D. He, L. Wu, New biometrics-based authentication scheme for multi-server environment in critical systems. *Journal of Ambient Intelligence and Humanized Computing* **6**(6), 825–834 (2015)
41. D. He, S. Zeadally, Authentication protocol for an ambient assisted living system. *IEEE Communications Magazine* **53**(1), 71–77 (2015)
42. D. He, An efficient remote user authentication and key agreement protocol for mobile client–server environment from pairings. *Ad Hoc Networks* **10**(6), 1009–1016 (2012)

43. D.M. Hein, J. Wolkerstorfer, N. Felber, ECC is ready for RFID-a proof in silicon. *Selected Areas in Cryptography* **5381**, 401–413 (2008) Springer
44. Y.K. Lee, K. Sakiyama, L. Batina, I. Verbauwhede, Elliptic-curve-based security processor for RFID. *IEEE Transactions on Computers* **57**(11), 1514–1527 (2008)
45. H. Ning, H. Liu, J. Mao, Y. Zhang, Scalable and distributed key array authentication protocol in radio frequency identification-based sensor systems. *IET communications* **5**(12), 1755–1768 (2011)
46. B. Alomair, A. Clark, J. Cuellar, R. Poovendran, Scalable RFID systems: a privacy-preserving protocol with constant-time identification. *IEEE Transactions on Parallel and Distributed Systems* **23**(8), 1536–1550 (2012)
47. B. Alomair, R. Poovendran, Privacy versus scalability in radio frequency identification systems. *Computer Communications* **33**(18), 2155–2163 (2010)
48. B. Song, C.J. Mitchell, Scalable RFID security protocols supporting tag ownership transfer. *Computer Communications* **34**(4), 556–566 (2011)
49. P. Guo, J. Wang, X. H. Geng, C. S. Kim, and J.-U. Kim, "A variable threshold-value authentication architecture for wireless mesh networks," vol. 15, no. 6, pp. 929-935, 2014.
50. J. Shen, H.-W. Tan, J. Wang, J.-W. Wang, and S.-Y. Lee, "A novel routing protocol providing good transmission reliability in underwater sensor networks," vol. 16, no. 1, pp. 171-178, 2015.
51. P. Tuyls and L. Batina, "RFID-tags for anti-counterfeiting," in *Cryptographers' Track at the RSA Conference*, 2006, pp. 115-131: Springer.
52. Y. K. Lee, L. Batina, and I. Verbauwhede, "EC-RAC (ECDLP based randomized access control): provably secure RFID authentication protocol," in *RFID, 2008 IEEE International Conference on*, 2008, pp. 97-104: IEEE.
53. L. Batina, J. Guajardo, T. Kerins, N. Mentens, P. Tuyls, and I. Verbauwhede, "Public-key cryptography for RFID-tags," in *Pervasive Computing and Communications Workshops, 2007. PerCom Workshops' 07. Fifth Annual IEEE International Conference on*, 2007, pp. 217-222: IEEE.
54. K. Kaur, N. Kumar, M. Singh, and M. S. Obaidat, "Lightweight authentication protocol for RFID-enabled systems based on ECC," in *Global Communications Conference (GLOBECOM), 2016 IEEE*, 2016, pp. 1-6: IEEE
55. A. ANSI, "X9. 62-1998: public key cryptography for the financial services industry: the elliptic curve digital signature algorithm (ECDSA)," *American National Standards Institute (ANSI), Washington, DC*, 1998.
56. D. Johnson, A. Menezes, S. Vanstone, The elliptic curve digital signature algorithm (ECDSA). *International Journal of Information Security* **1**(1), 36–63 (2001)
57. M. Nikooghadam, A. Zakerolhosseini, M.R. Bonyadi, A protocol for digital signature based on the elliptic curve discrete logarithm problem. Journal of Applied Sciences **8**(10), 1919–1925 (2008)
58. Azarderakhsh et al. A key management scheme for cluster based wireless sensor networks.2008 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing.
59. M. Nikooghadam, A. Zakerolhosseini, M.E. Moghaddam, Efficient utilization of elliptic curve cryptosystem for hierarchical access control. *Journal of Systems and Software* **83**(10), 1917–1929 (2010)

Publisher's Note