Advances in Computer, Signals and Systems (2022)
Clausius Scientific Press, Canada

DOI: 10.23977/acss.2022.060608
ISSN 2371-8838 Vol. 6 Num. 6

COVID-19 Prevention and Control System Based on RFID

Fan Lu, Xiuqing Chen*, Jiahao Li, Lei Kai, Ziyan Liu, Jianqiang Guo

School of Medical Information and Engineering, Xuzhou Medical University, Xuzhou, Jiangsu, China
**Corresponding author*

Keywords: RFID, COVID-19, Cloud technology, Mutual authentication

Abstract: Radio Frequency Identification (RFID) is a part of Internet of Things (IoT), using low-cost RFID tag to communicate. RFID plays an important role in COVID-19. Researchers have proposed RFID authentication systems for e-healthcare to address the issue of privacy leakage. However, it is significant to propose a lightweight and secure protocol for medical systems due to the weak computing power of the tag. We present an innovative and lightweight RFID authentication system using cloud technology, and we use the expanded formal security model to demonstrate the proposed protocol's security. The security model has an unstable channel between servers and readers, and we use the informal investigation to demonstrate how secure our protocol is. Through these analysis, our scheme can resist the common attacks, forward attacks and backward attacks and retain mutual authentication, information integrity. Moreover, tags and readers can be anonymous.

1. Introduction

In recent years, RFID technology has becomed more and more popular. It can be applied to many fields, such as medical treatment, material supply chain management, drug safety and traceability.

The outbreak of COVID-19 has attracted the attention of all countries. RFID can effectively track suspected COVID-19 cases. The development of medical electronic healthcare system based on RFID technology is very rapid [1]. RFID technology can ensure the traceability of real-time data for medical personnel and resources, provide communication and share location information [2]. Using RFID technology to deposit the acquired data in the database can better analyze the health of patients [3].

In order to design secure RFID authentication solutions to preserve the privacy of readers and tags, many schemes to ensure RFID security have been proposed, but they have been proved to be problematic. Niu *et al*. [4] proposed an ultra lightweight and privacy protection authentication scheme for mobile RFID system. This paper finds that the scheme [4] may be forged in the authentication process. Therefore, this paper proposes a novel and lightweight RFID authentication scheme to ensure the correct source and destination of information.

This paper makes the following contributions:

(1) A new RFID mutual authentication protocol based on hash is proposed to keep anonymity for both tags and readers.

(2) We use a reinforced formal model to illustrate the formal certification. Our protocol has correctness and security, and can resist forward attacks and backward attacks.

(3) Through informal analysis, we prove that the proposed protocol also achieves common security requirements and can be applied to practice.

Recently, RFID technology has a wide range of applications in various sectors. In order to prevent the spread of COVID-19, Rajasekar *et al*. [5] proposed an automatic tracking of COVID-19 by deploying RFID tags and personal mobile devices acting as readers. Lim *et al*. [6] pointed that installing RFID readers at toll stations and installing tags on all vehicles can minimize the spread of COVID-19.

RFID technology is widely used in healthcare systems, such as patient monitoring, drug management, and medical asset tracking [7]. Aiming at solving the problem of patient privacy information leakage in the RFID protocol of the wireless remote medical monitoring system, Agrahari *et al*. [1] proposed an elliptic curve-based RFID certification agreement.

RFID devices can be used to track patients, products, etc., but they have many security problems. Kumar *et al*. [8] discussed various attacks that RFID may encounter and put forward corresponding solutions, but there are still many problems that have not been solved. Chen *et al*. [9] proposed a tobacco product traceability protocol based on blockchain and RFID, which solves the problems of counterfeiting and traceability. Ai *et al*. [10] proposed a more general attack model based on RFID to solve the problem that cloning attack will seriously disrupt RFID system. Ali *et al*. [11] proposed a new blind signcryption scheme based on Hyperelliptic Curve, but it can not resist desynchronization attacks and data forgery attacks.

2. Preliminaries

2.1. Notations

The notations of our protocol are shown in Table1

Table 1: Notations

Symbols	Meaning
T_i	The i-th tag
R_j	The j-th reader
ID_i, PID_i	The i-th identity and pseudo-identity of T_i
RID_j, $PRID_j$	The j-th identity and pseudo-identity of R_j
S	Cloud server
R_r, R_t	The random number created by (R_j, T_i), respectively
$Data_i$	Messages of T_i, which is deposited in S
h(.)	One-way hash function which is collision resistant
||	The concatenation operation
$\oplus$	The bitwise XOR operation
A	An adversary
l	Security parameter used for the length of the hash result and the random number

2.2. Security Needs of RFID Systems for Informal Analysis

The communication between tags, readers and servers are considered. The channels among them are supposed to be exposed during the authentication process. The security needs of the informal analysis are explained below:

(1) Mutual authentication: since three entities are applied to the protocol, anyone is supposed to be authenticated by others.

(2) Anonymity: the identity of the tag should be hidden when transporting and should not be tracked. It is superior that if the identity of the reader can be untraceable, either.

(3) Scalability: servers should search the identity of tags in their databases to legalize it. But with the increasing of the number of tags, search calculations should change insignificantly. Or a tag's identity must be determined directly searching without performing any extra checking.

(4) Resist common attacks: replay attacks and de-synchronization attacks must be prevented.

2.3. Basic Knowledge about Hash Function

$l \in N$ is a security parameter and we can define a hash function as $H:\{0, 1\}^{*} \rightarrow \{0, 1\}^{l}$ (N is a set of natural numbers). Moreover, three conditions are required:

(1) For a given y, it is difficult to find a x satisfying $H(x) = y$.

(2) It is difficult to search two various binary strings x_1 and x_2 where $H(x_1) = H(x_2)$.

(3) It is difficult for A who asks for H in polynomial time to distinguish the outputs of H from random numbers.

3. Outline of Our Protocol

The proposed scheme is divided into two stages: registration and authentication.

3.1. Registration Stage

Step 1. T_i and S share ID_i. Then S chooses PID_i and x_i, and holds them in T_i. S sets $xnew\ j = xold\ j = x_i$ and $Pnew\ j = Pold\ j = PID_i$ and holds ($xnew\ j$, $xold\ j$, $Pnew\ j$, $Pold\ j$) in the database.

Step 2. R_j and S share RID_j. Then S chooses $PRID_j$ and x_j, and holds them in R_j. S defines $xnew\ j = xold\ j = x_j$ and $Pnew\ j = Pold\ j = PRID_j$ and saves ($xnew\ j$, $xold\ j$, $Pnew\ j$, $Pold\ j$) in its own database. Therefore, the records (ID_i, ($xnew\ j$, $Pnew\ j$), ($xold\ j$, $Pold\ j$)) and (RID_j, ($xnew\ j$, $Pnew\ 2$), ($xold\ j$, $Pold\ j$) are for i and R_j, respectively.

3.2. Authentication Stage

Six steps are included in this phase and listed in Figure.1.

Step 1. R_j creates R_r, and transmits $M_1 = \{R_r\}$ to i.

Step 2. After T_i accepts M_1, it creates R_t, calculates $B_1 = h\ (x_i||R_r||R_t||ID_i)$ and transmits $M_2 = \{B_1, R_t, PID_i\ \}$ to R_j.

Step 3. R_j calculates $B_2 = h\ (x_j\ ||R_r||R_t||RID_j)$, and transmits $M_3 = \{B_1, B_2, R_r, R_t, PID_i, PRID_j\}$ to S.

Step 4. After getting M_3 from R_j, S queries PID_i and transmits $PRID_j$. Either ineffectual query will result in rejection. The following operations are divided into three cases:

Case 1: If $PID_i = Pnew\ i$and $PRID_j = Pnew\ j$, S queries the relevant ID_i, $xnew\ i$, RID_j and $xnew\ j$, and examines if $B_1 = h\ (xnew\ i||R_r\ ||R_t\ ||ID_i)$ and $B_2 = h(xnew\ j||R_r\ ||R_t\ ||RID_j)$. If anyone of them is unsuccessful, the session will be refused. Otherwise, S renews ($xold\ i$, $Pold\ j$, $xold\ j$, $Pold\ j$) with ($xnew\ i$, $Pnew\ i$, $xnew\ j$, $Pnew\ j$) in databases, and calculates the new data as follows:

$$\text{xnew i=h(xold i||Rt||Rr||IDi)} \quad (1)$$

$$\text{Pnew j=h (xold i||Rt||Rr||RIDj)} \quad (2)$$

$$\text{xnew i=h (xold j||Rt||Rr||PRIDj)} \quad (3)$$

$$\text{Pnew j=h (xold j||Rt||Rr||PRIDi)} \quad (4)$$

$$\text{B3=h (xold i||xnew j||Pold i||Pnew i||IDj)} \oplus \text{h (xnew j||Pnew j||Rr)} \quad (5)$$

$$\text{B4=h (xold j||xnew j||Pold j||Pnew j||RIDj||Rr)} \oplus \text{datai} \quad (6)$$

$$\text{B6=h (xold j||RIDj||Pold j||datai||Rr)} \quad (7)$$

Finally, S transmits the information $M_4 = \{B_3, B_4, B_5\}$ to R_j. S employs the operations of this case, which shows that the last session ran normally.

Case 2: Otherwise, if $PID_i = Pold\ i$ and $PRID_j = Pold\ i$, $PRID_{j2} = h\ (x_j||R_t||R_r||RID_j)$, S queries the relevant ID_i, $xold\ j$, RID_j and $xold\ j$, and examines if $B_1 = h\ (xold\ i||R_r||R_t\ ||ID_i)$ and $B_2 = h(xold\ j||R_r||R_t||RID_j)$. If anyone of them is unsuccessful, the session will be refused. Otherwise, the elements in Eqs. (1)–(7) are calculated, and S transmits M_4 to R_j. The fact that S employs like this case shows that M_4 in the last session is stopped.

Case 3: Otherwise, if $PID_i = Pold\ i$ and $PRID_j = Pnew\ j$, S queries the relevant ID_i, $xold\ i$, RID_j and $xnew\ j$, and examines if $B_1 = h(xold\ i\ ||R_r\ ||R_t\ ||ID_i)$ and $B_2 = h(xold\ j||R_r||R_t||RID_j)$. If anyone of them is unsuccessful, the session will be refused. Otherwise, S renews ($xold\ i$, $Pold\ i$) with ($xnew\ j$, $Pnew\ j$), calculates Eqs. (1)–(7), and transmits the information M_4 to R_j. The fact that S employs like this case shows that M_5 in the last session is stopped.

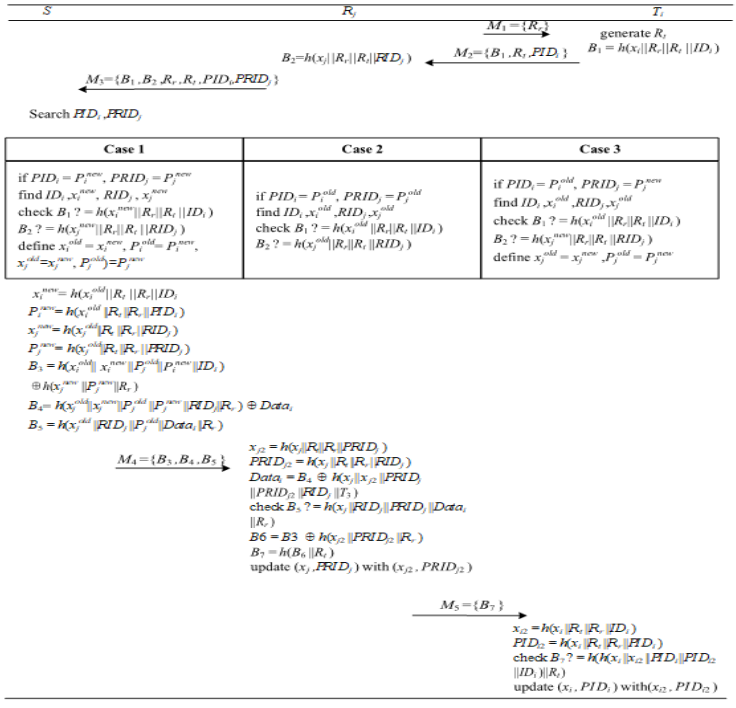

Figure 1: The proposed protocol

Step 5. R_j calculates $x_{j2} = h\ (x_j||R_t||R_r||PRID_j)$ and $PRID_{j2} = h\ (x_j||R_t||R_r||RID_j)$, receives T_i's message $Data_i = B_4 \oplus h\ x_j\ ||x_{j2}||PRID_j\ ||PRID_{j2}||RID_j\ ||T_3)$, and examines if $B_5 = h\ (x_j\ ||RID_j\ ||PRID_j\ ||Data_i\ ||R_r)$. If it is true, R_j calculates $B_6 = B_3 \oplus h\ (x_{j2}\ ||PRID_{j2}\ ||R_r)$ and $B_7 = h\ (B_6||R_t)$, renews (x_j, $PRID_j$) with (x_{j2}, $PRID_{j2}$) and transmits $M_5 = \{B_7\}$ to T_i.

Step 6. T_i computes $x_{i2} = h(x_i||R_t||R_r||PRID_i)$ and $PRID_{i2} = h(x_i||R_t||R_r||RID_i)$, and examines if $B_7 = h(h(x_i||x_{i2}||PID_i||PID_{i2}||ID_i)||R_t)$. If it is true, T_i replaces (x_i, PID_i) with (x_{i2}, PID_{i2}).

4. Informal Analysis

We compare some lately lightweight protocols with ours in this section and the results are illustrated in Table 2.

4.1. Scalability (R0)

Servers do not demand detailed search operations for verifying PID_i and $PRID_j$. No additional calculation is demanded before the search. So our protocol is scalability.

4.2. The Replay Attack Resistance (R1)

Every new session T_i and R_j produce R_t and R_r and this way forestalls the replay attacks. For example, if a new session begins with a new R_r transmitted from R_j, T_i will produce a fresh R_t and the latter information use the two new random numbers. They are clearly diverse from the historical ones. Therefore, our protocol can resist the replay attack.

4.3. The De-synchronization Attack Resistance (R2)

If A hinders M_4 or M_5, S will complete relevant operations in view of Case 2 or 3 in step 4 of our authentication stage in the next session. The process of the authentication phase can again synchronize the secret value among the three parties. Our protocol can resist the de-synchronization attack.

4.4. The Data Forgery Attack Resistance (R3)

In our protocol, $Data_i$ sent in M_4 is verified by R_j with computing B_5. Both B_4 and B_5 are difficult to fake because x_j is not known to A. Our protocol can withstand the data forgery attack.

Table 2: Comparison

	Ours	[8]	[9]	[10]	[11]
R0	√	×	×	×	√
R1	√	√	√	×	√
R2	√	×	×	×	×
R3	√	×	×	×	×

Table 2 shows the shortcomings of the existing protocols [8-11]. The comparison results show that only our proposed scheme can meet all the above security needs, such as scalability, the replay attack resistance, the de-synchronization attack resistance and the data forgery attack resistance.

5. Conclusion

In the battle against COVID-19, the transmission of medical data requires a safe communication environment, and needs to realize reciprocal authentication and anonymity. In this passage, we propose a new novel and lightweight RFID authentication scheme. Then, we compare the proposed protocol with other protocols, and prove that our scheme has the attributes of scalability and can resist the replay attack, the de-synchronization attack and the data forgery attack through informal

analysis.

Acknowledgement

This work was supported in part by the practice innovation training program projects for the Jiangsu college students (Grant No. 202110313032Z).

References

[1] Agrahari A K, Varma S, (2021) A Provably Secure RFID Authentication Protocol Based on ECQV for the Medical Internet of Things, Peer-to-Peer Networking and Applications, vol.14, no.5, pp. 1277-1289.
[2] Tayyaba S, Khalid W, Ashraf M W, and Balas V E, (2021) Principles and Paradigms in IoT-Based Healthcare Using RFID, Healthcare Paradigms in the Internet of Things Ecosystem, vol.12, no.8, pp. 251-269.
[3] Khan H A, Abdulla R, Selvaperumal S K, and Bathich A, (2021) IoT Based on Secure Personal Healthcare Using RFID Technology and Steganography, International Journal of Electrical and Computer Engineering, vol.11, no.4, pp. 2088-8708.
[4] Niu B, Zhu X, Chi H, and Li H, (2014) Privacy and Authentication Protocol for Mobile RFID Systems, Wireless Personal Communications, vol.77, no.3, pp. 1713-1731.
[5] Rajasekar S, (2021) An Enhanced IoT Based Tracing and Tracking Model for COVID-19 Cases, SN Computer Science, vol.2, no.1, pp. 1-16.
[6] Lim G C L, Arada G P, Abad A C, and Magsino E R, (2021) RFID Tag Data Encryption Using Triple DES and RSA Algorithms, Journal of Physics: Conference Series, vol.1997, no.1, pp. 12-28.
[7] Mondal S, Kumar D, Chahal P, (2021) Recent Advances and Applications of Passive Harmonic RFID Systems: A Review, Micromachines, vol.12, no.4, pp. 4-20.
[8] Kumar A, Jain A K, Dua M, (2021) A Comprehensive Taxonomy of Security and Privacy Issues in RFID, Complex & Intelligent Systems, vol.7, no.3, pp. 1327-1347.
[9] Chen C L, Lim Z Y, Liao H C, Deng Y Y and Chen P, (2021) A Traceable and Verifiable Tobacco Products Logistics System with GPS and RFID Technologies, Applied Sciences, vol.11, no.11, pp. 1-36.
[10] Ai X, Chen H, Lin K, Wang Z and Yu J, (2020) Nowhere to Hide: Efficiently Identifying Probabilistic Cloning Attacks in Large-Scale RFID Systems, IEEE Transactions on Information Forensics and Security, vol.16, no.3, pp. 1-10.
[11] Ali U, (2021) RFID Authentication Scheme Based on Hyperelliptic Curve Signcryption, IEEE Access, vol.14, no.99, pp. 1-1.