Biometric based RFID tag mutual authentication protocol defending against illegitimate access

Keerti Srivastava¹*, Amit K. Awasthi² and R. C. Mittal³

Abstract
This research paper focuses on structuring an RFID Protocol in which the answer to the question “Am I really the person who is accessing the resources” will be solved by implementing biometric techniques with RFID Protocol. Therefore, an effort will make to construct RFID protocol using biometric impression of RFID tag holder for resisting the protocol against illegitimate access.

Keywords
Illegitimate Access, RFID tag, biometric template.

1. Introduction
The growing use of Radio Frequency Identification (RFID) technology to enhance ubiquitous computing environments has only begun to be realized. It allows for the identification of objects and/or subjects remotely using attached RFID tags via a radio frequency channel.

Presently, most of the applications are faced with a process of access control, which is generally access by physical access control. When a physical access is initiated, it undergoes a verification of the person requesting access to a zone (e.g. building, office, parking, laboratory, etc.) for the accessing person’s lies necessities for the same.

If we take up an issue of individual user interface with its private or secret documents, assets, profile etc, there is an alarming level of risk on the rise. Analysts have proposed various names for such attacks, where an adversary with the help of an accomplice would try to gain access a target’s personal assets. The threat becomes even more challenging, when a legitimate user does all these attack in tandem with the adversary and willfully becomes the accomplice itself. Car theft is also the one of the example, wherein the car owner on approaching near to the car, opens the car door using a remote (automated system for opening a car door) provided. But if that remote in possession of an adversary, there is no system to insure car safety, which is called illegitimate access. So there is a need of improvisation in this area to enhance the security level.

Since last decade, many RFID Protocols [1], [2], [3], [12] have been proposed by different cryptographers to deal the first question, “Who am I”, i.e., the mutual authenticity of tag and reader is established and ensured but do not deal with the second question “Am I really the person who is proceeding” i.e., the legitimacy of the bearer of the tag remains in question.

In this paper, we propose an RFID authentication protocol
using biometric technique, which can reply both the questions—
(1) Who am I? (2) Am I really the person who is proceeding?
The proposed scheme provides un-traceability, mutual authen-
ticity between tag and reader. Finally, the security analysis
shows that proposed scheme can withstand against several
attacks and performance analysis with other related schemes
shows that it is reasonable in terms of computation cost and
communication cost. This work focuses to structure an au-
thentication protocol combined RFID-biometric system to
give a tertiary level of security in protocol, which ensures the
authenticity, privacy, secrecy. In our protocol, we use a PRNG
(Pseudo Number Generator) and a robust hash function. Also
in our protocol, we will use a biometric hash function for
optimizing and protecting the biometric template.

The rest of the paper is arranged as follows: section 2
presents related work. Section 3 presents the system and hy-
potheses. Section 4 presents the proposed protocol. Section
5 shows the security analysis of the proposed protocol. Fi-
nally, section VI presents a comparison of performances with
existing related works and conclude by a result and discussion.

2. Related Research Work

There are several RFID authentication protocols [1], [2],
[3], [12] have been proposed, wherein each scheme possess
the different level of security and complexity of implementation.
In all of these RFID Protocols, an identifier ID of tag is
utilized. It works on two mechanisms:

(1) **Static Identifier Mechanism**- In this mechanism, the
used Tag ID is unaltered throughout the authentication pro-
cess.

(2) **Dynamic Identifier Mechanism**- On the contrary, in this
mechanism, the used Tag ID is changeable throughout the
authentication process, both has its own advantages and draw-
backs. Here under, we focus the RFID Protocols based on
static identifier mechanism. In which, tag sends a series of
some sensitive information i.e. random number nt and a hash
value HI = h(ID, nt) to the reader over an insecure channel [3].
Thereby Weis et al’s protocol [3] becomes vulnerable to replay
and tracing attack. Further, Chien et al’s scheme [12] also
encounters replay attack and fortunately, both schemes [3]
[3] require random numbers generator, hence these schemes
could withstand against Man in the middle attack.

In 2008, Lee et al’s proposes an RFID Protocol [2] using
various hash operations to avoid tracing and spoofing attack.
But implementation of more hash operations increases the
cost, which is incompatible with storage space and lower
capacity to calculate. And enormous calculations with hash
operation influence the efficiency of protocol.

Of late many authentication protocols based on combined
smart card-biometric system have been proposed [7], [8], [9],
[10], [11] answering both the questions like “Who am I?” and
“Am I really the person who is proceeding”? First question
deals with identifying the person through smart card. While
the second question addresses the verification or authenti-
cation, it allows permission to the person claiming access
or defending against illegitimate accessing or forgery attack.
The implementation of these protocols [8], [10], [11] in RFID
systems will depend on the availability of computer resources
(memory, complexity, performance). Recent past have demon-
strated a few innovative blends of RFID and biometry system,
which ushers in further horizons of advanced research. The
propagators of RFID system, making use of biometric tech-
nique, proposed few solutions [4], [5], [6] to solve above
discussed problem.

3. System Modeling

RFID offers tremendous ease of work and most of the
organizations are rapidly accepting this technology. During
last few years, RFID Technology have been widely deployed
in every sector (health, supply chain management, access
control, etc). As compare to Contact-less smart card, RFID
system requires less computer resources (memory, processor,
computation energy, etc) which makes it more useful in to-
day’s technology. In this chapter, our proposed authentication
protocol consists of two sub systems: a RFID system and a
biometry system. RFID system consists of three units: tag,
reader, server, whereas biometry system consists of two units:
biometric sensor, biometric server.

3.1 RFID tag and reader

It contains user’s confidential ID and hash function, which
are shared between database of server and tag. Tag and Reader
generate a random numbers R, Rr respectively with help of
standard ISO and EPC GEN2 (Electronic Product Code Gen-
eration 2).

3.2 Server

In RFID-Biometric hybrid system, server has two services:
First, concerning with biometric system and another with
RFID system.

(i) To create biometric template B by extracting the biomet-
tric techniques (fingerprint, face, voice etc..) depending
upon usage.

(ii) It associates records with tag data collected by read-
ers, which are closely interrelated to each other in the
process of RFID Protocol.

3.3 Biometric Data

The tag and server contains biometric data, which gener-
ates a higher level of security and great mobility of the user.
Use of biometric template (bio-hashed value B) requires less
energy (300 bytes to 2K bytes) to store in memory, whereas
unprocessed biometric image (without hash function) requires
more energy (50 to 100K bytes), which is exhibited in this
proposed article. A hash function has been used to protect
and optimize the biometric data in the proposed work.
3.4 Biometric Sensor and Detector

Biometric sensors find their use in (fingerprint, face, voice etc..) recording and relaying various inputs, which are provided through a range of biometric technologies (fingerprint, face, voice etc..) and can be amicably, alternatively and profficably used as and in whichever form there either available/required. The variants of biometric technologies available and are also being explored make this user interface with biometric sensors (voice recognition-microphone, facial expression-camera, vein recognition) are making this process more and more convenient reliable and user friendly.

4. Proposed Protocol

Our proposed protocol needs a PRNG (Pseud-Random Number Generator), a robust hash function. Further to optimize and to protect biometric data, a biometric hash function is used. The proposed Protocol can be divided into two processes: the registration phase and the authentication phases. We, subsequently, use the following notations:

4.1 Preliminaries

\[ ID_k : \text{Identifier of the } k\text{th tag and mutually shared by back-end server and tag} \]

\[ ||: \text{Concatenation operation} \]

\[ R_t : \text{Random number generated by reader} \]

\[ R_i : \text{Random number generated by tag} \]

\[ B : \text{Biometric template} \]

\[ h(.) : \text{A one way hash function.} \]

\[ g(.) : \text{A Biometric hash function.} \]

\[ GB = g(B) : \text{Bio-Hashed value of } B \]

\[ \oplus : \text{Bit-wise XOR Operation.} \]

\[ DB : \text{Data Base.} \]

**Table 1. Proposed Protocol**

| Server | Reader | Tag |
|--------|--------|-----|
| Secure ID_k, GB | Generates Random no. R_t Send R_t to Tag | Generates a Random no. R_i Compute GB = g(B) A = h(GB|R_i) \oplus ID_k C = h(GB|R_i) \oplus ID_k Send (A, R_i, g(.), h(.)) to the Reader |
| Extract ID_k, B from DB Compute GB = g(B) Compute h(GB|R_i) Compute h(GB|R_i) \oplus A Check h(GB|R_i) \oplus A = ID_k If so, then Tag is authentic otherwise reject the request Again compute C = h(GB|R_i) \oplus ID_k send C to Reader | Send (A, R_i, g(.), h(.)) to the Server | Check C = C If so, then server is authentic otherwise session expire |

4.2 Registration phase

Registration phase is also called Pre-Phase. The main purpose of this phase is to construct a biometric template and stored in server with identity. In this phase, it has to enact the following operations to get RFID tag.

**Step-1:** The legitimate user inputs his/her personal biometrics, to pass it on to the server of the trusted registration center (RC).

**Step-2:** The RC extracts biometric characteristics and creates a biometric template B.

**Step-3:** Then RC computes the biometric hash function GB such as GB = g(B).

**Step-4:** The registration center RC sends the sensitive information ID, GB in the user’s tag over a secure channel.

(To see Table 1)

4.3 Mutual Authentication phase

This phase consists of authentication of tag and tag holder. The process of authentication takes place as follows.

**Step-1:** Reader’s request-

The RFID reader randomly generates a number R_t, then sends a request to tag with random number R_t. Three cases may arise: 1) No tag replies, 2) Only single tag will reply, 3) Many tags reply at a time. Here last case is invalid due to the using of biometric template of individual, which is different for each tag.

**Step-2:** Communication of messages between tag and reader-

**Step-2.1:** The found tag by step-1, generates a random number R_t

**Step-2.2:** Tag computes A = h(GB||R_t) \oplus ID_k and C = h(GB||R_t) \oplus ID_k

**Step-2.3:** Then tag sends the message (A, R_t) to the RFID reader.

**Step-2.4:** The reader re-sends this message (A, R_t) to the back-end server after reforming the message by adding R_t such that (A, R_t, R_t).

**Step-3:** Authentication of the tag and tag holder-

Extract the tag’s and tag holder’s information ID_k, GB from data base. Then back-end server performs the following calculations using the saved information of each tag.

**Step-3.1:** Server computes h(GB||R_t) and h(GB||R_t)

**Step-3.2:** Server computes h(GB||R_t) \oplus A

**Step-3.3:** Server calculates h(GB||R_t) \oplus A = ID_k, if it will be same as extracted ID_k from data base. Then tag and tag holder both are authentic, otherwise session will be expired.

**Step-3.4:** After assuring the mutual authenticity between the tag and tag holder, server computes C’ = h(GB||R_t) \oplus ID_k and sends it back to the RFID reader

**Step-4:** Back-end server authentication-

After getting appropriate tag and tag holder, server receives the message C’ and pass it to the tag, then tag authenticates server by following calculations as follows;
5. Security Analysis

This section examine the security level of our proposed protocol and also gives a comparison of security threats with related previous work. The proposed RFID mutual authentication protocol is based on biometric template which offers a high resistance to common attacks related to RFID system.

(i) **Mutual Authentication** - The proposed protocol provides bilateral authentication between Tag and Server. The tag gets authenticated by the step-3 of Mutual Authentication phase-C and server authentication is shown in step-4 of Mutual Authentication phase-C.

(ii) **Untraceability** - The barrier against tracing is raised through the use of random numbers and anonymity. Therefore, no message that transports crucial information can appear twice due to the challenge/response mechanism by using changed random numbers $R_t$ and $R_r$ in each session. Also adversary cannot deduce $ID_t$ due one way hash function and xor operation. In this way, an attacker cannot trace or track the tag.

(iii) **Forgery attack Resistance** - Our Protocol belongs to the biometric impression, which creates the tertiary level of security. Therefore, if any attacker wants to forged login, then use of biometric fails to establishing the forgery attack.

(iv) **Man-in-the-middle Attack Resistance** - The proposed protocol could resistance to this attack by applying hash operation in each message. Man-in-the-middle attack that simply replays messages can only be avoided by using the random numbers related operations in each message.

(v) **De-synchronization Resistance** - Our proposed protocol uses static mechanism $ID$, which is fixed in every communication for each tag. So, in dropping of message between communication, failing of energy, breaking of connection during in authentication process, session will not be effected. Which can also resist the denial of service attack.

Table 2 gives a security comparison of above discussed RFID Protocols [1], [2], [3], [12] with our proposed work. By which it is showing that our proposed protocol is highly secure than any of the previously discussed RFID system based schemes.

| RFID Protocol | [12] | [11] | [12] | [12] | Our Proposed protocol |
|---------------|------|------|------|------|----------------------|
| Mutual Authentica tion | Yes | Yes | Yes | Yes | Yes |
| Untraceability | Yes | Yes | No | Yes | |
| Forgery attack Resistance | No | No | No | Yes | |
| Man-in-the-middle Attack Resistance | No | Yes | Yes | Yes | |
| De-synchronization | Yes | Yes | Yes | Yes | |

6. Performance Analysis

This section focuses on the performance of the proposed protocol based on costs during the authentication and login phases. Table 3 illustrates computation cost, communication cost, and storage cost of one RFID protocol [2], other 3 smart card based protocols [8], [10], [11] and finally of our proposed protocol.

| Protocol | Computation Cost | Storage Cost | Comm. Cost |
|----------|------------------|--------------|------------|
| [2] RFID | $4l$ | $2l$ | $5l(1l + 2l)$ |
| [8] Smart Card | $4h$ | $3l$ | $5l(2l + 3l)$ |
| [10] Smart Card | $4h$ | $3l$ | $5l(2l + 3l)$ |
| [11] Smart Card | $3h$ | $4l$ | $5l(2l + 3l)$ |
| Our Protocol | $2h$ | $2l$ | $4l(3l + 1l)$ |

$h$: cost of hash operation  
$l$: size of required memory

(i) **Computation Cost** - The computation cost is the function of the number of operations of the hash function in login and authentication phases on the tag in RFID protocols as well as on the Smart card in smart card based protocols using biometric technique. In our proposed RFID Protocol, we need only two hash operations in the tag, which shows the cost effectiveness of our protocol.

(ii) **Communication Cost** - Communication cost is the combination of the number of messages exchanges and the total bit length of conveyed messages in each communication between tag and reader. Concerning our protocol, the total bit length of communicated message from tag to reader is $3l$ and that for reader to tag is $l$

(iii) **Storage Cost** - The another important issue is the cost required for storage in server. In our proposed protocol, the tag needs $2l$ to keep or store the tag’s identity $ID$ and biometric template $B$.

Thus, we can see from the table, our protocol is more efficient and user friendly to RFID tags as far as the computation cost, communication cost, storage cost are concerned.

7. Result and Discussion

Our proposed protocol is accordant with the limited computational and memory resources of RFID tags. Also, we apply here a biometric hash function on biometric data for optimizing and protecting the biometric data. Here, we also made a comparison of security analysis by table 2, which shows that our proposed protocol is more secure than few related protocols [1], [2], [3], [12] and performance analysis table 3 shows that our proposed protocol is cost effective other than related schemes [2], [8], [10], [11].

References

[1] S. M. Lee and Y. J. Hwang and D. H. Lee and J. I. Lim, *Efficient Authentication for Low-Cost RFID Systems*,...
Biometric based RFID tag mutual authentication protocol defending against illegitimate access — 106/106

International Conference on Computational Science and its Applications - ICCSA 2005.

[2] Y.-C. Lee, and Y.-C. Hsieh, and P.-S. You, and T.-C. Chen, An Improvement on RFID Authentication Protocol with Privacy Protection, Proceedings of 3rd International Conference on Convergence and Hybrid Information Technology, South Korea: Busan-IEEE 2008, vol.2, pp.569–573.

[3] S. Weis and S. Sarma and R. Rivest and D. Engels Security and privacy aspects of low-cost radio frequency identification systems, Proceeding of International Conference on Security in Pervasive Computing SPC-2003, pp.454–469.

[4] H.-A. Aboalsamh, A Potable Biometric Access device using Dedicated Fingerprint Processor, WSEAS Transaction on Computers 2010, vol.9(8), pp.878-887.

[5] J.-P.-C Rodrigues, and F.-D Heirto, and B. Vaidya, Decentralized RFID authentication Solution for embedded Systems, Proceedings of 4th Int. Conference on Systems and Networks Communications, IEEE-2009, pp.174-178.

[6] N. Chikouche, and F.Cherif, and M. Benmohammed, An authentication Protocol based on Combined RFID-Biometric System, IJACSA-2012, vol.3(4), pp.62-67.

[7] A. Das Analysis and improvement on an efficient biometric based remote user authentication scheme using smart cards, Information Security, IET-2011, vol.5(3), pp.145–151.

[8] M.K. Khan, and J. Zhang, and X. Wang, Chaotic hash-based fingerprint biometric remote user authentication scheme on mobile devices, Chaos Solitons and Fractals-2008, vol.35(3), pp.519–524.

[9] C. C. Lee and R. X. Chang and L. A. Chen Improvement of Li-Hwang’s biometric-based remote user authentication scheme using smart cards, WSEAS Transactions on Communications-2011, vol.10(7), pp.193–200.

[10] Li, Chun-Ta and Hwang, Min-Shiang An efficient biometrics-based remote user authentication scheme using smart cards, Journal of Network and Computer Applications-2010, vol.33(1), pp.1–5.

[11] Y.-W. Lai, and S.-C. Chang, and C. Chang, An Improved Biometrics-based User Authentication Scheme without Concurrency System, International Journal of Intelligent Information Processing-2010, vol.1(1).

[12] H-Y. Chien and C-W Huang A lightweight RFID Protocol using substring Proceedings of International Federation for Information Processing, IFIP-2007, pp.422–431.

**********
ISSN(P):2319-3786
Malaya Journal of Matematik
ISSN(O):2321-5666
**********