IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

A LIGHTWEIGHT AUTHENTICATION PROTOCOL ON RFID SYSTEM USING PUF FUNCTION IN HEALTHCARE

[1]Mohammad Abdul Aeraf, [2] Dr. M.Arathi, [3]Mohammad Abdussami, [4] Dr. Mohd Shariq

[1, 2, 3,4] Department of computer science and Engineering,
[1,2]School of Information Technology, JNTUH, Hyderabad, India, 500 085, [3] IIIT Naya Raipur, Chhattisgarh, India, 892002
[4]Meerut Institute of Engineering and Technology, Meerut, Uttar Pradesh, India, 250005

Abstract: The rapid evolution of IoT devices has revolutionized the IT field, where automation has been given prime importance. RFID is one of such most prominent in-use technology used to track real-world entities. The entity could be a living object or a non-living object. The tag-attached object and the reader-server communicate wirelessly with each other. Applying RFID in healthcare has revolutionized the treatment process. The doctor and a patient, communicating over a wireless, insecure channel over the network, are subjected to threat by an unauthorized user. The clear text data sent over a wireless channel is insecure and subject to capture, due to known disclosure attacks. A protocol that is a necessity to prevent the data from leakage and to protect privacy is the requirement. This paper presents a protocol in which we use the hash function and the PUF function. The protocol is programmed and is simulated using the Scyther tool and tested for the possible attacks. The security analysis by Scyther shows that our proposed protocol is secure against known attacks. Upon analysis, we found that the communication cost and computation cost are considerably low. Hence, we design a light weight Authentication protocol such that if it is deployed over devices where the storage as well as computing capacity is low

***Index Terms* – Healthcare, attacks, PUF function, privacy, Scyther tool.**

I INTRODUCTION

Radio-frequency Identification (RFID) technology has vast applications in healthcare[1]. The RFID works on the frequency of radio waves. The RFID system includes the following components as follows: 1) A tag-attached object. 2) A reader used to read the tag. In vast domains such as IoT, all the things in modern-day-to-day life are connected to the internet. With the ability of these devices to communicate with other devices, the usage of these devices has increased. The use of various sensors-transceivers, micro-controllers lead to the design of smart cities, smart homes, monitoring and regulation of traffic with very little to no involvement of humans. The usage of cheap sensors enabled the patients in healthcare to benefit from nook and corners of the world [2]. The RFID being a wireless communication technology through which two or more communication devices communicate with each other at a time within a given range is used in the Internet of Things (IoT), which stores sensitive data, helps the entities to communicate with each other [3]. It was introduced in the Second World War to identify the plane from being a friend or enemy. The RFID technology uses a range of sight, in contrast to bar code technology, which uses the line-of-sight[4] .

The RFID technology is used in health care in conjugation to IoT to enhance the services in health care such as in tracking the assets such as a wheelchair, bottle of medicines, Newborn identification, patient identification, tracking, and validation, Locating the patient, managing the procedure & wellness center, etc. [4], [5]. The introduction of RFID technology helped in the treatment of patients of diverse age groups removing the barriers such as waiting in queue for the treatment and in the case when a patient couldn't meet the doctor physically and the treatment is being delivered at home over the internet. The various benefits of using RFID technology in health care include drastic improvement in patient safety with tracking, management, and validation acting as a facilitator in health care between medical staff and patient and also facilitating in reducing the cost in health care, reduction in treatment time and subsequently in increasing the productivity. With enhancement in sharing patient's data, such as his/her body temperature, blood sugar level, blood pressure, etc. with the doctor over the internet between the medical server and the RFID tag over a wireless channel. As the channel is public and wireless, any changes in the record can affect the medication and health of the patient [6]. This variation may occur due to the attack, which takes place on this public channel, from the unauthorized user. It causes leakage in the patient's data which has become one of the most challenging issues. An effective authentication protocol helps in preserving privacy in the RFID system [7]. Many protocols have been created to guarantee secure communication in the health care system [8], [9]. In this paper we use PUF function in creating a protocol which helps in securing the communication taking place over the insecure channel which have lower communication and computation cost as compared with the other protocols discussed in paper thereby practically implementing it for a secure communication. The Architecture for the RFID system consists of Tag, Reader and server The Tag and Reader communicating with each other over an insecure channel whereas the reader and server communicating with each other over a secure channel this is shown in Figure 1.

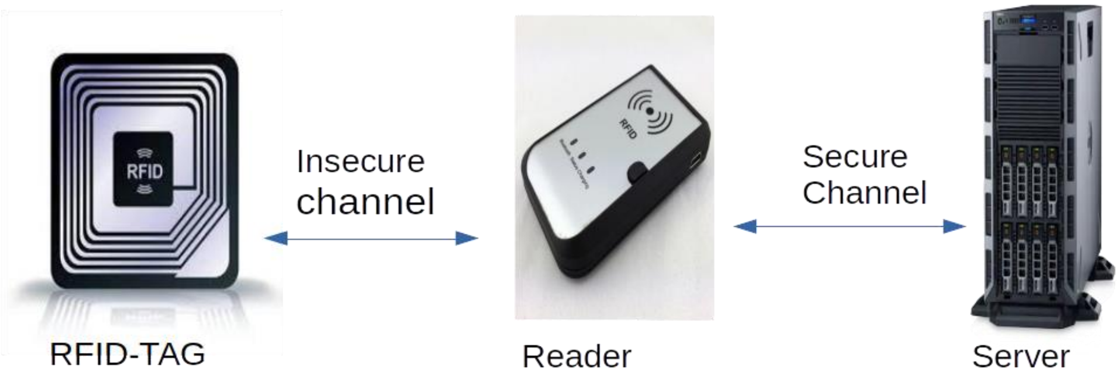


Figure 1 Architecture for an RFID Authentication Scheme

1.1 Privacy and security requirements

The requirements for secure communication between the reader, server, and tag are as follows:

Tag Anonymity

In the tag anonymity, the communicating tag should be anonymous, so the tag's identity is hidden from the outside world except for the reader, server. To prevent it from being forged.

Tag Privacy

In the entire communication, if the identity of the tag gets leaked, it is sure that the privacy is getting compromised and data communication is insecure and subjected to attack. So preserving tag privacy is one of our main criteria. In order to achieve integrity, we have to assure that during the communication between the tag and the reader server there should be no modification done during the transmission. This can be achieved by ensuring that the message has not been altered or tampered and ensuring that the received message is originated from the intended sender and was not modified.

Data secrecy

Data confidentiality or data secrecy is the property that the original plain text cannot be determined by the attacker who intercepts the cipher text of original message

Availability

The authentication must occur between the communicating entities. Achieving the availability property is the criteria. The information shared between the two entities must be updated; else it gets affected by various attacks by which the efficiency of the RFID gets affected.

Mutual Authentication

The mutual authentication between the two entities must be achieved. To identify that it is communicating with the genuine entity and not with the unauthorized entity.

Forward secrecy

Tracing the earlier information about the tag means compromising the tag's privacy and secrecy. By using the present tags, information should not lead that the previous tag information tracked down. So, Forward Secrecy should be a consideration which is the requirement.

1.2 Possible attacks in RFID systems

The various attacks which can take place in RFID systems are as follows:

Eavesdropping

In an eavesdropping attack, the attacker observes that information gets transferred among the two entities. It is a passive attack in which data modification does not take place

Man-in-the-middle attack

Man-in-the-middle attack refers to the method in which the data sent across the communication channel between the two entities gets intercepted by an unauthorized user by replacing the public key on-the-fly

Spoofing

When both the parties tag and reader server communicating across a communication channel. the tag meant for sending the message to the reader server, there is a chance that an unauthorized user was posing as reader server conversely reader server believes they received a message from the tag, there is a chance that an attacker was posing as tag this problem is referred to as spoofing

De-synchronization attack

An attacker would block the insecure communication channel. As a result, the key stored key in the tags, memory, and server would not be the same. To provide forward secrecy. The secret key in both the communicating entities must be updated. Because of the blocked channel, the communicating entities would not know that either of them had updated their secret keys. It is called a de-synchronization attack

Traceability attack

In this type of attack, the attacker would know the location of the Tag and be able to track down that genuine sender or the receiver of the message, the Tag which is involved in the communication hence the attack refers to a traceability attack.

Replay attack

In an insecure channel, the message received twice. A message received from the authentic communicating entity. And the other from the attacker. This leads to confusion for the receiving entity. To know the actual sender of the message, this is called a replay attack.

1.3 Our contribution

- We have taken into consideration the TMIS and used the PUF function for designing a protocol for the RFID system.
- The proposed protocol satisfies all the security requirements, as discussed in Section 5
- The security requirements have been simulated using the Scyther tool.
- The performance is found to be better than the existing protocols as compared in this paper.

1.4 Paper organization

The paper arrangement is as follows. Section 1 consists of the introduction and security requirements. Section 2 is composed of related work which describes the work of various authors with their protocols. Preliminaries and assumptions are provided in Section 3. Security and privacy analysis are in Section 4. Performance analysis is put forth in Section 5. The results of the simulation shown in section 6. The conclusion is present in Section 7.

II RELATED WORK

The various authentication protocols proposed are based on the NPK cryptosystem and PK cryptosystem. In contrast to the NPK cryptosystem-based keys whose performance, despite being better as no complex operations are needed. Such as the schemes proposed on non-public cyclic redundancy check[10]–[13], by using one-way hash function[14]–[19], bitwise operations[20], [21], an algorithm based on symmetric encryption[22] are proposed for various RFID-based authentication for management of goods, verification of identity, public security and administration of road traffic, and electronic health care. A PUF based key agreement scheme between the smart meters and service providers in AMI N/W has been proposed [23]. Gope et al. proposed a lightweight protocol by considering the ideal PUF environment for preserving privacy with the resistance of DoS attack that is practical[24]. He et al. proposed a protocol in which he discusses the requirements for the security of RFID authentication through the schemes by reviewing ECC-based RFID authentication in terms of security and performance[6]. Salem et al. proposed a protocol in which he uses Elgamal cryptosystem for increasing medication safety of patients in TMIS that can resist various attacks and achieve various security services[25]. The author proposed a protocol for authenticating users using the RSA algorithm in TMIS, which is identified to be unsafe for brute force techniques and privilege insider attacks. Amin et al. proposed a protocol to preserve user anonymity, claiming it to be secure against passive attacks and active attacks as well including man-in-the-middle attack and Replay attack[26]. In Sadeghi et al.'s protocol, he uses the PUF function for RFID authentication is identified by Kardas et al. to be subjected to a cold boot attack. The schemes are designed on the assumption of noise-resilient or Ideal PUF. Shariq and Singh proposed a protocol with a reduced computation cost using the basic mechanism of vector space and linear mapping to achieve privacy and security[27]. Dinarvand and Barati proposed a ECC based protocol satisfying the security requirements for the tag with limited resources[28]

III. PRELIMINARIES

3.1 System Model

The architecture of our system model for the healthcare comprises of a tag attached entity deployed with various sensors and a reader server which communicates with the tag. The tag sends the information of the patient such as blood pressure, body temperature, sugar levels, oxygen levels etc. to the reader server over the wireless channel. The reader server receives the information obtained from the tag and stores it in the database server. The health care personnel get to know the information of the patient by extracting it from the database server.

3.2 Adversary Model

According to the dolev-yao model[29], the communication occurring in between the tag and reader-server may be intercepted by the adversary, as the channel is wireless and assuming it to be insecure. The various threats such as eaves dropping, man-in-the-middle, spoofing, desynchronization and traceability etc. could occur due to which the secret information shared by the tag and the reader-server is subjected to be tampered by the adversary resulting in threat to the life of the patient in such a case.

3.3 Physically Unclonable Function

Physically unclonable function (PUF) provides hardware security as they are unclonable on micro scale. The main feature of PUF is that of its challenge-response pairs, where a single challenge when given as an input to two different PUF's deliver two different responses i.e. given a particular challenge we can use the response to identify the hardware depending on acceptance, PUF's are categorized into strong PUF and weak PUF. A strong PUF accepts many challenges in contrast to weak PUF which accepts only a single challenge. The main characteristics of PUF are 1) They offer low cost security 2) They are useful in authentication of devices and storing the secret keys. 3) They are sensitive to invasive attacks[30].

3.4 Assumptions considered

- The tag in an RFID system consists of a microcontroller attached to a Physically Unclonable Function (PUF). The tag uses the PUF function with the challenge and response pairs which are unique for every PUF. An attempt to modify the PUF will lead to change the way the tag works, finally the tag will turn worthless. The unique feature of the PUF is of its challenge c and Response R pair, where $R = PUF(C)$
- The tags in the RFID system have limited resources.
- The backend server doesn't have any such limitations.
- We assume (reader-server) to be a single unit.

IV PROPOSED PROTOCOL

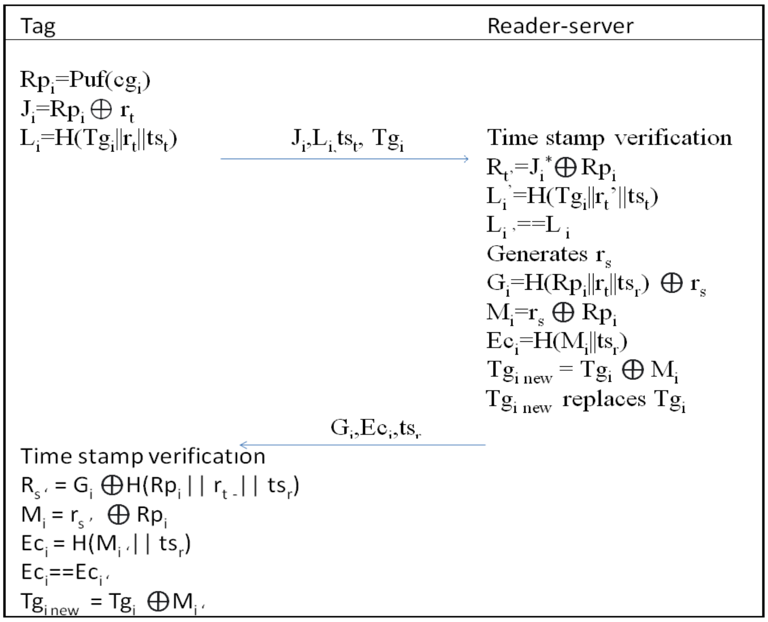


Figure 2.Proposed Protocol

4.1 Setup and registration of tag with reader-server

Initially the tag needs to be registered with the reader-server. Let IDibe the tag identity. The reader-server will generate the challenge Cgi , random number K$_i$, computes temporary identityTg$_i$=H(ID$_i$ || K$_i$) and sends $< Cgi, Tidi >$ to the tag via secure channel. Now, the tag will generate the response Rp$_i$=Puf (Cg$_i$) using the PUF embedded on it and sends it to the reader-server. Reader-Server will store in its memory$< IDi, Tgi, Cgi, Rpi >$. Tag will store in its memory $< IDi, Tgi, Cgi >$.

4.2 Mutual Authentication between tag and Reader-server

This section presents the mutual authentication and session key agreement between tag and reader-server

Step 1: Tag will generate a response Rp$_i$= PUF (Cg$_i$) by taking challenge Cg$_i$ as input to the. PUF embedded to it. Then the tag will generate a random number r$_t$ and computesJi = Rpi ⊕ rt, Li = H(Tgi || rt || tst). Now tag will send to reader-server the message $M1 =< Ji, Li, tst, Tgi >$ through public channel

Step 2: After receiving the M1, Reader-server will first perform time stamp verification. Then it will compute $rt' = ji'\oplus Rpi,Li' = H(Tgi||rt'||\ tst)$ and compares if $Li' = Li$. If the values match then reader- server will authenticate the tag and computes $gi = H(Rpi||rt||tsr)\oplus rs,Mi = rs\oplus Rpi\ and\ Eci = H(Mi||tsr), Tgnew = Tgi\oplus Mi$ and $Tgnew$ will replace Tgi when current session expires. Further reader-server will send the message $M2 =< gi, Eci, tsr >$ to tag through public channel.

Step3: After receiving the $M2$, the tag will first perform time stamp verification. Then it will compute $rs' = gi\oplus H(Rpi||rt||tsr, Mi' = rs'\oplus Rpi), Eci' = H(Mi'||tsr)$ and compares if $Eci' = Eci$. If the values match then tag will authenticate the reader-server and computes $Tginew = Tgi\oplus Mi'$ and $Tginew$ will replace Tgi when current session expires.

V SECURITY AND PRIVACY ANALYSIS

Theorem 1: The recommended protocol satisfies the Property of tag Anonymity.

Proof: In tag anonymity, the identity of the tag should be unidentified. This property stops the unauthorized user from an attack. In our proposed protocol, more than one session will have two different identities, and the identity goes on changing as the session does and hence our protocol provides the tag anonymity property.

Theorem 2: The recommended protocol satisfies the property of tag privacy.

Proof: As the Tgi is sent by the tag to the server, along with the other parameters. The reader-server on receiving the identity changes it to a new identity as $Tginew = Tgi\oplus Mi$, where Mi is difficult to be known, and this $Tginew$replaces the Tgi when the current session expires, and hence our protocol satisfies the tag privacy property.

Theorem3: The recommended protocol satisfies the property of tag availability

Proof: The challenge cgi and response Rpi pairs are unique for each tag. It is easy to identify the tag for the authorized user after the protocol has been successfully executed, as the calculated response $Rpi = PUF(cgi)$. Due to availability property, we can claim the tag to be legitimate by the challenge and response pairs discarding the cloned tag claiming it to be legitimate. Hence our proposed protocol provides availability property.

Theorem 4: The recommended protocol is safe from the replay attack.

Proof: Replay attack causes the same message to be sent twice, one from the authorized user and the other from the attacker. As the tag communicates with the reader-server it sends the data with a time stamp tst to the reader-server. The tag calculates $Li = H(Tgi||rt||tst)$ and sends to the reader server if, an attacker knows the other parameter and sends a false message to the reader-server. The reader-server calculates $Li' = H(Tgi||rt'||tst)$. The change in timestamp leads to acceptance of only the authentic tags data where the false message from the unauthorized user is not accepted by the reader-server. And hence the protocol is safe against replay attack.

Theorem 5: The recommended protocol is safe from tag impersonation.

Proof: PUF generates a response on the fly. Even if a challenge is impersonated, it is hard to know the response. The challenge-response pair is unique for each tag. Even if the challenge is impersonated, the PUF produce a different response, and hence, as Rpi is not the same, the Ji calculated differs from that of the actual tag. And hence the tag impersonation is not possible

VI PERFORMANCE ANALYSIS

Function	EAP		ESAP		Our Protocol	
	T	S	T	S	T	S
Modular Exponentiation	2	1	0	0	0	0
Hash Function	2	2	0	0	3	3
Scalar Multiplication	0	0	3	3	0	0
Modular Multiplication	1	1	0	0	0	0
Multiplicative Inverse	0	1	0	0	0	0
PUF Function	0	0	0	0	1	0

Table 1 Complexity Comparision

The computation cost for hash function, PUF function, modular exponentiation, modular multiplication are 0.00032, 0.00012, 0.0192, 0.000015 seconds respectively[25], [31]. Hence the total computation cost of our protocol is 0.00204 seconds where as that of fatty Salem's is 0.07811 seconds[25] and for Dinarvand it is 0.04416 seconds[28]. The communication cost for the tag identity is 128 bits, time stamp tst is 32 bits, hash function-256 bits, PUF Function-128 bits,Ji-128 bits $Li - 256$bits,$Gi - 256$ bits, $Eci - 256$bits, time stamp of reader server tsr is 32 bits and the total communication cost is 1088 bits.

6.1 Computation cost comparison with various protocols

The cost for computation of the recommended protocol is found to be very low when compared to that of fatty Salem[25] and Dinarvand et al. protocols[28]. Hence, our protocol is suitable to design a protocol for RFID system for the Healthcare domain.

Protocol	Total computation cost
EAP[25]	0.07811
ESAP[28]	0.04416
Our protocol	0.00252

Table 2 Computation Cost Comparision with various protocols

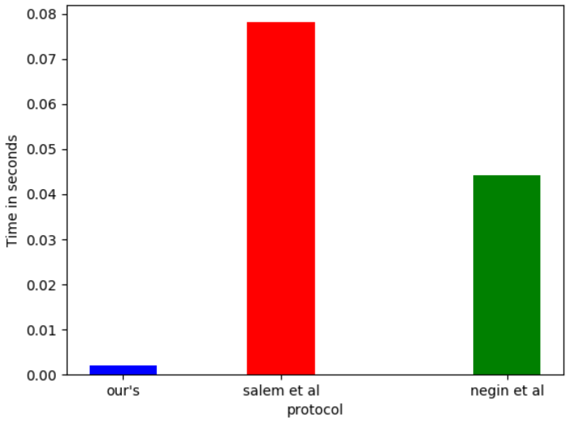


Figure 3 Computation Cost

6.2 Communication cost comparison with various protocols

The cost of communication is calculated based on the number of messages transferred between the two communicating entities and the total number of bits used. The communication cost of our protocol is 1088 bits compared to other protocols where the communication cost of other protocols is above 2000 bits. The total number of messages transferred from Salem et al. protocol is 3 messages[25]. For Dinarvand et.al. it is 4 messages[28], and for ours it is 3 messages. Hence our protocol has a low communication cost that is total number of messages transferred between the communicating entities and the total number of bits used is low and hence our protocol is suitable to design a protocol for RFID system for healthcare. This demonstrated using Fig.4.

Protocol	No. of messages exchanged	Total no. of bits
EAP[25]	3	4256
ESAP[28]	4	1440
Our Protocol	2	1088

Table 3 Communication Cost Comparision with various Protocols

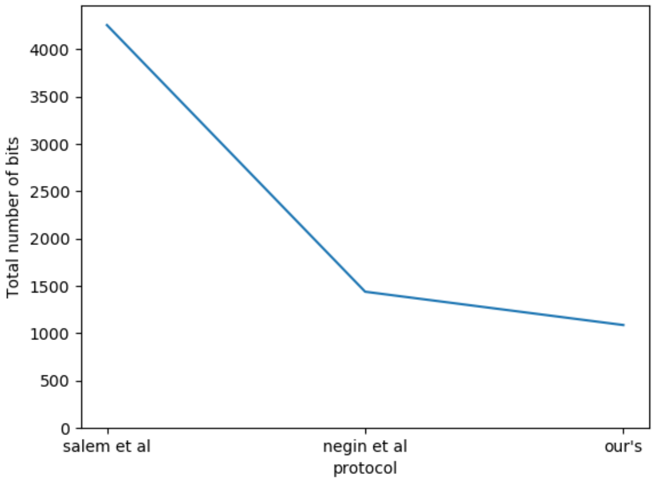
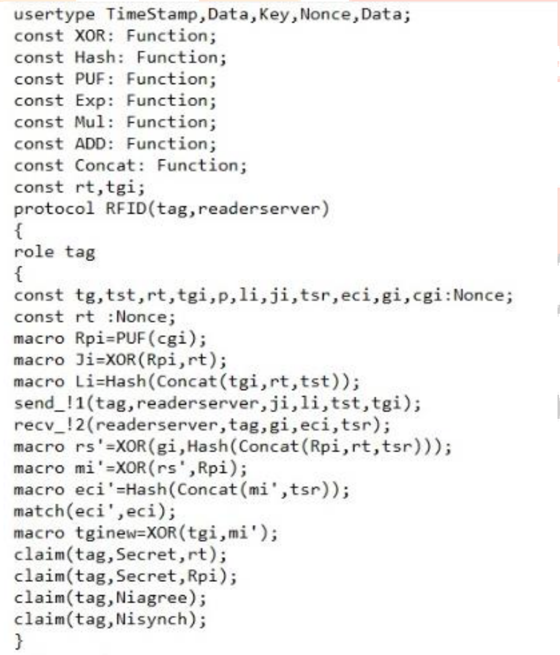
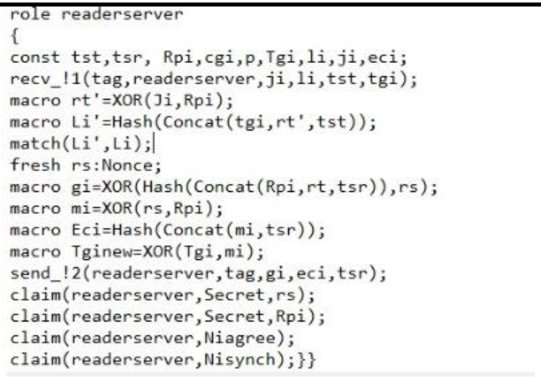


Figure 4 Communication Cost



```
usertype TimeStamp,Data,Key,Nonce,Data;
const XOR: Function;
const Hash: Function;
const PUF: Function;
const Exp: Function;
const Mul: Function;
const ADD: Function;
const Concat: Function;
const rt,tgi;
protocol RFID(tag,readerserver)
{
role tag
{
const tg,tst,rt,tgi,p,li,ji,tsr,eci,gi,cgi:Nonce;
const rt :Nonce;
macro Rpi=PUF(cgi);
macro Ji=XOR(Rpi,rt);
macro Li=Hash(Concat(tgi,rt,tst));
send_!1(tag,readerserver,ji,li,tst,tgi);
recv_!2(readerserver,tag,gi,eci,tsr);
macro rs'=XOR(gi,Hash(Concat(Rpi,rt,tsr)));
macro mi'=XOR(rs',Rpi);
macro eci'=Hash(Concat(mi',tsr));
match(eci',eci);
macro tginew=XOR(tgi,mi');
claim(tag,Secret,rt);
claim(tag,Secret,Rpi);
claim(tag,Niagree);
claim(tag,Nisynch);
}
```

Figure 5 SPDL Code For Tag

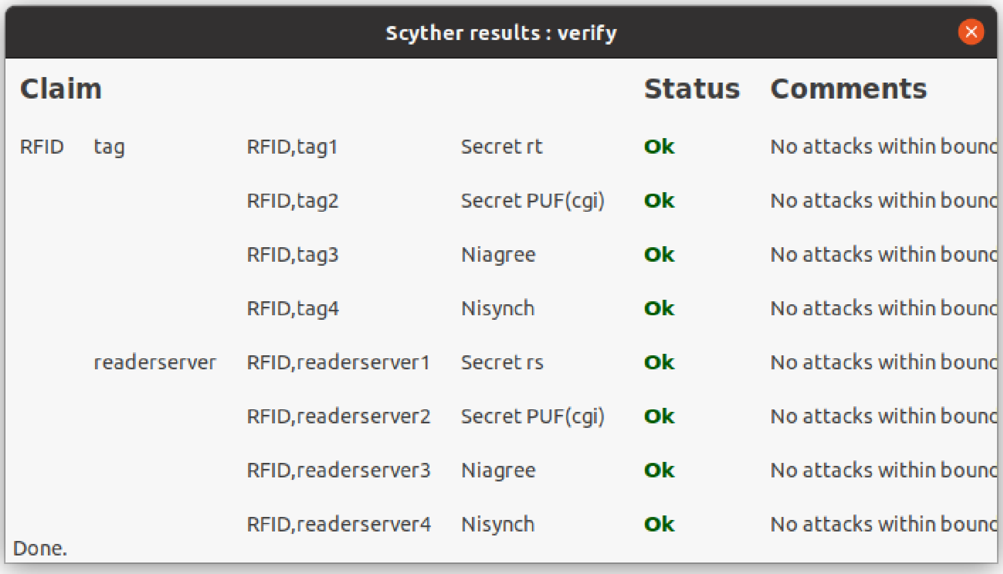


```
role readerserver
{
const tst,tsr, Rpi,cgi,p,Tgi,li,ji,eci;
recv_!1(tag,readerserver,ji,li,tst,tgi);
macro rt'=XOR(Ji,Rpi);
macro Li'=Hash(Concat(tgi,rt',tst));
match(Li',Li);|
fresh rs:Nonce;
macro gi=XOR(Hash(Concat(Rpi,rt,tsr)),rs);
macro mi=XOR(rs,Rpi);
macro Eci=Hash(Concat(mi,tsr));
macro Tginew=XOR(Tgi,mi);
send_!2(readerserver,tag,gi,eci,tsr);
claim(readerserver,Secret,rs);
claim(readerserver,Secret,Rpi);
claim(readerserver,Niagree);
claim(readerserver,Nisynch);}}
```

Figure 6 SPDL Code for Reader Server

VII SIMULATION RESULTS USING SCYTHER TOOL

Scyther tool is used for verification of security protocol. The tool uses the the Dolev-Yao model as the adversary model and hence is more useful in automatic verification of protocols. Our protocol is simulated using the Scyther tool, which is a formal security evaluation tool to check against possible attacks. We have two entities namely Tag and reader-server. $rt \oplus Rpi$ and rs are secret parameters, after the security evaluation is performed between these two entities the above parameters are verified to be secret and hence there are no attacks within the bounds. The unauthorized user cannot access these parameters. Our protocol is assumed to be safe from all the attacks. The SPDL code for the tag and the reader-server unit are shown in Figure 5 and Figure 6 respectively and the output generated is shown in Figure 7.



Scyther results : verify

Claim				Status	Comments
RFID	tag	RFID,tag1	Secret rt	Ok	No attacks within bound
		RFID,tag2	Secret PUF(cgi)	Ok	No attacks within bound
		RFID,tag3	Niagree	Ok	No attacks within bound
		RFID,tag4	Nisynch	Ok	No attacks within bound
	readerserver	RFID,readerserver1	Secret rs	Ok	No attacks within bound
		RFID,readerserver2	Secret PUF(cgi)	Ok	No attacks within bound
		RFID,readerserver3	Niagree	Ok	No attacks within bound
		RFID,readerserver4	Nisynch	Ok	No attacks within bound

Done.

Figure 7 Scyther Simulation result

VIII CONCLUSION

A lightweight protocol that is secure against the various attacks has been proposed using PUF and is evaluated to be safe from the attacks. The analysis performed shows that the recommended protocol is safe even if the attacker gets the RFID tag physically. The tag doesn’t need to store the secret keys. The performance analysis shows that the communication and computation costs are low when compared to another RFID- based protocol and hence our protocol is much suitable to design a secure RFID system for healthcare. The protocol is tested for the attacks using the Scyther model checker and have found that there are no attacks within bounds and thus being with low computation and communication cost it can be implemented in devices with low storage, low processing speed and low memory capacity which helps in a secure communication in the insecure communication channel in the RFID architecture system

REFERENCES

[1] Z. Zhu, "An efficient authentication scheme for telecare medicine information systems," *J. Med. Syst.*, vol. 36, no. 6, pp. 3833–3838, 2012.

[2] R. Weinstein, "RFID: a technical overview and its application to the enterprise," *IT Prof.*, vol. 7, no. 3, pp. 27–33, 2005.

[3] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," *Comput. networks*, vol. 54, no. 15, pp. 2787–2805, 2010.

[4] D. C. Ranasinghe, M. Sheng, and S. Zeadally, "Unique radio innovation for the 21st Century: building scalable and global RFID networks," 2010.

[5] P. Najera, J. Lopez, and R. Roman, "Real-time location and inpatient care systems based on passive RFID," *J. Netw. Comput. Appl.*, vol. 34, no. 3, pp. 980–989, 2011.

[6] D. He and S. Zeadally, "An analysis of RFID authentication schemes for internet of things in healthcare environment using elliptic curve cryptography," *IEEE internet things J.*, vol. 2, no. 1, pp. 72–83, 2014.

[7] F. Furbass and J. Wolkerstorfer, "ECC processor with low die size for RFID applications," in *2007 IEEE International Symposium on Circuits and Systems*, 2007, pp. 1835–1838.

[8] G. Gaubatz, J.-P. Kaps, E. Ozturk, and B. Sunar, "State of the art in ultra-low power public key cryptography for wireless sensor networks," in *Third IEEE International Conference on Pervasive Computing and Communications Workshops*, 2005, pp. 146–150.

[9] H.-Y. Chien and C.-H. Chen, "Mutual authentication protocol for RFID conforming to EPC class 1 generation 2 standards," *Comput. Stand. \& Interfaces*, vol. 29, no. 2, pp. 254–259, 2007.

[10] D. N. Duc, J. Park, H. Lee, and K. Kim, "Enhancing security of EPCglobal Gen-2 RFID tag against traceability and cloning," in *SCIS 2006*, 2006, p. 97.

[11] A. Juels, "Strengthening EPC tags against cloning," in *Proceedings of the 4th ACM workshop on Wireless security*, 2005, pp. 67–76.

[12] T.-C. Yeh, Y.-J. Wang, T.-C. Kuo, and S.-S. Wang, "Securing RFID systems conforming to EPC Class 1 Generation 2 standard," *Expert Syst. Appl.*, vol. 37, no. 12, pp. 7678–7683, 2010.

[13] P. Peris-Lopez, J. C. Hernandez-Castro, J. M. Estévez-Tapiador, and A. Ribagorda, "LMAP: A real lightweight mutual authentication protocol for low-cost RFID tags," in *Proc. of 2nd Workshop on RFID Security*, 2006, vol. 6.

[14] H.-Y. Chien, "Secure access control schemes for RFID systems with anonymity," in *7th International Conference on Mobile Data Management (MDM'06)*, 2006, p. 96.

[15] J. Lim, H. Oh, and S. Kim, "A new hash-based RFID mutual authentication protocol providing enhanced user privacy protection," in *International Conference on Information Security Practice and Experience*, 2008, pp. 278–289.

[16] A. X. Liu and L. A. Bailey, "PAP: A privacy and authentication protocol for passive RFID tags," *Comput. Commun.*, vol. 32, no. 7–10, pp. 1194–1199, 2009.

[17] S.-Y. Kang, D.-G. Lee, and I.-Y. Lee, "A study on secure RFID mutual authentication scheme in pervasive computing environment," *Comput. Commun.*, vol. 31, no. 18, pp. 4248–4254, 2008.

[18] J.-S. Cho, S.-S. Yeo, and S. K. Kim, "Securing against brute-force attack: A hash-based RFID mutual authentication protocol using a secret value," *Comput. Commun.*, vol. 34, no. 3, pp. 391–397, 2011.

[19] A. Juels, D. Molnar, and D. Wagner, "Security and privacy issues in e-passports," in *First International Conference on Security and Privacy for Emerging Areas in Communications Networks (SECURECOMM'05)*, 2005, pp. 74–88.

[20] P. Peris-Lopez, J. C. Hernandez-Castro, J. M. Estevez-Tapiador, and A. Ribagorda, "EMAP: An efficient mutual-authentication protocol for low-cost RFID tags," in *OTM Confederated International Conferences" On the Move to Meaningful Internet Systems"*, 2006, pp. 352–361.

[21] S. A. Weis, S. E. Sarma, R. L. Rivest, and D. W. Engels, "Security and privacy aspects of low-cost radio frequency identification systems," in *Security in pervasive computing*, Springer, 2004, pp. 201–212.

[22] M. Burmester, B. De Medeiros, and R. Motta, "Robust, anonymous RFID authentication with constant key-lookup," in *Proceedings of the 2008 ACM Symposium on information, Computer and Communications Security*, 2008, pp. 283–291.

[23] M. Tahavori and F. Moazami, "Lightweight and secure PUF-based authenticated key agreement scheme for smart grid," *Peer-to-Peer Netw. Appl.*, vol. 13, pp. 1616–1628, 2020.

[24] P. Gope, J. Lee, and T. Q. S. Quek, "Lightweight and practical anonymous authentication protocol for RFID systems using physically unclonable functions," *IEEE Trans. Inf. Forensics Secur.*, vol. 13, no. 11, pp. 2831–2843, 2018.

[25] F. M. Salem and R. Amin, "A privacy-preserving RFID authentication protocol based on El-Gamal cryptosystem for secure TMIS," *Inf. Sci. (Ny).*, vol. 527, pp. 382–393, 2020.

[26] R. Amin and G. P. Biswas, “An improved rsa based user authentication and session key agreement protocol usable in tmis,” *J. Med. Syst.*, vol. 39, no. 8, pp. 1–14, 2015.

[27] M. Shariq and K. Singh, “A novel vector-space-based lightweight privacy-preserving RFID authentication protocol for IoT environment,” *J. Supercomput.*, vol. 77, pp. 8532–8562, 2021.

[28] N. Dinarvand and H. Barati, “An efficient and secure RFID authentication protocol using elliptic curve cryptography,” *Wirel. Networks*, vol. 25, no. 1, pp. 415–428, 2019.

[29] D. Dolev and A. Yao, “On the security of public key protocols,” *IEEE Trans. Inf. theory*, vol. 29, no. 2, pp. 198–208, 1983.

[30] C. Herder, Y. Meng-Day, F. Koushanfar, and D. Srinivas, “Physical Unclonable Functions and Applications: A Tutorial,” *Proc. IEEE*, vol. 102, no. 8, pp. 1126–1141, 2014.

[31] Y. Guo, Z. Zhang, and Y. Guo, “Fog-centric authenticated key agreement scheme without trusted parties,” *IEEE Syst. J.*, 2020.