Grenze International Journal of Engineering and Technology, Special Issue

An RFID-based Authentication Protocol for IoT Healthcare Environment

Mohd. Shariq[1], Karan Singh[2,] and Manisha Manjul[3]
[1-2]School of Computer and Systems Sciences, JNU, New Delhi, India
Email: {shariq99ansari, karancs12}@gmail.com
[3]CSE, G. B. Pant Government Engineering College, New Delhi, India
Email: manishamanjul@gmail.com

***Abstract*—Over the past years, the data related to traditional medical privacy and many other similar cases are at a serious risk of disclosure by the third party or it may be an adversary or an attacker. For instance, there is some probability of leakage the personal medical privacy data by some insurance companies, which can also disrupt the healthy environment of medical industries as well as compromise the privacy of individuals. With the continuous growth ofsometechnologies likebig data and cloud computing, the Internet of Things (IoT) has become more and more popular that provides interaction between physical devices and cyber world over the internet without any need for human intervention. On the other hand, RFID is one of the core identification technology which comes under the IoT environment as well as has a paradigm in the various fields of healthcare system. In this research, we wish to design an RFID-enabled authentication scheme in healthcare field that provides better and efficient medical privacy protection in IoT with low cost, prevents various kinds of security threats, and reduces the performance overhead.**

***Index Terms*— IoT, RFID, Healthcare, Authentication, Privacy.**

I. INTRODUCTION

The term IoT stands for Internet-of-Things and behaves as an umbrella keyword that covers many aspects related to the extension of the internet.Over the last several years, the vast development of "Internet-of-Things" has grown up more and more in a variety of ways as well as a number of benefits have also given to society.

In healthcare regards, patient medication safety is a major concern for global public health. According to the official statistics, due to the improper identification of the patients, there are becoming more mistreatments in the healthcare systems. After considerations these issues, to overcome the aforementioned medical errors, the RFID technology makes an important contribution in the field of medical healthcare system for assets tracking and information tracking of patients [1]. Some of the RFID-enabled healthcare applications such as patient's identification, asset tracking, access control, location tracking, and many others are shown in Figure 2.

Even though, the RFID technology helps to provide various advantages over healthcare industries such as cost-saving, safety enhancement, and high operational efficiency. Apart from security and privacy, the risks

Grenze ID: 01.GIJET.6.2.504

associated with human safety are the foremost barriers to adopting this technology [2, 3].
RFID-enabled technology is the most promising and contactless technology which is used to identify objects by using radio frequency (RF) waves. More precisely, the growing popularity of this technology because of its ease to use and makes convenience as well as low-cost. Moreover, in recent years, the widespread use of this technology in various real-life applications like supply chain management, logistic, access control, e-health system, internet-of-vehicles, automatic toll collection, e-passport and many other applications [4, 5].
More specifically, the RFID system is a composition of some entities such as the tag, reader, and a backend server.In this context, the RFID tags arealso said to be transponder and made up of silicon material, also stores the information related to that object or attached with the particular object. Although the tags consist of two components namely an integrated circuit and an antenna. Consequently, the integrated circuit is used to store and process the data whereas an antenna is also used to transmits and receives the signal corresponding to the reader or the backend server. Moreover, the tags basically used a power system that helps to provide the energy for its operation. In this way, the working operation on the RFID system is described step-by-step in Figure 1 as shown below. Further,the RFID tags are categorized into three types of tags based on their different characteristics: active tags, semi-active tags, and passive tags. Moreover, most of the RFIDtags are being used every day in ourdaily lives. However, the passive tags are quite cheaper as compare to active tagsbecause these tags do not have any battery to get the power and charged with the help of radiofrequency (RF) waves from the RFID reader. On the other hand, the active tags get power and charged with their own battery or energy sources and transmit signals periodically, even semi-active tags get power and charged with their internal energy sources or own battery. In addition, the passive tags have read-only capability on tags whereas the active and the semi-active tags have both read/write capability.
In order to that, the RFID readercontains mainly three components such as RF signal generator, microcontroller, and receiver or signal detector. Besides, the RF signal generator helps to generate the radio frequencies waves which are transmitted through an antenna and also it receives the feedback signal which comes from the tags.In particular, the receiver or a signal detector further proceeds the information that is sent by the RFID tags. Accordingly, the main role of the backend server is to stores the specific information of an objects in its database which is sent by the reader and also performs the high-load computations.

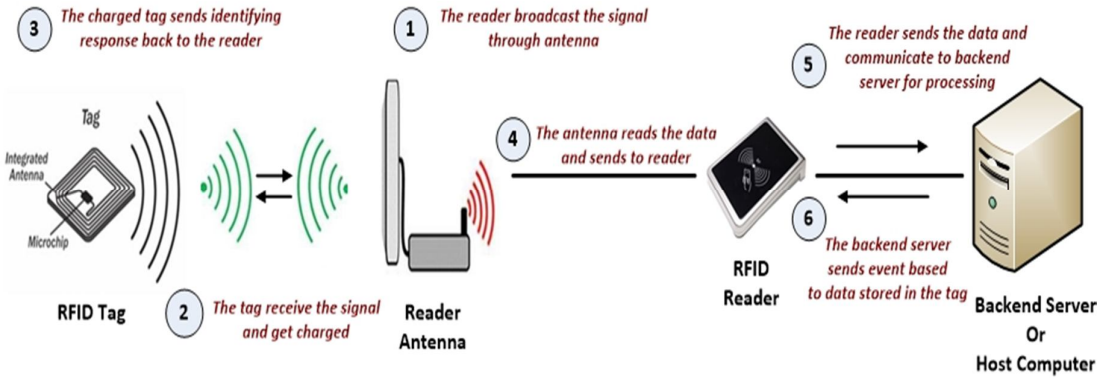

Figure 1. Typical architecture of an RFID system

II. Related Work

After an extensive study of the various literature reviews related to healthcare system, we got a great inspiration to design a lightweight privacy protection RFID authentication scheme that can beemployed in healthcare system and which ensures the various imperative security requirements such as the resistance to DoS attack, the location privacy attack, the replay attack, untraceability, and anonymity, etc.
In 2014, Zhenguo Zhao[6] proposed a secure RFID authentication scheme based on elliptic curve cryptography (ECC) that can be appliedin telecare medical information systems (TMIS). In addition, this scheme ensures that the protocol is safe under some kinds of security attacks and more reliable for healthcare systems. Although the authorsshowed that their scheme is secure against the forward untraceability and more suitable for healthcare environments. However, in 2016, Farash et al. [7] foundZhenguo Zhaoscheme shows the security weakness against forward untraceability.

Xie et al. [8] presented an RFID authentication scheme based on the cloud server. Unfortunately, this scheme shows the security weakness against location tracking attacks, invasion of data privacy, andreader impersonation attacks. In order to fix the shortcomings of Xie's scheme, Abughazalah et al. [9] presented an improved version of a new RFID authentication scheme based on cloud that achieves the data secrecy and the mutual authentication. Moreover, this scheme also has good performance for storage and scalability.

In respect ofthe healthcare IoT environment, He and Zeadally [10] show a complete security and performance analysis of various RFID authentication schemes based on ECC techniques. Furthermore, the IoT application brings a lot of changes such as convivence to physicians and patients in several medical fields, for instance, real-time monitoring, patient's medication records, blood bank management,patients information management, medical emergency management, and many others. In addition to that, usually cryptographic ECC tool is used to achieves better security privacy and performance requirements. In 2018, Wazid et al. [11] shows the weakness of their scheme that is cannot support to dynamic implantable medical devices (IDMs) which are used to implant in the human body for improving some functionalities of many organs, for instance, an insulin pump is used in human body for monitoring the level of blood pressure.

In 2017, Rahman et al. [12] proposed a framework related to privacy-preserving for RFID based healthcare environments to fulfills the various typical security requirements. Furthermore, there are two major concerns for privacy-preserving that shows an important paradigm in the RFID-enabled healthcare environment. In this way, the primary concern describes an RFID authentication protocol which preserves the privacyfor monitoring purpose and sensing RFID tags for different ways of identification.Despite the first one, the secondary concern describes, during providing the healthcare services with the help of tag ID, privacy preserving access control system is needed to prevent the unauthorized access of the secret information. Despite such privacy concerns, the framework solves the trade-off problem between privacy and scalability in the RFID systems. According tothe authors, data security, privacy, and access,these are the paramount factors of RFID adoption in the healthcare systems.

In 2018, Chiou and Chang [13] proposed an enhanced authentication approach for anRFID system and that can be also employed in the mobile RFID system. The main feature of this scheme is to provide security in mobile devices, mobile RFID systems, and make it more efficient and convenient for the wireless environment. Also, the scheme can be successfully employedin mobile devices that show proof of using mobile or wireless RFID systems. Moreover, the secure channel is not required in this scheme as well as the Electronic Product Code (EPC) Class-1 Gen-2 standards also. In addition to that, the scheme holds some security requirementsnamely the resistance against replay attacks, the desynchronization attacks, and the reader tracking attacks. Unfortunately, Priyanka and Turuk [14] claim that the high computational cost does exist in Rahman et al.'s scheme.

In 2018, Fan et al. [15] introduced a lightweight RFID scheme employed in the IoT environment for protecting the medical privacy of the stored information. However, the author ensures that their schemeprovidesresistance against various typical attacks named as a replay attack, synchronization attack, and anti-Denial-of-service (anti-DoS) attack. Subsequently,Aghili et al. [16] pointed out that their protocol cannot withstand some serious vulnerabilities such as the tag traceability attack, the secret disclosure attack, and the reader impersonation attack. Also, their scheme does not preserve anonymity of the reader as well as the tag.

In 2019, Aghili et al. [16] presented an improvement in Fan's et al. protocol named secure LRAP protocol also known as SecLAP. Unfortunately, Safkhani et al. [17] show the security weakness of Aghili et al.'s protocol i.e., SecLAP cannot withstand the partial secret disclosure attack, the full secret disclosure attack, and the traceability attack. In addition to that, the privacy of the tags and the readers is compromised by the disclosed parameters.

Typically, the main objective of an RFID system is to ensure the authentication and integrity of the system. More specifically, the privacy-preserving of the tags must be satisfied.

Security Ensures that the rejection of involving fake RFID tags and identify the counterfeit tags during communication with the reader.

Privacy Ensures that the privacy protection of valid or legitimate tags during communication with the reader.

III. Proposed Protocol

In the protocol designing section, we introduced a new scheme an RFID-based scheme for IoT healthcare which integrates the concept of secure cryptographic HMAC(.) function. However, there are basically two phases of the designed scheme namely the pre-setup and the mutual authentication phase as shown in Figure

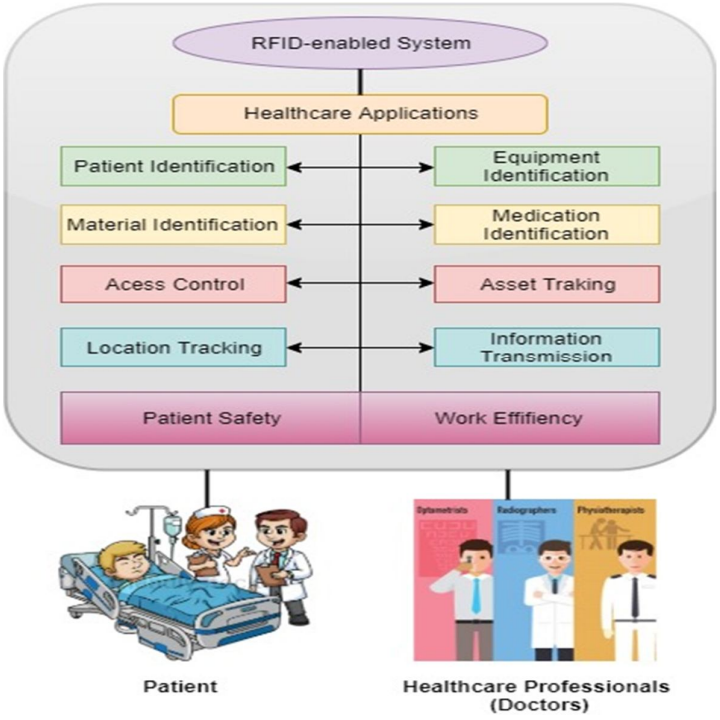

Figure 2. RFID-enabled healthcare applications

3 and Figure 4 respectively. Some notations are used to design the proposed authentication protocol given in Table I.

A. Assumptions Considered

There are being used some considerations for designing the proposed authentication scheme.

- HMAC(.) function is considered asrobust.
- The communication channel is secure between the reader and the backend server.
- The communication channel is insecure between the tag and reader.

B. Pre-setup Phase

In the pre-setup phase, backend server makes a selection of three secret shared keys denotes as the square binary matrices of order $n \times n$ namely key_1, key_2, and key_3, where key_1 defined as non-singular matrix and key_2 as a singular matrix. On the other hand, for each tag, the server generates two matrix keys defined as K_{t_1}=$key_1 key_3 S_t$ and K_{t_2}=$key_2 key_3 S_t$, where S_t represents a $n \times n$ size random matrix. Accordingly, an identification number ID for each tag, stored by the server. Subsequently, the identification number ID for each tag stored at database corresponding the matrix K_{t_2}.

Figure 3.Pre-setup phase

C. Authentication Phase

The following execution steps of the designed scheme are as given below:

- The first step states thatthe reader randomly generates a random number R_r, and also sends an authentication query *Query* and R_r to the tag.
- The second step states thatafter receiving the authentication query*Query*, the tag generates a random number R_t and subsequently computes $V_1 = K_{t_1}R_t$ and $V_2 = K_{t_2}R_t \oplus ID$. After that, the tag computes $V_3 = HMAC_{ID}(V_1 \parallel K_{t_2}R_r)$. At last, the tag sends the computed messages V_1, V_2 and V_3 to the reader. Then the reader includes the value of R_r with received response messages V_1, V_2 and V_3 and again sendsit to the backend server.
- The third step states thatupon receiving the response messages V_1, V_2 and V_3 from the reader, the backend server computes$V_4 = key_2 key_1^{-1} * V_1$, which is equal to $K_{t_2}R_t$, extracts ID' by computing $ID' = V_4 \oplus V_2$ and subsequently verifies the corresponding matrix key K'_{t_2} verifies the response message V_3 by using $V'_3 = HMAC_{ID'}(V_1 \parallel K'_{t_2}R_r)$. If $V'_3 ?= V_3$ holds, then the backend server believes that the received message V_3 is sent by a legitimate tag. Otherwise,the server restarts or terminate the communication by the reader.
  Further, the server computes $V_5 = HMAC_{ID'}(V_4)$ and send it to the tag.
- The fourth step states thatupon receiving the response message V_5, tag computes$V'_5 = HMAC_{ID}(K_{t_2}R_t)$. If $V'_5 ?= V_5$ holds, then the backend server authenticates the tag otherwise not.

TABLE I. LIST OF SYMBOLS AND THEIR DESCRIPTION

Symbols	Description
$\mathcal{T}$	Denotes the RFID tag
$\mathcal{R}$	Denotes the RFID reader
BS	Denotes the backend server
ID	Denotes the unique tag's identification number
R_t	Denotes the random number generated at tag
K_t	Denotes the shared key of $\mathcal{T}$ generated by BS
Key	Denotes the shared key of BS
R_r	Denotes the random number generated at reader
$HMAC(.)$	Denotes the secure cryptographic keyed-hash/hash-based message authentication code function
$\parallel$	Denotes the concatenation operation
$\oplus$	Denotes the simple bitwise $EX-OR$ operation
?=	Denotes the comparison operator whether two values are equal

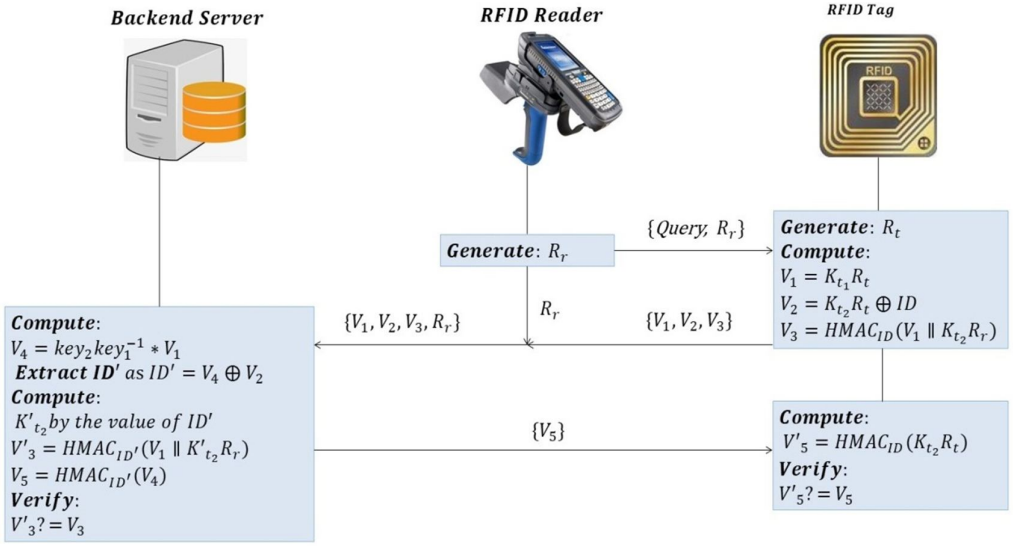

Figure4.Proposed protocol

IV. Analysis And Evaluation

In this part, we make a security and privacy comparative analysis of our newly designed scheme with some typicallyrelated RFID authentication schemes.

A. Security and Privacy Analysis

- *Mutual authentication resistance:* There are considered to be both of the communication channels between the reader and the server as well as the tag and the server should provide guaranteed secure authentication. Moreover, when the reader sends a random number R_r to the tag then the tag computes the values of V_1, V_2 and V_3. In order to that, the tag sends those values to the backend server along with R_r. In this way, the reader authenticates the server by verifying ${V'}_3 \stackrel{?}{=} V_3$ when it receives V_3 from the reader, while the server authenticates the tag by verifying ${V'}_5 \stackrel{?}{=} V_5$ when it receives V_5 from the server. Therefore, the mutual authentication exists in the designed scheme.
- *Traceability attack resistance:* In our protocol, the adversary could not eavesdrop the exchange messages during the execution of the designed scheme between the tag, reader, and backend server. So, our designed scheme demonstrates the security against traceability attack.
- *Secret disclosure attack resistance:*In particular, the main purpose of this attack is to recover the secret key shared between the RFID system entities (the tag, reader, and backend server). In our protocol, the adversary could not eavesdrop the transmitted messages during the execution. Also, the secret shared cannot be obtained by the adversary. So, our scheme achieves the security against secret disclosure attack.
- *Scalability:* The backend server only executes one time matrix multiplication $key_2 key_1^{-1} * V_1$, and one time bitwise EX-OR operation on V_2 and V_4 such that $(V_4 \oplus V_2)$ to get the identification number of the tag (tag's identifier). To maintain the scalability property, the backend server finds a match record from its database torecognize and authenticates the tag in the RFID system. In this way, our designed scheme ensures scalability property.
- *Tag and reader impersonation attack resistance:*The adversary has an ability to compute such response messages V_1, V_2 and V_3 to impersonate both the tag and the reader. But it is quite difficult to compute the above messages without knowing of ID and K_t.

TABLE II. Security And Privacy Comparision

Protocol→ ↓	Xie et al. [8]	Abughazalah et al. [9]	Fan et al. [15]	Aghili et al. [16]	Our Protocol
Mutual authentication	✗	✓	✓	✓	✓
Traceability attack resistance	✗	✗	✗	✓	✓
Secret disclosure attack resistance	✗	✗	✗	✗	✓
Tag impersonation attack resistance	✓	✓	✓	✓	✓
Reader impersonation attack resistance	✗	✓	✗	✓	✓
Scalability	✗	✗	✗	✗	✓

B. Performance Analysis

In regards to an RFID system, the tags have limitations of computational capability and memory in comparison to the reader and the backend server. After all, it is essential that besides security, any designed scheme has consideration for the RFID system to show the performance overhead in terms of computational operations and communication cost as shown in Table III, where L is denoted as the length of communicated data.

Furthermore, we make a comparative analysis of the designed scheme namely an RFID-based authentication protocol for IoT healthcare environment with the previous related RFID authentication schemes. In addition, "$\wedge$" represents the bitwise ANDoperation, "$\vee$" reparents bitwise OR operation,"$\oplus$"represents bitwise$Ex-OR$,"Cro" representsthe cross operation, "Rot" reparents rotation operation, and modular rotate function represented as $MRot_K(x, y)$, where K represents the key.On comparing with some related schemes, our designed scheme shows outstanding performance with respect to communication consumption.

TABLE III. PERFORMANCE COMPARISION

Protocol→ ↓	**Xie et al. [8]**	**Abughazalah et al. [9]**	**Fan et al. [15]**	**Aghili et al. [16]**	**Our Protocol**
Communication cost	$8L$	$7L$	$8L$	$9L$	$3L$
Computation operations	$\oplus, \|\|, Hash$	$\oplus, \wedge, \|\|, Hash$	$\oplus, \|\|, Cro, Rot$	$\oplus, \|\|, Cro, Rot, MRot_K(.,.)$	$\oplus, \|\|, HMAC(.)$

V. CONCLUSIONS

As we all knowbetter, IoT is a wide domain which contains lots of promising technologies, whereas RFID is one of the core identification technology which comes under IoT environment as well as it has a paradigm in the various fields of healthcare system. With the rapid development of medical technologies, there is an essential need to deploy more and more privacy associated with medical data. This paper presents a secure RFID-based authentication protocol for the IoT healthcare environment that ensures some security and privacy features, less communication cost, and less computational operationsas comparedto many other existing schemes.In order tothe medical environment, an RFID system receives more and more attention for security purposes.

In future studies, we will focus to implement our scheme on the real world RFID healthcare applications and also ensures the optimum consumption during the communication performance.

ACKNOWLEDGMENT

This work was supported by the project entitled “Development of Intelligent Device for Security Enhancement (iEYE)” with sanction order: DST/TDT/DDP-12/2017-G, under the guidance of Dr. Karan Singh, Assistant Professor, SC&SS, JNU, New Delhi.

REFERENCES

[1] Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. Computer networks, 54(15), pp. 2787-2805.

[2] Yao, W., Chu, C. H., & Li, Z. (2010, June). The use of RFID in healthcare: Benefits and barriers. In 2010 IEEE International Conference on RFID-Technology and Applications (pp. 128-134). IEEE.

[3] Haddara, M., &Staaby, A. (2018). RFID applications and adoptions in healthcare: a review on patient safety. Procedia computer science, 138, 80-88.

[4] Nambiar, A. N. (2009, October). RFID technology: A review of its applications. In Proceedings of the world congress on engineering and computer science (Vol. 2, pp. 20-22).

[5] Langheinrich, M. (2009). A survey of RFID privacy approaches. Personal and Ubiquitous Computing, 13(6), 413-421.

[6] Zhao, Z. (2014). A secure RFID authentication protocol for healthcare environments using elliptic curve cryptosystem. Journal of medical systems, 38(5), pp.46.

[7] Farash, M. S., Nawaz, O., Mahmood, K., Chaudhry, S. A., & Khan, M. K. (2016). A provably secure RFID authentication protocol based on elliptic curve for healthcare environments. Journal of medical systems, 40(7), pp.165.

[8] Xie, W., Xie, L., Zhang, C., Zhang, Q. and Tang, C., 2013, April. Cloud-based RFID authentication. In 2013 IEEE International Conference on RFID (RFID) (pp. 168-175). IEEE.

[9] Abughazalah, S., Markantonakis, K. and Mayes, K., 2014. Secure improved cloud-based RFID authentication protocol. In Data Privacy Management, Autonomous Spontaneous Security, and Security Assurance (pp. 147-164). Springer, Cham.

[10] He, D., &Zeadally, S. (2014). An analysis of RFID authentication schemes for internet of things in healthcare environment using elliptic curve cryptography. IEEE internet of things journal, 2(1), pp. 72-83.

[11] Wazid, M., Das, A. K., Kumar, N., Conti, M., &Vasilakos, A. V. (2017). A novel authentication and key agreement scheme for implantable medical devices deployment. IEEE journal of biomedical and health informatics, 22(4), pp. 1299-1309.

[12] Rahman, F., Bhuiyan, M. Z. A., & Ahamed, S. I. (2017). A privacy preserving framework for RFID based healthcare systems. Future generation computer systems, 72, pp. 339-352.

[13] Chiou, S. Y., & Chang, S. Y. (2018). An enhanced authentication scheme in mobile RFID system. Ad Hoc Networks, 71, pp. 1-13.

[14] Priyanka, Y. J., &Turuk, A. K. (2018, March). RFID Authentication Protocol for mobile readers satisfying EPC-C1-GEN2 standard of Passive Tags. In 2018 Technologies for Smart-City Energy Security and Power (ICSESP) (pp. 1-5). IEEE.
[15] Fan, K., Jiang, W., Li, H., & Yang, Y. (2018). Lightweight RFID protocol for medical privacy protection in IoT. IEEE Transactions on Industrial Informatics, 14(4), pp. 1656-1665.
[16] Aghili, S. F., Mala, H., Kaliyar, P., & Conti, M. (2019). Seclap: Secure and lightweight rfid authentication protocol for medical iot. Future Generation Computer Systems, 101, pp. 621-634.
[17] Safkhani, M., Bendavid, Y., Rostampour, S., & Bagheri, N. On Designing Lightweight RFID Security Protocols for Medical IoT. Cryptology ePrint Archive, Report 2019/851, 2019. https://eprint. iacr. org/2019/851.