Computers, Materials & Continua
DOI: 10.32604/cmc.2022.027118
Article

Tech Science Press

Lightweight Authentication Protocol Based on Physical Unclonable Function

Hanguang Luo[1], Tao Zou[1,*], Chunming Wu[2], Dan Li[3], Shunbin Li[1] and Chu Chu[4]

[1]Zhejiang Lab, Hangzhou, 311121, China
[2]Zhejiang University, Hangzhou, 310058, China
[3]Tsinghua University, Beijing, 100084, China
[4]The University of British Columbia, Vancouver, V1V1V7, Canada
*Corresponding Author: Tao Zou. Email: zout@zhejianglab.com
Received: 11 January 2022; Accepted: 04 March 2022

Abstract: In the emerging Industrial Internet of Things (IIoT), authentication problems have become an urgent issue for massive resource-constrained devices because traditional costly security mechanisms are not suitable for them. The security protocol designed for resource-constrained systems should not only be secure but also efficient in terms of usage of energy, storage, and processing. Although recently many lightweight schemes have been proposed, to the best of our knowledge, they are unable to address the problem of privacy preservation with the resistance of Denial of Service (DoS) attacks in a practical way. In this paper, we propose a lightweight authentication protocol based on the Physically Unclonable Function (PUF) to overcome the limitations of existing schemes. The protocol provides an ingenious authentication and synchronization mechanism to solve the contradictions amount forward secrecy, DoS attacks, and resource-constrained. The performance analysis and comparison show that the proposed scheme can better improve the authentication security and efficiency for resource-constrained systems in IIoT.

Keywords: Lightweight; authentication; physically unclonable functions

1 Introduction

With the development of Internet of Things (IoT) technology, machine-to-machine (M2M) communication supports various applications for monitoring and control in such areas as eHealth, smart factory, and smart city. The research by Gartner [1] estimates that up to $2.5 million will be spent on sensing devices/actuators in a single minute by 2021, which means that the IoT devices will not only be used in home or office but also deployed in industrial manufacture, known as Industrial IoT or Industrial 4.0. A typical IIoT scenario primarily comprises the sensors, actuators, and other devices that periodically capture data of their immediate surroundings. A specific resource-constrained IIoT system is depicted in Fig. 1.

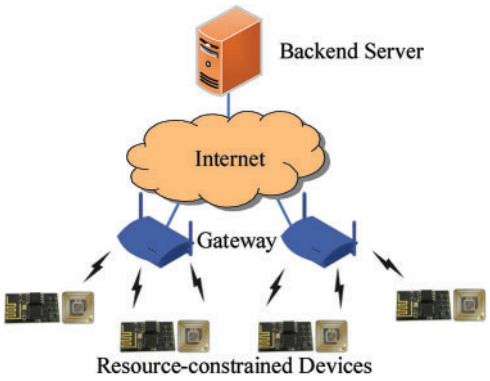

Figure 1: Typical resource-constrained IIoT system

Since the development of openness and extensive interconnection in IIoT, security has become a global challenge in M2M communication. Although authentication is the cornerstone of providing adequate protection, and numerous schemes have been proposed to ensure security in traditional IT networks [2–10], these schemes cannot be readily applied for IIoT. Because in IIoT, many resource-constrained devices are limited to computation power and communication bandwidth, such as Radio Frequency Identification (RFID) chips, wireless sensors, and so on. Therefore, it is essential to reduce the operational cost while ensuring the authentication protocol's security for resource-constrained devices. This paper proposes a lightweight authentication protocol based on a series of operations, namely Physically Unclonable Functions (PUF), hash function, and exclusive-OR (XOR) operations, respectively, to provide mutual authentication between resource-constrained IIoT devices and gateway. The proposed protocol guarantees a higher degree of practicality, efficiency, and security than existing schemes.

2 Related Work and Motivation

Over the past years, some lightweight authentication schemes for IIoT have been proposed, which can be divided into two categories: hash-based schemes and PUF based schemes. Hash-based methods are designed only on the hash function, which cannot guarantee security against cloning attacks. On the contrary, PUF based methods add Physically Unclonable Functions to the authentication process on the foundation of a hash-based scheme to resist cloning attacks. A PUF is considered a unique physical feature of an electronic device, just like biometric features like fingerprints. When queried with a challenge C, it generates a response R that depends on both C and the specific physical properties of the device that cannot be reproduced or cloned, i.e., $R = PUF(C)$. Because of that, PUF based schemes have become popular research in recent years.

In 2012, Kardas et al. [11] proposed an RFID authentication scheme based on PUFs. However, this protocol cannot ensure forward secrecy and resilience of DoS [12] attacks. Hereafter, Akgun et al. [13] proposed another PUF based protocol. Regrettably, their scheme cannot ensure forward secrecy, which is an imperative security requirement for the authentication protocol. In 2017, Esfahani et al. [14] proposed a hash-based authentication scheme for M2M communication, but the protocol is vulnerable to traceability, impersonation, DoS, and cloning attacks. Recently, Gope et al. [15] proposed a novel PUF based scheme and claimed that the protocol is more practical and can overcome the limitations of existing schemes, especially ensuring forward secrecy and resilience of DoS attacks simultaneously. However, according to our analysis, the DoS resistance mechanism of their

protocol is impractical. In their scheme, the additional use of emergency challenge and response pairs (i.e., the (C_{em}, R_{em})) will be exhausted soon and unable to be synchronized again when suffered from DoS attacks frequently. Furthermore, the large number of (C_{em}, R_{em}) pairs stored in the server will cost expensive search and synchronization recovery overhead, which cannot be scalable for applications with a large database scale.

To solve the problems in the existing authentication schemes above, we proposed a lightweight PUF based authentication protocol in this paper. Our new method achieves higher security, efficiency, and practicality compared to the existing schemes. Furthermore, our protocol's novel authentication and synchronization recovery mechanism can better deal with the problem between forward secrecy and resilience of DoS attacks that cannot be well resolved in the existing schemes.

3 Proposed Scheme

In this section, we describe the proposed lightweight authentication protocol for resource-constrained devices in IIoT. The proposed scheme has two phases: registration and authentication. The symbols and cryptographic functions used in this article are defined in Tab. 1.

Table 1: Symbols and cryptographic function

Symbol	Definition
$\boldsymbol{D}$	Resource-constrained devices in IIoT
$\boldsymbol{GSU}$	Gateway-Server Unit
TID_j^i	Temporary identity of the device j for i-th round
C_j^i	Challenge of the device j for i-th round
R_j^i	Response of the device j for i-th round
N_d/N_s	Random number generated by device/server
$PUF(\cdot)$	Secure physically unclonable function
$h(\cdot)$	One way Hash Function
$\oplus$	Exclusive-OR operation
$\|\|$	Concatenation operation

3.1 Registration Phase

Each resource-constrained device should be registered into the backend server through a secure channel. Firstly, the server generates a random challenge C_j^1 and a temporary identity TID_j^1 and then sends them to the device. Upon receiving the server's message, the device stores TID_j^1 and C_j^1 then produces and sends the corresponding responses R_j^1 to the server. Finally, the server stores the corresponding entry for each device, i.e., the $\{C_j^1, R_j^1, TID_j^1\}$. Details of this phase are depicted in Fig. 2.

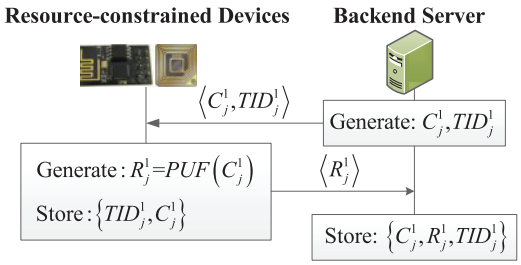

Figure 2: Registration phase of the proposed scheme

3.2 Authentication Phase

This phase achieves authentication between the resource-constrained devices (abbreviated as D), gateway, and the backend server. Since each gateway is connected to the server through a secure wired link, we consider the gateway and server as a single unit ***GSU*** in the authentication phase. For that, the authentication phase consists of the following steps. The details of the authentication phase are depicted in Fig. 3.

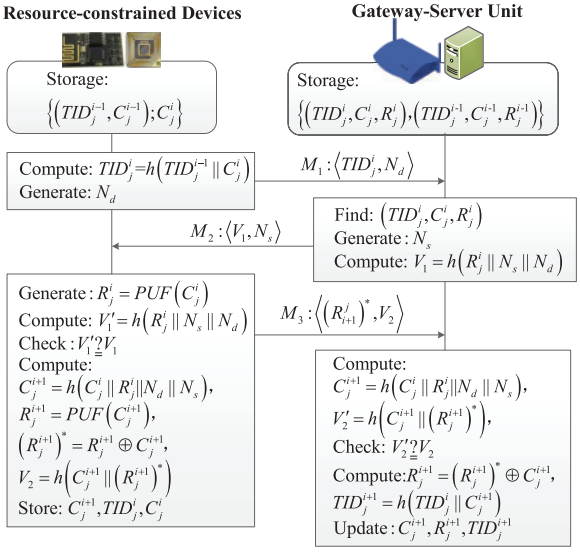

Figure 3: Authentication phase of the proposed scheme

(1) The ***D*** generates a random number N_d, computes its temporary identity TID_j^i, and then sends them to the ***GSU***. There are two cases. For the first round (when $i = 1$), the TID_j^1 can be picked from the register directly. When the $i > 1$, TID_j^i can achieve by $h\left(TID_j^{i-1} || C_j^i\right)$, where C_j^i is the challenge for i-th round and TID_j^{i-1} is the temporary identity for $(i-1)$-th round.

(2) Upon receiving the TID_j^i, ***GSU*** uses it as an index to search the corresponding entry in the database. When a matched entry is found, the ***GSU*** generates a random number N_s and computes $V_1 = h\left(R_j^i || N_s || N_d\right)$. At last, ***GSU*** constitutes a response message $M_2 : \langle V_1, N_s \rangle$ and sends it to the D. If there is no match TID_j^i in the database, the authentication requests will be rejected.

(3) After receiving the ***GSU***'s response message, the ***D*** uses C_j^i to generate the response R_j^i by its PUF. Subsequently, ***D*** checks whether the response parameter V_1 is valid or not. If the validation is successful, then ***D*** computes $C_j^{i+1} = h\left(C_j^i||R_j^i||N_d||N_s\right)$, $R_j^{i+1} = PUF\left(C_j^{i+1}\right)$, $\left(R_j^{i+1}\right)^* = R_j^{i+1} \oplus C_j^{i+1}$, $V_2 = h\left(C_j^{i+1}||\left(R_j^{i+1}\right)^*\right)$ and sends $M_3 : \left\langle\left(R_{i+1}^j\right)^*, V_2\right\rangle$ to ***GSU***. Finally, ***D*** updates C_j^i, TID_j^{i-1} and C_j^{i-1} with C_j^{i+1}, TID_j^i and C_j^i respectively.

(4) Upon receiving the response message from D, ***GSU*** first computes $C_j^{i+1} = h\left(C_j^i||R_j^i||N_d||N_s\right)$ and $V_2' = h\left(C_j^{i+1}||\left(R_j^{i+1}\right)^*\right)$. Then validates whether the response parameter V_2 is valid or not. If the validation is successful, then ***GSU*** calculates $R_j^{i+1} = \left(R_j^{i+1}\right)^* \oplus C_j^{i+1}$ and $TID_j^{i+1} = h\left(TID_j^i||C_j^{i+1}\right)$, and subsequently stores C_j^{i+1}, R_j^{i+1} and TID_j^{i+1} in its memory for the following round communication.

In the case of the DoS attacks, the resynchronization mechanism will be executed by our scheme. When the ***GSU*** rejects the authentication request from ***D*** for the first time, where the temporary identity TID_j^i is computed by $h\left(TID_j^{i-1}||C_j^i\right)$, the ***D*** will directly choose TID_j^{i-1} as the request parameter and generate a new random number, then send them to ***GSU*** again. Since TID_j^{i-1} must have been used in the previous round successfully, ***GSU*** definitely can find the matched entry in its database. After that, the authentication process will do the same as the process above from steps (1) to (4). Finally, ***GSU*** and ***D*** will update and hold the newest authentication entry together after the resynchronization mechanism.

4 Security Analysis

In this section, the security analysis shows that our scheme can overcome several imperative security properties and the malicious behaviors assumed in the security properties. Through both the rigorous informal and formal security analysis, we figure out that our proposed scheme achieves the desired security features to tolerate various known attacks in authentication in IIoT.

4.1 Informal Security Analysis

4.1.1 User Anonymity

Anonymity includes untraceability and unlinkability. Untraceability means that an adversary cannot identify which identities from the same group belong to whom. In comparison, unlinkability implies that an adversary cannot distinguish whether two identities belong to the same user. In our proposed scheme, the devices don't reveal their real identities or secrets during each authentication instance since all the transmitted messages are computed with a random number. Hence, the devices are not traceable to the adversary with temporary identities or other secrets. Moreover, the temporary identities TID_j^i are calculated by random challenge C_j^{i+1} and one-way hash function h, i.e., $TID_j^i = h\left(TID_j^{i-1}||C_j^i\right)$, where C_j^i is updated with the random number in each round. So, it is difficult for an adversary to correlate the current round temporary identity TID_j^i with the next round TID_j^{i+1}. The same is between the different devices.

4.1.2 Confidentiality

The transmitted messages M_1, M_2 and M_3 between the ***D*** and ***GSU*** are all related to the secret response parameter R_j^i. Without knowing R_j^i, the adversary cannot forge the valid parameter V_1, $\left(R_j^{i+1}\right)^*$ and V_2, which are used for authentication and transmitting confidential information. Besides, in the authentication process, all the verified messages and parameters are protected by hash function h. Even if the adversary may obtain the corresponding temporary identities and challenges from the captured

device's memory, it cannot recover other secrets that can help itself pass the ***GSU***'s interrogation process.

4.1.3 Forward Secrecy

In the authentication phase, mutual authentication between the ***D*** and ***GSU*** can be achieved based on the verified messages M_2 and M_3. ***D*** authenticates ***GSU*** by verifying the parameter $V_1 = h\left(R_j^i||N_s||N_d\right)$, where an adversary cannot generate legitimate V_1 without knowing the response R_j^i. A similar process takes place when the ***GSU*** receives messages M_3. The ***GSU*** verifies the parameter $V_2 = h\left(C_j^{i+1}||\left(R_j^{i+1}\right)^*\right)$ to verify the legality of D. As depicted in the authentication process, an attacker also cannot generate a legal V_2 without the correct response R_j^i. Hence, our protocol achieves mutual authentication between resource constrain device and Gateway-Server Unit.

4.1.4 Mutual Authentication

An authentication protocol should provide forward secrecy to protect past sessions against future compromises of the secret keys. In our protocol, after completing each successful mutual authentication, the challenge parameter C_j^i and response parameter R_j^i will be updated with the random number, i.e., $C_j^{i+1} = h\left(C_j^i||R_j^i||N_d||N_s\right)$ and $R_j^{i+1} = PUF\left(C_j^{i+1}\right)$. Due to the one-way characteristic of the hash function and PUF, the attacker cannot acquire C_j^i from C_j^{i+1} or R_j^i from R_j^{i+1}.

4.1.5 The Resilience of DoS Attacks

Since both communicators need to update their secret security credentials to ensure forward secrecy, an attacker can cause a desynchronization problem by blocking the messages between two communicators, eventually causing the DoS problem. As mentioned in sect.2, almost all the existing lightweight authentication protocols fail to deal with the problem of forward secrecy and DoS attacks at once. In our proposed scheme, we utilize an ingenious resynchronization mechanism to cope with this problem. Since ***D*** and ***GSU*** update temporary identity TID_j^i, challenge C_j^i, and response R_j^i after each authentication process, the ***GSU*** needs to preserve current and previous round authentication entry, i.e., $\left(TID_j^i, C_j^i, R_j^i\right)$ and $\left(TID_j^{i-1}, C_j^{i-1}, R_j^{i-1}\right)$, while ***D*** only needs to preserve the last round authentication entry $\left(TID_j^{i-1}, C_j^{i-1}\right)$ and the present round challenge parameter C_j^i. When it comes to the i-th round authentication, ***D*** computes the current round temporary identity TID_j^i by TID_j^{i-1}, C_j^i and one-way hash function h, i.e., the $TID_j^i = h\left(TID_j^{i-1}||C_j^i\right)$. Suppose that ***GSU*** has rejected D's first authentication request because ***GSU*** failed to update the authentication entry during the last round by spontaneous failure or malicious attack. Since both ***D*** and ***GSU*** must have kept the previous successful authentication entry, they can revert to the synchronization state by ***D*** sending TID_j^{i-1} to ***GSU*** once again. In this way, the proposed scheme ensures security against DoS to desynchronization attacks.

4.1.6 The Resilience of Clone Card Attack

An attacker can capture a valid device and access secrets stored in it to produce the cloned devices. Since PUF is based on a unique and complex physical characteristic, in our proposed scheme, even if the attackers obtain the device's memory (i.e., the TID_j^{i-1}, C_j^{i-1} and C_j^i), they cannot use them to forge or get the secret R_j^i, which must be generated by the PUF. As a result, the attacker cannot impersonate a valid device by clone attack to pass the ***GSU***'s authentication in our proposed scheme.

4.2 Formal Security Analysis

This section conducts a formal security verification using the widely accepted Automated Validation of Internet Security Protocols and Applications (AVISPA) [16] tool to demonstrate that our protocol fulfills the required security properties. It provides a modular and expressive formal language for specifying protocols and their security properties and integrates different backends that implement various state-of-the-art automatic analysis techniques. The formal security verification and the results of our protocol using OFMC backend are depicted in Fig. 4. The details of the HLPSL code are provided in the supplementary material at https://github.com/lhguestc/AVISPA.

```
% OFMC
% Version of 2006/02/13
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  /home/span/span/testsuite/results/PUF.if
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 0.02s
  visitedNodes: 4 nodes
  depth: 2 plies
```

Figure 4: The result of the analysis of the proposed scheme using OFMC

5 Performance Analysis and Comparison

5.1 Security Feature Comparison

In this section, we compare some critical security properties of our protocol with recently proposed schemes. From Tab. 2, we can see that our protocol can satisfy all the important required security requirements. Particularly, only our scheme can better ensure forward secrecy with the resistance of the DoS attack.

Table 2: Comparison of the required security properties (SP)

Schemes	SP1	SP2	SP3	SP4	SP5
Esfahani [14]	YES	NO	NO	NO	NA
Kardas [11]	YES	YES	YES	NO	NO
Akgun [13]	YES	YES	YES	NO	NA
Gope [15]	YES	YES	YES	YES	LIMITED
Ours	YES	YES	YES	YES	YES

SP1: Mutual authentication; **SP2:** Untraceability; **SP3:** Unclonability; **SP4:** Forward secrecy; **SP5:** Resilience of dos attacks

5.2 Computational and Communication Cost Comparison

Since resource-constrained devices generally have limited resources such as storage and computation, it is important to consider the efficiency of the proposed scheme. We compare the performance of the proposed scheme in terms of the computation cost as shown in Tab. 3, which illustrates the numbers of operations including hash (denoted by H), PUF (denoted by P), and random number generator (denoted by RNG). Tab. 3 shows that our protocol's computation overhead is lower than other existing schemes for the same condition. However, it provides better security which is shown earlier in Tab. 2. It is worth mentioning that the computational cost of SHA-256 is similar to 256-bit Arbiter PUF [17], which can provide a reference for the comparison between our scheme and [14].

Table 3: Comparison of the computational cost

Schemes	Resource-constrained device	Gateway-server unit
Esfahani [14]	7H + RNG	6H + RNG
Kardas [11]	5H + 2P + RNG	4H + RNG
Akgun [13]	4H + 2P + RNG	4H + RNG
Gope [15]	5H + 2P + RNG	5H + RNG
Ours	4H + 2P + RNG	4H + RNG

In Tab. 4, we compare the efficiency of our scheme to the existing schemes in terms of device storage overhead, communication cost, and resynchronization complexity. According to [14] and [15], each authentication parameter will cause 128-bit storage or communication costs. Tab. 4 shows that, in our proposed scheme, the device storage overhead and communication costs are 384-bit and 768-bit, which is less than all other existing schemes for the same condition. Furthermore, the proposed protocol's resynchronization mechanism complexity is less than the latest Gope scheme [15], which claims to be the only scheme to meet the challenge between forward secrecy and DoS attacks.

Table 4: Comparison of the other cost

Schemes	Device storage overhead	Communication cost	Resynchronization complexity
Esfahani [14]	384-bit	1024-bit	NA
Kardas [11]	768-bit	1480-bit	NO
Akgun [13]	512-bit	896-bit	NA
Gope [15]	128 + n∗64-bit	832-bit	O(n)
Ours	384-bit	768-bit	O(1)

6 Conclusion

In this paper, we propose a PUF based lightweight authentication scheme for resource-constrained devices in IIoT. The proposed scheme provides ubiquitous demands for mutual authentication in M2M communication. Formal and informal security analysis shows that the proposed protocol achieves better security features than existing schemes. Moreover, the performance analysis and

comparison indicate that our proposed approaches are more practical and suitable for ensuring secure communication in IIoT.

Funding Statement: This work was supported by China Postdoctoral Science Foundation under Grant Nos. 2020M681959 and 2020TQ0291, in part by the national key R&D project under Grant No. 2018YFB2100401, in part by the National Key Research and Development Project No. 2018YFB2100400.

Conflicts of Interest: The authors of this paper declare that there are no conflicts of interest regarding the publication of this paper.

References

[1] W. Goertz, N. Heudecker, M. Beyer, F. Chesini, H. LeHong *et al.,* "Top strategic predictions for 2017 and beyond: Surviving the storm winds of digital disruption," Accessed: May 2019. [Online]. Available: https://www.gartner.com/doc/3471568.

[2] J. -Y. Lee, W. -C. Lin and Y. -H. Huang, "A lightweight authentication protocol for internet of things," in *Proc. ISNE*, pp. 1–2, Kwei-Shan Tao-Yuan, Taiwan, 2014.

[3] W. -L. Chin, Y. -H. Lin and H. -H. Chen, "A framework of machine-to-machine authentication in smart grid: A two-layer approach," *IEEE Communications Magazine*, vol. 54, no. 12, pp. 102–107, 2016.

[4] Y. Qiu and M. Ma, "A mutual authentication and key establishment scheme for M2M communication in 6LoWPAN networks," *IEEE Transactions on Industrial Informatics*, vol. 12, no. 6, pp. 2074–2085, 2016.

[5] H. Luo, G. Wen, J. Su and Z. Huang. "SLAP: Succinct and lightweight authentication protocol for low-cost RFID system," *Wireless Networks*, vol. 24, no. 1, pp. 67–78, 2018.

[6] H. Luo, G. Wen and J. Su, "Lightweight three factor scheme for real-time data access in wireless sensor networks," *Wireless Networks*, vol. 26,. no. 2, pp. 955–970, 2020.

[7] H. Luo, G. Wen, J. Su, Z. Huang and D. Inserra, "Multi-hop distance-bounding for improving security and efficiency of Ad-Hoc networks," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 5312–5323, 2019.

[8] S. M. Aljuaid and A. S. Ansari, "Automated teller machine authentication using biometric," *Computer Systems Science and Engineering*, vol. 41, no. 3, pp. 1009–1025, 2022.

[9] M. Alshammari and S. Nashwan, "Fully authentication services scheme for nfc mobile payment systems," *Intelligent Automation & Soft Computing*, vol. 32, no. 1, pp. 401–428, 2022.

[10] S. G. Oliver and T. Purusothaman, "Lightweight and secure mutual authentication scheme for iot devices using coap protocol," *Computer Systems Science and Engineering*, vol. 41, no. 2, pp. 767–780, 2022.

[11] S. Kardas, S. Celik and M. Yildiz, "Puf-enhanced offline RFID security and privacy," *Journal of Network and Computer Applications*, vol. 35, no. 6, pp. 2059–2067, 2012.

[12] P. Gope, J. Lee and T. Q. S. Quek, "Resilience of DoS attack in designing anonymous user authentication protocol for wireless sensor networks," *IEEE Sensors Journal*, vol. 17, no. 2, pp. 498–503, 2017.

[13] M. Akgun and M. U. Caglayan, "Providing destructive privacy and scalability in RFID systems using PUFs," *Ad Hoc Networks*, vol. 32, pp. 32–42, Sep. 2015.

[14] A. Esfahani, G. Mantas, R. Matischek, F. B. Saghezchi, J. Rodriguez *et al.,* "A lightweight authentication mechanism for M2M communication in industrial IoT environment," *IEEE Internet of Things Journal*, vol. 6, no. 1, pp. 288–296, 2017.

[15] P. Gope, J. Lee and T. Q. S. Quek, "Lightweight and practical anonymous authentication protocol for RFID systems using physically unclonable functions," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 11, pp. 2831–2843, 2018.
[16] "AVISPA automated validation of internet security protocols and applications," Last Accessed on April 25, 2016. [Online]. http://www.avispa-project.org/.
[17] M. Kaveh and M. Mosavi, "A lightweight mutual authentication for smart grid neighborhood area network communications based on physically unclonable function," *IEEE Systems Journal*, vol. 14, no. 3, pp. 4535–4544, 2020.