Computer Systems Science & Engineering
DOI:10.32604/csse.2022.021129
Article

Tech Science Press

Secured Cloud Communication Using Lightweight Hash Authentication with PUF

R. Padmavathy* **and M. Newlin Rajkumar**

Department of Computer Science and Engineering, Anna University Regional Center, Coimbatore, 641046, India
*Corresponding Author: R. Padmavathy. Email: padmavathyre21@yahoo.com
Received: 24 June 2021; Accepted: 08 October 2021

Abstract: Internet-of-Things (IoT) is an awaited technology in real-world applications to process daily tasks using intelligent techniques. The main process of data in IoT involves communication, integration, and coordination with other real-world applications. The security of transferred, stored, and processed data in IoT is not ensured in many constraints. Internet-enabled smart devices are widely used among populations for all types of applications, thus increasing the popularity of IoT among widely used server technologies. Smart grid is used in this article with IoT to manage large data. A smart grid is a collection of numerous users in the network with the fastest response time. This article aims to provide high authentication to the smart grid, which constitutes secure communication in cloud-based IoT. Many IoT devices are deployed openly in all places. This open-access is vulnerable toward cloning attacks. Authentication is a significant process that provides strength while attacking. The security of the cloud and IoT must be computationally high. A lightweight authentication using hashing technique is proposed considering the aforementioned condition. The main factor of the authentication involves physically unclonable functions, which are utilized in improving the performance of the authentication. The proposed approach is evaluated with the existing techniques. Results show that the performance of the proposed algorithm provides high robust security.

Keywords: Cloud; IoT; smart grid; PUF; lightweight authentication

1 Introduction

A smart grid is considered to be a critical infrastructure combined with a large-scale power grid system, which performs in large IoT networks. Technologies, such as IoT smart grids, are currently utilized in smart homes, smart cities, and other digital applications. In a smart grid, every sensor device monitors the power consumption of each device in the network. Such monitoring helps in the power optimization of smart grid environments based on low consumption rates. AI/ML in the grid system is used to monitor the traffic networks and improves the navigation in networks with less traffic. Applications, such as smart home, are utilized to access and control data through a remote. IoT devices are easy to access in most real-time applications but lack in providing high authentication for the user data in communication.

The current research aims to protect data in the communication channel of IoT smart grids. The authentication of IoT is an indispensable task in developing technologies. When the authentication is ensured in an IoT network, the user guarantees the data transferred and received as legal from the sender and the receiver. IoT generally acts as a base authentication factor in the communication network. Security is the key technique required in every data processing sector. Furthermore, cryptography is the most widely used method in data authentication [1]. Data encryption is classified into two broad categories: symmetric and asymmetric. Some of the asymmetric techniques employed in data encryption include elliptic curve and RSA techniques. The paired key (such as public and private keys) is used in asymmetric data encryption. The main problem in implementing the asymmetric techniques is the high computational cost. Moreover, these techniques tend to share the keys between two or more parties. In the case of sharing the key in common encryption techniques, security is the big question in the standard of advanced data encryption. Symmetric encryption is unsuitable for the advanced techniques despite its low computational cost and high-speed encryption techniques. Most of the authentication processes select only the asymmetric techniques to be presented [2–9]. Today, technologies, such as IoT, cloud, and edge computing, are unsatisfied with traditional authentication and other cryptographic methods.

The traditional drawbacks introduce new approaches, such as lightweight security schemes. This scheme was first proposed by Lamport in 1981 and was fully processed using a password [10]. The later advancement modified the lightweight schemes and enhanced then with key negotiation techniques [11–14]. The multiserver environment used a hash function in the lightweight authentication process [15]. The disadvantages of this lightweight hashing technique include its predisposition to insider, masquerade, and forgery attacks. The smart grid-based security with the light weight, which possesses the universal characteristics of authentication, has been recently suggested [16]. The hash functions with exclusive OR operation are used in the lightweight authentication process to achieve mutuality. A new lightweight hash chain-based forward two-factor authentication with PUF is proposed to improve the process of high security and authentication for the secure communication of cloud IoT.

The main contributions of the proposed security techniques are as presented as follows.

1. The IoT attacks in cloud and smart grids are addressed using two-factor authentications for physical and cloning problems.

2. A lightweight authentication process with the hash function and physical unclonable function (PUF) equipped with IoT devices is proposed to safeguard against physical and cloning attacks.

3. Three registration phases for authentication, such as user, sensor, and cloud server registration, are performed. The security is then ensured in the phases of authentication and password change.

4. The session keys for all the entities considering user, sensor, and gateway are calculated in the authentication phase. User anonymity is also ensured with the hash function. If any malicious attacker wants to hack the user identity, then this attacker can be verified with the hash function.

The remainder of the article is arranged and structured as follows. Section 2 discusses the traditional and new authentication techniques in IoT smart grid environments. Section 3 implements the proposed techniques. Section 4 evaluates the result of the proposed techniques. Section 5 concludes the proposed work.

2 Related Work

The user sign in password scheme was used in the authentication process in the IoT cloud architecture [17]. However, a one-factor security scheme was inapplicable for the smart infrastructure. Therefore, two or more factor authentication schemes, such as biometric, smartphone, and smart card, are necessary for the improvement of security in the IoT smart grid infrastructure. The wireless networks in medical applications using IoT sensors [18] employ the two-factor schemes for the security process. These

schemes use smart cards with password-driven authentication process. The two-factor authentication enhances the security of the IoT cloud infrastructure. Moreover, the patient is accessed steadily with a two-factor authentication process. The network-based health care system [19] had also used the smart card with a password for the data authentication process. The two-factor security schemes are highly recommendable for wireless networks considering the forgery attacks [20,21] discussed in the network. Some of the vulnerabilities encountered by insider attacks are unsatisfied with two-factor normal authentication. Thus, certain security techniques to well-known applications are introduced with new authentication schemes [22,23]. However, some of these techniques are lagging behind guessing attacks. Similarly, the simple two-factor is highly lagging in guessing the attacks.

A new authentication scheme called lightweight authentication was proposed [24,25] for high-level security in two-factor authentication. In lightweight security, the three parties co-operated in generating a session key for security. However, the main problem lies in the guessing attacks. Security for IoT networks using a novel authentication protocol is constructed to overcome these guessing attacks [26]. The specified protocol helps the sender and the receiver with the authentication scheme to verify the intruders. Three- or multi-factor security schemes are remarkably complex and difficult in computational cost [27]. Therefore, two-factor authentication is highly encouraged in the field of IoT-based security systems. The lightweight scheme, which is used in medical applications, has been proven to be resistant to threats from insiders, guessing, and session key-based disclosure attacks. However, lightweight schemes cannot provide forward secrecy techniques according to the limitation studies. The biometric-based security in two-factor security techniques uses the key managing protocols in sensor networks. The extraction of biometric features (ID) is performed using fuzzy logic extraction concepts.

The security schemes are found to be user-centric in many applications that use smart cards, passwords, and smart devices for two-factor authentication. The study of smart card security schemes revealed the absence of tamper proofs and the high vulnerability of such schemes to physical insider or outsider attacks. This particular problem was recently addressed using physical uncloned function (PUF). The new PUF is used in IoT-based devices for providing high security. However, computation (PUF) is difficult in public key systems. Some of the researchers implemented PUF authentication with cryptography symmetric techniques. The PUF challenges were highly addressed in several research works. Some of the techniques reviewed the usage of authentication protocols in the hardware to protect intellectual ideas. Wireless sensor networks used the authentication protocol with PUF to provide high security in radio-frequency identification systems [28]. Mutual security in PUF was suggested for the authentication protocols. The only disadvantage of PUF in the protocol lies in the privacy preservation of IoT devices in the network. Thus, a lightweight-based PUF authentication system is proposed on the basis of the aforementioned studies to obtain satisfactory results.

3 Proposed Lightweight Authentication with PUF Methodology

The major applications of IoT are smart grids. The acquired data from consumers, transmission lines, and distribution subtractions are collected using power grids, which are integrated into the smart grid data communication network. The collected data from the sensors in the IoT smart grid are of large volume and consume a considerable amount of energy and resources, which, in turn, become a bottleneck. Enhancing smart grids is necessary to overcome the issues with efficient storage. Various applications are generally available on cloud data management with IoT smart grid security and storage. However, these applications lack mutual authentication and cannot guarantee secrecy in the authentication phase. The proposed approach used lightweight hash-chain-based forward two-factor authentication with PUF for cloud IoT secure communication to overcome the aforementioned issues.

3.1 System Model

The cloud architecture of the proposed work comprised a cloud server with several private servers for distributing the IoT devices through the IoT layers. The overview of the proposed system model is shown in Fig. 1. This study used the lightweight hash-chain-based two-factor authentication and PUF as an authentication factor equipped with IoT devices to safeguard against physical and cloning attacks. The architecture comprised the following subsections: IoT layers, registration phase for users, IoT device sensors and cloud server, authentication phase using the proposed authentication scheme, and password change phase.

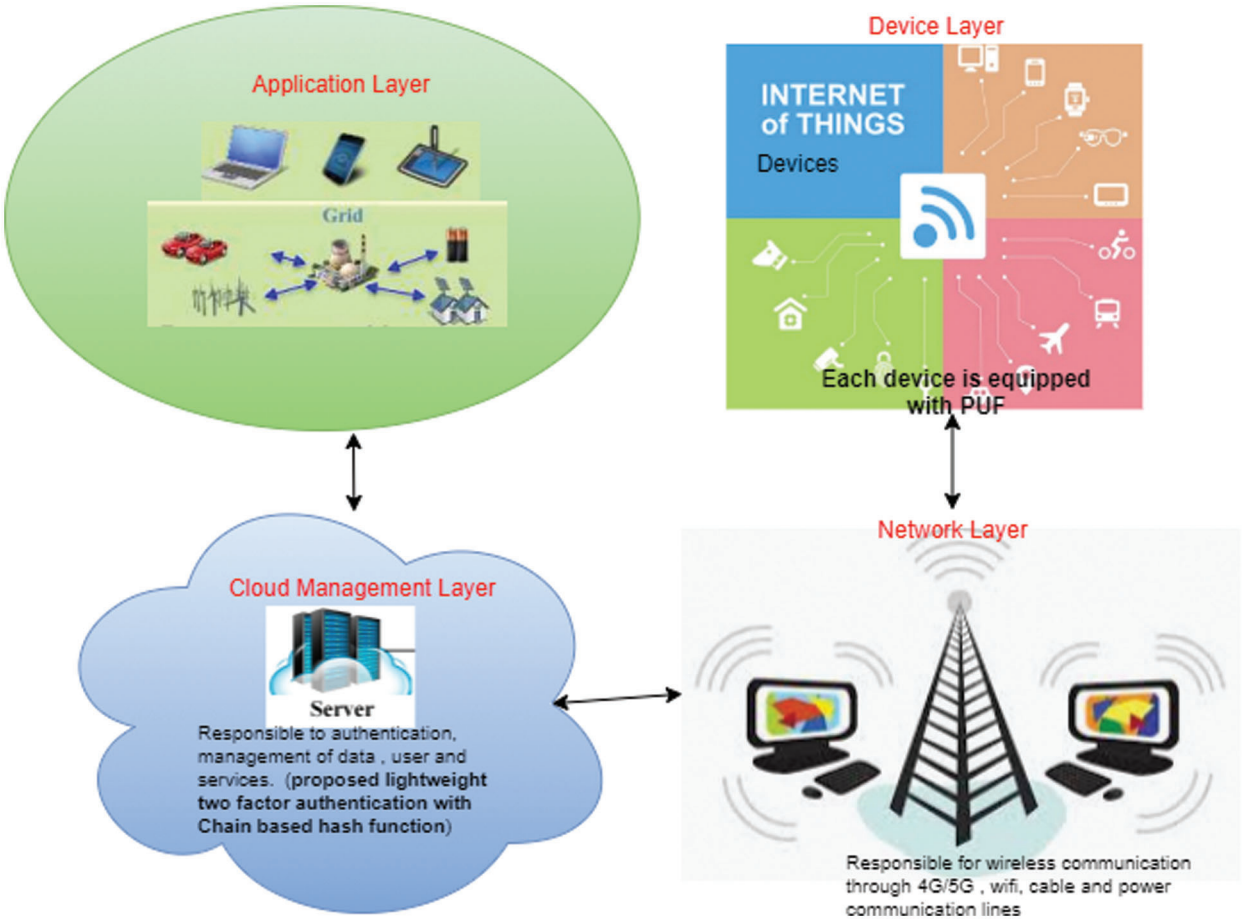

Figure 1: Proposed IoT smart grid authentication system model

3.2 IoT Layers

The layers involved in this architecture include the device, network, cloud management, and application layers. The specified work followed the previously proposed architectural layers. The device layers comprised sensors, actuators, and smart plugs, which are responsible for collecting data and controlling the IoT devices through the gateway with a microcontroller, internal display, and storage and communication modules. The layer connecting the device to the application layer is the network layer for sending data. The cloud management layer is responsible for handling data and user storage management with authentication schemes for data security transmission. The application layer is used to provide services to end-users, such as owners or smart grids, with efficient energy management.

3.3 Physically Unclonable Function (PUF)

PUF, a circuit embedded into the IoT devices to avoid physical attacks, maps a group of challenges with the responses. PUF is difficult to clone. This circuit is characterized by the group of CRPs (challenge-response pairs) and represented as $R = PUF(C)$, where C is the challenge, and R is the response. The noise in the PUF can be removed with the aforementioned fuzzy extractor. PUF is generally robust and secure, thus avoiding persistent attacks, and the session keys are generated without storing. Thus, hardware authentication is secure and simple. The PUF is also considered secured with the requirements mentioned below.

- For any two PUFs with the challenge $C_1 \in \{0,1\}^k$ and $\Pr[hd(PUF_1(C_1), PUF_2(C_2) > d] \geq 1 - \varepsilon$, where Hd is the hamming distance.
- For any input of $C_1,\ldots,C_n \in \{0,1\}^k$, $\Pr[hd\left(PUF_D(i), PUF_D\left(C_j\right)1 < i,j, \leq n, i \neq j > \lambda\right] \geq 1 - \varepsilon$. The output of the PUF is always larger than λ. The distance between two PUF responses for the same challenge is always larger than d. This will be used in the authentication phase of the proposed work.

3.4 Registration Phase

The registration phase is divided into three parts: user, sensor, and cloud server registration. Addition to the system by the user, sensor, or cloud server must be registered through this phase. The user, sensor, and cloud servers can start the authentication and data transfer processes once the registration is successful. The notations used in this work are listed in Tab. 1.

Table 1: Notations used

Symbol	Description
U_i,UID_i	i^{th} user and their identity number
PWD_i	Password of the i^{th} user.
GS_j, GID_j	jth gateway identity and secret key
CS, ID_{cs}	Control server and its identity
S_k,SID_k	k^{th} sensor node and its identity
n_i	Secret random number
N	Number of sensor node
SG_k	Secret key shared between sensor and gateway
P	Secret key of CS
SK_s,SK_u,SK_g	Session key generated by sensor, user, and gateway
M_i	i^{th} user message in the authentication phase
$PUID_i$,$PSID_i$	Pseudo identity of user and sensors of i^{th} user
H	Cryptographic one-way hash function
rd_u, rd_s, rd_{cs}	User, sensor, and CS random numbers, respectively

3.4.1 User Registration

Based on the two-factor authentication, the user of the network system is responsible for selecting its identity with a respective password, and the IoT device stores the registration information.

Step 1: User U_i selects its identity UID_i and respective password PWD_i and a random number n_i to compute the hidden password. The user sends the ID to CS, which checks the validity of the UID: if valid, then the password computation process starts; otherwise, the phase is stopped. The computed hidden password is $HPWD_i = h(PWD||IDcs||ni)$. The UID with this HPWD of i is sent to the gateway GW_j through a secure channel.

Step 2: If UID_i is already registered, then the gateway (GW_j) will select the pseudo-identity of the user ($PUID_i$) and its random number (rd_u) for the user U_i and stores its information with $HPWD_i$ in the database. Then, the gateway sends A, B, PUIDi, I D_{cs}, and GWj to the Ui via a secure channel. A and B are respectively calculated as follows:

$$A = h\left(PUID_i||rd_u||GID_j, GS_j\right) \oplus HPWD_i \tag{1}$$

$$B = h(UID_i||GS_j) \oplus h(UID_i, HPWD_i) \tag{2}$$

Step 3: Ui calculates C and stores the registered information (A, B, C, PUIDi, GIDj) to its IoT mobile device. $C = h(UIDi||PWDi) \oplus n_i$. The successful registered user U_i is ready for authentication.

3.4.2 Sensor Registration

Each of the sensors (Sk) and their identity (SIDk) have the network identifier N. Each sensor and the gateway (GWj) can communicate with each other and share a secret key (SGk) that is equal to h(SIDk, GWj, N). The gateway (GWj) selects the random number rdg with pseudo-identity PSIDi for each sensor and sends SIDk, SGk, GIDj, rdg, and PSIDi. The sensor is then installed and ready for processing.

3.4.3 Cloud Server Registration

The cloud server (ClS_j) sends its identity (ID_{cs}) and its pseudo identity ($PCLID_j$) to the control server (CS) via secure channel. The CS then uses the secret key p to compute $A = h\left(PCLID_j||ID_{cs}||p\right)$ and $B = h(SID_j||p)$, store SID_k in the database, and send A, B, ID_{cs} to the ClS_j. The cloud server (ClS_j) stores A, B, SID_j, $PCLID_j$, and ID_{cs} in its memory.

3.4.4 Authentication Phase

The authentication must occur while the user U_i receives the services from the cloud server (ClS_j) to improve the authenticity between the user and the server. The user obtains the session key once the authentication phase is completed. The user can connect with the cloud server for accessing the data securely using the session key. The authentication process involves the following steps.

Step 1: Once the registration phase is over, the user U_i selects the sensor and sends the UID_i and PWD_i to the IoT device to calculate the random number $n_i = C \oplus h(UID_i||PWD_i)$ and $HPWD_i = PUF_{Di}(h(PWD_i \parallel n_i))$. Then, the user random number rd_u is generated, and the sensor SID_k is selected calculated B as follows: $B = h(PUID_i||GID_j \parallel SID_k \parallel B \parallel UID_i \parallel rd_u)$. The message M_1 contains $PUID_i$, GID_j and B sent to GW_j.

Step 2: The cloud server (ClS_j) receives M_1, and ClS_j fetches the equivalent UID_i, n_i, and $HPWD_i$ from the database. $B_1 = h\left(PUID_k \parallel rd_s \parallel GID_j \parallel GS_j\right)$ and $rd_u = B_1 \oplus B \oplus HPWD_i$ are then computed. The new pseudo random number for the sensor $PSID_i^{new}$ is calculated by extracting the PUF output and generating the secret key as SG_k as $SG_k = PUF_{Di}\left(h\left(SID_k \parallel GS_j \parallel N\right)\right)$ and computing $B_2 = A \oplus rd_s$, $B_3 = h\left(rd_s \parallel PSID_j \parallel ID_{cs}\right) \oplus SID_k$, $B_4 = B \oplus PSID_i^{new} \oplus h(rd_s \parallel PSID_i)$, and $B_5 = h\left(SID_k \parallel PSID_j \parallel PSID_j^{new} \parallel rd_s \parallel B_4\right)$. The ClS_j then sends the message $M_2 = \{M_1, PSID_j, B_2, B_3, B_4, B_5\}$ to the CS.

Step 3: Once the message is received, the sensor checks the $PSID_i$, calculates $S = h(SG_k \parallel GID_j)$, and generates $rd_g = B_4 \oplus S \oplus SID_k \oplus rd_u$. If B_4 is correct, then the random number for the sensor rd_s is generated and computed as $rd_s^{new} = h(rd_g \parallel rd_u \parallel S)$ and $PSID_i^{new} = B_3 \oplus rd_g \oplus rd_u$. $(PSID_i^{new},\ rd_s^{new})$ is stored, and the common session key is generated as follows: $SK_s = h(rd_u \oplus HPWD_i \parallel rd_g \parallel rd_s)$. The sensor then generates $B_5 = h(SG_k \parallel rd_g) \oplus h(rd_u) \oplus rd_s$, $B_6 = h(B_4 \parallel B_5 \parallel SK_s \parallel SID_k \parallel GID_j \parallel rd_s)$ and sends $M_3 = (B_4,\ B_5,\ B_6)$ to the gateway (GW_j).

Step 4: Once the sensor receives the response, the gateway (GWj) computes the new random number $rd_u^{new} = h(rd_u)$, and the rd_u is fetched from the database. Then, $rd_s^{new} = rd_g \oplus S \oplus B_4$. If $h\ is\ rd_s == rd_s^{new}$, then the session key is calculated as common using $SK_g = h(rd_u \oplus HPWD_i \parallel rd_g \parallel rd_s)$. If this equation is valid, then the CS is legal. Otherwise, the authentication process is terminated. The ClS_j calculates and updates $A_j^{new} = B_4 \oplus h(rd_s \parallel PSID_i^{new})$. ClS_j finally sends $M_4 = \left\{rd_s^{new}\ ,\ A_j^{new},\ SK_g\right\}$ to the user (U_i).

Step 5: The IoT device of the user U_i extracts the PUF output and receives rd_g and rd_s with the calculation of $rd_g = B_5 \oplus h(rd_u \parallel UID_i)$ and $rd_s = B_6 \oplus h(rd_u \parallel rd_g \parallel HPWD_i)$. The device re-computes the common session key as $SK_u = h(rd_u \oplus HPWD_i \parallel rd_g \parallel rd_s)$, and the IoT device of the user sends $h(SK_u)$ to the cloud server ClS_j.

Step 6: ClS_j finally checks $h(SK_u) == h(SK_s)$, which means the session key is identified correctly.

3.4.5 Password Change Phase

If the user wants to change the password, then he/she executes this phase. Assume the user has $\{A, B_1, B_2, B_3, B_4, PUID_i^{new}, ID_{cs}\}$. The IoT device of the user will calculate $n_i = B_2 \oplus h(UID_i \parallel PWD_i) == B_3$ and check the condition. If satisfied, U_i sends the new password PWD_i^{new}. Ui then recalculates B_2, B_3, B_4 with $B_2^{new}, B_3^{new}, B_4^{new}$. $B_2^{new} = B_2 \oplus h(PWD_i \parallel n_i) \oplus h(PWD_i^{new} \parallel n_i), B_3^{new} = B_3 \oplus h(UID_i \parallel PWD_i) \oplus h(UID_i \parallel PWD_i^{new})$, $B_4^{new} = B_4 \oplus h(UID_i \parallel PWD_i \parallel n_i) \oplus h(UID_i \parallel PWD_i^{new} \parallel n_i)$. The user finally accesses the network with the new password PWD_i^{new} with all the details for authentication.

3.5 Security Analysis of Proposed System

The proposed lightweight two-factor authentication with PUF can ensure the mutual authentication of control server (CS) between the cloud server and user. The CS can verify the identity of the user in the registration phase that uses A to hide the random number of the user rd_u. The identity of the sensor and the cloud server is also acknowledged in the registration phase through the computation of A and B. The session keys for all the entities, such as user, sensor, and gateway, are also calculated in the authentication phase. User anonymity is ensured with the hash function. If any malicious attacker wants to hack the user identity, then this attacker can be verified with the hash function. The attacker must compute the hash function with ID and the random number of users for verification. Thus, the attacker is cannot identify the user, increasing the user anonymity of the proposed work. The offline and physical attacks of the network can be avoided with the PUF-embedded IoT devices.

4 Performance Evaluation

These authentication schemes use hash functions, XOR operation, and concatenation operations for the authentication process. The comparative study considering computation, communication, and storage costs will prove the efficiency of the proposed algorithm. The security properties of the algorithms are shown in Tab. 2. Compared with other algorithms, the proposed algorithm satisfies all the security properties with its lightweight two-factor authentication scheme with PUF.

Table 2: Security property comparison of authentication schemes

Security Properties	Maitra et al.	Amin et al.	Zhou et al.	Wu et al.	Gope et al.	Proposed scheme
Mutual authentication	Yes	Yes	Yes	Yes	Yes	Yes
Perfect forward secrecy	Yes	No	Yes	No	Yes	Yes
Resistance to insider attack	Yes	Yes	Yes	Yes	Yes	Yes
Resistance to user forgery attack	Yes	Yes	Yes	Yes	Yes	Yes
Resistance to DoS attack	Yes	No	Yes	No	Yes	Yes
Revocability	Yes	No	Yes	Yes	No	Yes
User anonymity	No	Yes	No	Yes	No	Yes
Resistance to physical attack	No	No	No	No	No	Yes

The computation cost of these authentication schemes is compared as shown in Tab. 3. The cost of cryptographic operations is assumed as follows: Th = 0.00032 s, Ts = 0.0056 s, Chaotic map Tc = 0.0171 s, and fuzzy extractor function Tfc = 0.0171 s. The computation cost is the sum of the cost of user, sensor, and gateway nodes. Compared with the other algorithms, the proposed algorithm obtained low computation cost with high security. Additionally, the proposed algorithm obtained 9.6 ms of the authentication process, which was lower than that of the other authentication methods. Thus, the proposed system is faster than the other algorithms. The pictorial representation of computation cost comparison is shown in Fig. 2. The comparison of communication and storage costs is shown in Tab. 4.

Table 3: Computation cost comparison of authentication schemes

Schemes	User	Sensor	Gateway	Total computation cost	Total computation (ms)
Maitra et al.	21 T_h	7 T_h	10 T_h + 6 T_s	38 T_h + 6 T_s	33.66
Amin et al.	18 T_h	4 T_h	14 T_h	36 T_h	11.52
Zhou et al.	24 T_h	7 T_h	31 T_h	62 T_h	19.84
Wu et al.	6 T_h	0 T_h	0 T_h	39 T_h	12.48
Gope et al.	17 T_h	8 T_h	7 T_h	32 T_h	10.24
Proposed scheme	15 T_h	9 T_h	6 T_h	30 T_h	9.6

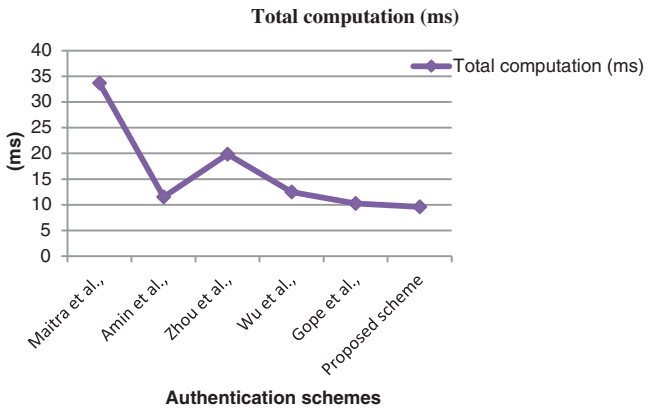

Figure 2: Comparison of authentication scheme considering computation cost

Table 4: Communication and storage cost comparison of authentication schemes

Schemes	Communication cost (bits)	Storage cost (bits)
Maitra et al.	3072	2530
Amin et al.	4736	1920
Zhou et al.	5760	3400
Wu et al.	2720	2240
Gope et al.	2400	2300
Proposed scheme	2300	1700

The observation of the comparison evaluation from Fig. 3 considering communication and storage costs proved that the proposed algorithm attained lesser communication and storage costs than the other existing approaches. The security level of storage bits for the hash values is 162 bits. The proposed authentication scheme utilized 2300 bits of communication cost and 1700 bits of storage cost for storing all the parameters.

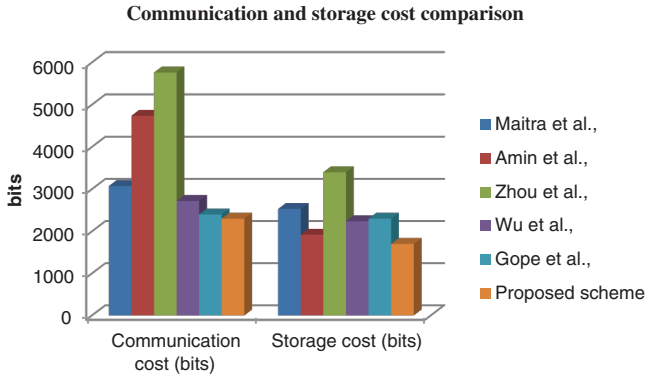

Figure 3: Storage and communication cost comparison of authentication schemes

Hence, the proposed method is more secure than all the existing schemes based on all levels of evaluation. The proposed method is superior not only in obtaining mutual authentication but also in resisting physical, DoS, and all kinds of forgery attacks with revocability and user and sensor anonymities. Thus, the proposed two-factor authentication with PUF is efficient for cloud IoT environments with fast computation and minimal storage cost.

5 Conclusions

Security is a major problem in every environment, such as IoT, cloud, big data, and networking. Additional intelligent techniques are needed to keep data away from intruders and attackers. The advantages of lightweight authentication and PUF are combined in this article to provide high security in IoT smart grid systems. These systems are deployed using cloud infrastructure for high storage processing. Two-factor authentications are highly considerable in cryptography and network security models. The proposed authentication schemes use hash functions, XOR operation, and concatenation operations for the authentication process. The comparative study considering computation, communication, and storage costs of the proposed 2FA will prove the efficiency of the proposed algorithm. The limitation of the security scheme lies in insider attacks. Moreover, the proposed algorithm succeeds in detecting the insiders in all cases. However, addressing remarkably sensitive insiders is

difficult. Machine learning-based sensitive authentication techniques can be used in the future for authentication. Machine learning plays a positive role in all data processing and communication techniques. Security is also highly required in every application. Similarly, machine learning schemes can be introduced for future intelligent authentication processes.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that there is no conflict of interest regarding the publication of the paper.

References

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

[2] M. Qi, J. Chen and Y. Chen, "A secure authentication with key agreement scheme using ECC for satellite communication systems," *International Journal of Satellite Communications and Networking*, vol. 37, no. 3, pp. 234–244, 2019.

[3] T. Kothmayr, C. Schmitt, W. Hu, M. Brünig and G. Carle, "DTLS based security and two-way authentication for the Internet of Things," *Ad Hoc Networks*, vol. 11, no. 8, pp. 2710–2723, 2013.

[4] H. Pranata, R. Athauda and G. Skinner, "Securing and governing access in ad-hoc networks of internet of things," in *Proc. EAS*, Colombo, Sri Lanka, pp. 84–90, 2012.

[5] M. Durairaj and K. Muthuramalingam, "A new authentication scheme with elliptical curve cryptography for Internet of Things (IoT) environments," *International Journal of Engineering and Technology*, vol. 7, no. 2.26, pp. 119–124, 2018.

[6] N. Hong, "A security framework for the internet of things based on public key infrastructure," *Advanced Materials Research*, vol. 671, pp. 3223–3226, 2013.

[7] P. Hao, X. Wang and W. Shen, "A collaborative PHY-aided technique for end-to-end IoT device authentication," *IEEE Access*, vol. 6, pp. 42279–42293, 2018.

[8] K. Mahmood, S. A. Chaudhry, H. Naqvi, T. Shon and H. F. Ahmad, "A lightweight message authentication scheme for smart grid communications in power sector," *Computers & Electrical Engineering*, vol. 52, no. 4, pp. 114–124, 2016.

[9] S. Challa, A.K. Das, V. Odelu, N. Kumar, S. Kumari *et al.,* "An efficient ECC-based provably secure three-factor user authentication and key agreement protocol for wireless healthcare sensor networks," *Computers & Electrical Engineering*, vol. 69, no. 6, pp. 534–554, 2018.

[10] L. Lamport, "Password authentication with insecure communication," *Communications of the ACM*, vol. 24, no. 11, pp. 770–772, 1981.

[11] J. Katz, P. MacKenzie, G. Taban and V. Gligor, "Two-server password-only authenticated key exchange," in *Proc. ICACNS*, New York, NY, USA, pp. 1–16, 2005.

[12] T. Xiang, K. Wong and X. Liao, "Cryptanalysis of a password authentication scheme over insecure networks," *Journal of Computer and System Sciences*, vol. 74, no. 5, pp. 657–661, 2008.

[13] H. M. Sun and H. T. Yeh, "Password based authentication and key distribution protocols with perfect forward secrecy," *Journal of Computer and System Sciences*, vol. 72, no. 6, pp. 1002–1011, 2006.

[14] J. Zhang, J. Cui, H. Zhong, Z. Chen and L. Liu, "PA-CRT: Chinese remainder theorem based conditional privacy-preserving authentication scheme in vehicular ad-hoc networks," *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 2, pp. 722–735, 2019.

[15] T. H. Chen and W. K. Shih, "A robust mutual authentication protocol for wireless sensor networks," *ETRI Journal*, vol. 32, no. 5, pp. 704–712, 2010.

[16] R. Amin, S. Islam, M. K. Khan, A. Karati, D. Giri *et al.,* "A two-factor RSA-based robust authentication system for multiserver environments," *Security and Communication Networks*, vol. 2017, no. 13, pp. 1–15, 2017.

[17] Z. Y. Wu, Y. C. Lee, F. Lai, H. C. Lee and Y. Chung, "A secure authentication scheme for telecare medicine information systems," *Journal of Medical Systems*, vol. 36, no. 3, pp. 1529–1535, 2012.

[18] D. He, N. Kumar, J. Chen, C. C. Lee, N. Chilamkurti *et al.,* "Robust anonymous authentication protocol for health-care applications using wireless medical sensor networks," *Multimedia Systems*, vol. 21, no. 1, pp. 49–60, 2015.

[19] X. Li, J. Niu, M. Karuppiah, S. Kumari and F. Wu, "Secure and efficient two-factor user authentication scheme with user anonymity for network based e-health care applications," *Journal of Medical Systems*, vol. 40, no. 12, pp. 1–12, 2016.

[20] C. C. Lee, M. S. Hwang and I. E. Liao, "Security enhancement on a new authentication scheme with anonymity for wireless environments," *IEEE Transactions on Industrial Electronics*, vol. 53, no. 5, pp. 1683–1687, 2006.

[21] M. L. Das, "Two-factor user authentication in wireless sensor networks," *IEEE Transactions on Wireless Communications*, vol. 8, no. 3, pp. 1086–1090, 2009.

[22] D. He, Y. Gao, S. Chan, C. Chen and J. Bu, "An enhanced two-factor user authentication scheme in wireless sensor networks," *Ad Hoc & Sensor Wireless Networks*, vol. 10, no. 4, pp. 361–371, 2010.

[23] M. K. Khan and K. Alghathbar, "Cryptanalysis and security improvements of two-factor user authentication in wireless sensor networks," *Sensors*, vol. 10, no. 3, pp. 2450–2459, 2010.

[24] R. Amin, S. H. Islam, G. Biswas, M. K. Khan and N. Kumar, "A robust and anonymous patient monitoring system using wireless medical sensor networks," *Future Generation Computer Systems*, vol. 80, no. 4, pp. 483–495, 2018.

[25] S. Kumari and H. Om, "Authentication protocol for wireless sensor networks applications like safety monitoring in coal mines," *Computer Networks*, vol. 104, no. 1, pp. 137–154, 2016.

[26] Q. Jiang, J. Ma, G. Li and L. Yang, "An enhanced authentication scheme with privacy preservation for roaming service in global mobility networks," *Wireless Personal Communications*, vol. 68, no. 4, pp. 1477–1491, 2013.

[27] S. Sathesh, V. A. Pradheep, S. Maheswaran, P. Premkumar, S. Gokul Nathan *et al.,* "Computer vision based real time tracking system to identify overtaking vehicles for safety precaution using single board computer," *JARDCS*, vol. 12, no. SP7, pp. 1551–1561, 2020.

[28] M. Shanmugam and A. Ramasamy, "Sensor-based turmeric finger growth characteristics monitoring using embedded system under soil," *International Journal of Distributed Sensor Networks*, vol. 10, no. 6, pp. 476176, 2014.