PUF-ILM: A PUF-Enabled Authentication Scheme for Internet of Vehicles Using Improved Logical Mapping

Sajjad Hussain Chauhdary, *Senior Member, IEEE*, Tengfei Ma, Linhua Jiang, Farrukh Aslam Khan, *Senior Member, IEEE*, Ashok Kumar Das, *Senior Member, IEEE*, and Shehzad Ashraf Chaudhry, *Senior Member, IEEE*

***Abstract*—This article proposes a lightweight two-way authentication scheme, PUF-ILM, that integrates physical unclonable function (PUF) and improved logistic map (ILM). The PUF generates unique challenge-response pairs (CRPs) for each device using its inherent physical randomness, thereby achieving reliable device identity authentication. The ILM encrypts and obfuscates the transmitted CRPs by enhancing their chaotic characteristics, expanding the parameter range, and eliminating periodic windows, effectively resisting modeling and eavesdropping attacks. Security analysis indicates that this scheme possesses several known security attributes, including anti-cloning, anonymity, two-way authentication, forward/backward security, and anti-machine-learning modeling. Performance evaluation shows that PUF-ILM maintains low communication overhead while maintaining a simple system structure and does not rely on complex hardware or external trusted institutions, offering high security and strong practicality, making it especially suitable for large-scale deployment in resource-constrained Internet of Vehicles environments.**

***Index Terms*—Internet of Vehicles, logistic mapping, physical unclonable function (PUF), resource-constrained.**

NOMENCLATURE

D_i, GW_i	Device, gateway.
$\mathrm{PID}_i, \mathrm{PID}_{\mathrm{TM}}$	Pseudo-identity of the device in round i.
$\mathrm{RID}_i, \mathrm{RID}_{\mathrm{GWi}}$	Real identity of the device.
$h()$	One-way hash function.
$\|\|$	Connection operation.
(C_i, R_i)	Challenge and response pair.
$L_r(x)$	ILM map.
$\mathrm{RN}_d, \mathrm{RN}_u, \mathrm{RN}_s, r, s$	Random number.
T, T_u, T_s	Timestamp.
$\oplus$	Heterodyne operation.
SK	Session key.

Received 6 January 2026; accepted 16 January 2026. Date of publication 20 January 2026; date of current version 26 March 2026. *(Corresponding author: Linhua Jiang.)*

Sajjad Hussain Chauhdary, Tengfei Ma, and Linhua Jiang are with the School of Information Engineering, Huzhou University, Huzhou 313000, China (e-mail: 60717@zjhu.edu.cn; 2024388226@stu.zjhu.edu.cn; 11594@zjhu.edu.cn).

Farrukh Aslam Khan is with the Center of Excellence in Information Assurance (CoEIA), King Saud University, Riyadh 11653, Saudi Arabia (e-mail: fakhan@ksu.edu.sa).

Ashok Kumar Das is with the Center for Security, Theory and Algorithmic Research, International Institute of Information Technology, Hyderabad 500032, India, and also with the Department of Computer Science and Engineering, College of Informatics, Korea University, Seongbuk-gu, Seoul 02841, South Korea (e-mail: ashok.das@iiit.ac.in).

Shehzad Ashraf Chaudhry is with the Department of Computer Science and Information Technology, College of Engineering, Abu Dhabi University, Abu Dhabi, United Arab Emirates, and also with the Department of Software Engineering, Faculty of Engineering and Architecture, Nisantasi University, 34398 Istanbul, Türkiye (e-mail: ashraf.shehzad.ch@gmail.com).

Digital Object Identifier 10.1109/JIOT.2026.3656432

I. INTRODUCTION

WITH the advancement of the IoV [1], [2], issues such as data theft, information tampering, and malicious attacks on user devices during information exchange persistently emerge, posing substantial risks and challenges to a stable societal environment [3], [4]. For example, although the onboard unit (OBU) in vehicles is designed to be tamper-resistant, attackers can extract private information stored within through side-channel attacks or power analysis attacks [5], [6]. In scenarios where devices are left unattended, they become vulnerable to physical attacks, including side-channel analysis, memory extraction, and reverse engineering, potentially resulting in the leakage of sensitive information such as cryptographic keys. Conventional authentication protocols often fail to provide adequate protection against such physical attacks [7], [8].

It is evident that security remains a primary concern for lightweight devices today. Current technologies employed to safeguard information transmission and prevent privacy leakage in such devices include physical-layer authentication [9], [10], blockchain [11], [12], fog computing [13], [14], [15], and physical unclonable function (PUF) [16], [17], among others. Designing schemes and protocols that ensure communication security and privacy protection for lightweight devices has become a key research focus in related fields. For instance, Cui et al. [16] proposed an authentication key agreement protocol based on chaotic maps to enable secure remote control of autonomous vehicles. Their approach establishes three independent session keys among the user, data center (DC), and autonomous vehicle to construct a secure communication channel, with a trusted private key generated during authentication via PUF. Wang and Mu [18] introduced a lightweight vehicle-to-roadside (V2R) authentication protocol utilizing PUF and Chebyshev chaotic mapping. This method uses a fuzzy extractor to mitigate environmental impacts on

PUF responses and leverages the cryptographic strengths of Chebyshev chaotic mapping to establish a secure session key while achieving mutual authentication in V2R scenarios. Alawida et al. [19] developed a block cipher algorithm based on an enhanced logistic chaotic map, incorporating a novel chaotic method with multiplicative inverse functions to improve properties such as ergodicity and entropy, thereby enhancing the overall performance of logistic chaotic mapping.

The current security risks faced by lightweight devices include the following aspects:

1) Cryptographic keys serve as a critical mechanism for ensuring information security in lightweight devices. However, during key management processes—including key generation, distribution, storage, and updating—any vulnerability may allow attackers to decrypt communication content and access sensitive data. Such weaknesses significantly escalate security risks in vehicular systems [20], [21], [22].
2) Given the limited computational power, storage, and energy in lightweight devices, the design of authentication protocols places a paramount emphasis on low overhead and high operational efficiency. Thus, in contrast to traditional identity authentication protocols, those for lightweight devices are required to attain a level of efficiency and accuracy that is at least on par with conventional approaches, yet under a stringent resource budget [23], [24], [25].
3) During the device identity authentication process, continuous communication with the server is required. Attackers can exploit technical means to spoof the device's identity, thereby gaining unauthorized access to the lightweight device system and performing malicious operations [10], [26].

To address the aforementioned challenges, this article adopts the PUF—known for its resistance to counterfeiting and theft, thereby offering enhanced security—and integrates it with an improved logistic chaotic map to ensure secure information communication in lightweight devices. On this basis, we propose a lightweight device authentication scheme leveraging PUF and the improved logistic map (ILM). The scheme employs PUF to achieve reliable identity authentication, while the chaotic and parameter-sensitive properties of the logistic map are utilized to encrypt challenge-response pair (CRP), thus ensuring their confidentiality during transmission. Furthermore, the inherent lightweight nature of PUF helps minimize the computational and storage costs of the solution, facilitating its deployment across a large network of resource-constrained devices and providing robust support for secure interdevice communication. The main contributions of this work are summarized as follows:

1) We propose a lightweight authentication scheme that utilizes a PUF for mutual authentication and key agreement, thereby countering man-in-the-middle attacks. By leveraging an ILM to protect CRPs in insecure channels, the scheme also achieves robust resistance against physical and machine-learning attacks.
2) While resource constraints are a common limitation in lightweight devices, the proposed scheme effectively exploits the lightweight nature of PUF to significantly alleviate the authentication overhead. This ensures that even resource-limited devices can achieve secure system access and efficient information transmission.
3) By leveraging the PUF, the scheme achieves mutual authentication between devices without relying on traditional cryptographic operations like key storage and digital signatures. This significantly lowers the computational and storage demands on the devices, thereby simultaneously improving the security of the communication channel.

The remainder of this article is organized as follows: Section II reviews related work. Section III details the preliminaries of PUF and logistic mapping, and conducts a multifaceted analysis of the ILM. Section IV elaborates on the proposed scheme, detailing the registration and authentication stages. The security analysis and performance evaluation of the scheme are presented in Sections V and VI. Finally, Section VII concludes this article.

II. Related Work

Driven by the increasing scale of the IoV, attention has shifted toward data and privacy security in mobile devices. Conventional authentication schemes are infeasible for lightweight devices due to their high computational and storage demands. To address this, we introduce an authentication scheme that leverages PUF to replace traditional methods and employs logistic mapping to strengthen CRP security, thereby providing a practical solution for resource-constrained devices.

Kim et al. [22] introduced a PUF-based authentication scheme for IoT devices, which alleviates the server-side burden by storing and updating only a single CRP. Each authentication session employs a newly generated CRP to encrypt messages, thereby enhancing security. However, this approach remains vulnerable to machine-learning-based modeling attacks. Also, Nozaki and Yoshikawa [23] developed a PUF authentication method based on secret sharing. Their technique derives shares from the PUF response values via a secret sharing scheme and uses these distributed values during authentication. By avoiding direct use of raw PUF responses, the method improves resilience against machine-learning attacks. Nevertheless, the authentication process is computationally complex and introduces additional communication overhead, making it less suitable for resource-constrained devices. Ding et al. [26] proposed a lightweight anonymous authentication protocol for resource-constrained IoT environments. The protocol adopts signcryption and related techniques to reduce communication and computational costs. While it exhibits advantages in terms of efficiency and certain security aspects, it does not guarantee security across all practical deployment scenarios. Siddiqui et al. [24] presented a digital certificate authentication mechanism combining PUF and public key infrastructure (PKI), which incorporates two certificate authorities to improve security. However, the use of digital certificates and PKI introduces implementation complexity and increases the computational

load, rendering it less practical for lightweight IoT devices. Tun and Mambo [25] designed a PUF-based authentication system that leverages Paillier homomorphic encryption or plaintext equality testing. This allows a verifier to authenticate devices without accessing plaintext CRPs, thus reducing local computation. However, the introduced cryptographic techniques increase the overall system complexity. Singh et al. [20] developed an anonymous authentication and key establishment mechanism based on elliptic curve cryptography (ECC). Their design strengthens resistance against conventional and differential attacks while reducing certain system complexities. Nonetheless, the scheme requires users and network nodes to store substantial data—such as ECC parameters and keys—and relies heavily on elliptic curve point multiplication. As a result, it is not well-suited for resource-constrained devices.

Given the considerable computational overhead of ECC algorithms, they are often unsuitable for resource-constrained IoV devices. As a result, many researchers have turned to chaotic maps as alternatives to ECC in the design of authentication schemes. Cui et al. [16] proposed a three-factor authentication and key agreement protocol based on chaotic maps, which enables users, DCs, and vehicles to securely exchange confidential information, thereby addressing security issues in remote control systems. However, this protocol involves multiple complex cryptographic operations, which may impose a significant burden on lightweight devices. Wang and Mu [18] introduced a vehicular authentication protocol employing PUF and Chebyshev chaotic maps. Their scheme leverages the favorable cryptographic properties of Chebyshev chaotic maps to achieve mutual authentication and secure session key establishment. Nevertheless, the identity tracking and revocation mechanisms employed introduce additional communication overhead and latency. More recently, Lu and Song [21] developed a data encryption scheme for the IoV based on a generative adversarial network (GAN) and a logistic chaotic algorithm, enhancing the security of data transmission. However, the training process of the GAN is highly complex and demands substantial computational resources and time.

Nevertheless, a number of currently proposed PUF-based authentication schemes exhibit certain limitations in terms of either security or suitability for lightweight devices. These shortcomings stem primarily from specific flaws in their design methodologies, which can be summarized as follows:

1) Many schemes are critically vulnerable to machine-learning modeling attacks. By acquiring a set of CRPs, an attacker can exploit machine learning to accurately mimic the target PUF. This directly undermines the fundamental security guarantees of unclonability and unpredictability. As demonstrated against the schemes [18], [20], [23], successful CRP extraction leads directly to a successful modeling attack, highlighting a common design flaw.
2) *High Computational Overhead:* Schemes [21], [24], [26], incorporate ECC, which demands considerable computational resources. This poses a significant challenge for their deployment on resource-constrained devices.
3) *Excessive System Complexity:* Although the encryption algorithms employed in [16], [22], [23], and [25], provide data confidentiality, their implementation involves intricate procedures. This significantly increases the overall system complexity and, consequently, the difficulty of practical deployment.

Although chaotic mappings such as the Chebyshev mapping are widely used, in order to strike a balance between efficiency and security, this article chose ILM. It maintains simplicity while expanding the chaotic range, eliminating the periodic window, and being more sensitive to parameters, effectively resisting differential and statistical attacks. Compared with existing schemes, PUF-ILM demonstrates multiple advantages: it does not require complex hardware or external trusted institutions, has a simple system structure, and has a lower cost; the computational and storage overhead is extremely low, suitable for resource-constrained devices; by encrypting CRP with chaotic mappings and updating the key in real time, it is difficult to model or forge; only the basic PUF circuit is needed, avoiding the complexity and risks of biometric devices or dynamic reconfiguration. PUF-ILM integrates the mathematical enhancement of a single PUF and ILM, maintaining high security while being easier to deploy on a large scale, with higher practicality and reliability. The specific comparison is shown in Table I.

III. General Methodology

A. Physical Unclonable Functions

For traditional authentication schemes, they usually store confidential information such as keys in electrically erasable programmable read-only memory (EEPROM) or static random access memory (SRAM) and protect the confidential information through some encryption operations. However, traditional authentication schemes have many security vulnerabilities and are vulnerable to various attacks. As an emerging security technology for hardware, PUF can generate a unique identifier for each chip through the random physical characteristics during the chip manufacturing process, playing a significant role in key generation and authentication. Its response value does not need to be stored in the chip or external storage devices and can be extracted in real time from the hardware structure of the chip. Moreover, its value is determined by its internal physical properties and is technically very difficult to replicate or clone [29], [30]. However, PUF is susceptible to external environmental factors such as temperature and noise, which may cause PUF to respond differently to the challenges of response. Therefore, in the practical application of PUF, the influence of these factors should be fully considered, and various measures should be taken to reduce the interference of these factors on PUF and improve its stability and reliability.

The PUF operates by leveraging inherent microscopic variations within the device to map an input challenge (C) to a corresponding output response (R). This mapping is both unique and uncloneable, making it suitable for use as a device-specific identifier. The mapping process is formally defined by the following equation and illustrated in Fig. 1:

$$\mathrm{PUF}(C) \rightarrow R. \tag{1}$$

TABLE I
COMPARISON TABLE OF PUF-ILM WITH EXISTING FRAMEWORKS

Research	Proposed method	Advantages of PUF-ILM
[16]	Based on the enhanced Chebyshev chaotic mapping and PUF	Not relying on complex hardware such as smart cards or biometric devices, the system has a low level of complexity.
[18]	V2R Authentication Scheme Based on PUF and Chebyshev	Chaotic Mapping and Supports two-way authentication and key negotiation, without relying on a centralized TA, and is more suitable for a distributed architecture.
[21]	Chaos Logistic Trajectory Encryption Method Based on GAN	Avoids the need for a large amount of computing power to train the model and is suitable for resource-constrained devices.
[26]	Anonymity Authentication Protocol Based on ECC and Signcryption Technology	CRP is encrypted by chaotic mapping, making it difficult to model. The session key parameters are updated in real time, making it hard to forge.
[27]	A lightweight AKE protocol based on PUF and TinyJAMBU	Not relying on external trust institutions or high-performance computing devices.
[28]	Process biometric features using the fuzzy extractor and encrypt with TinyJAMBU	Only a basic PUF circuit is required, without the need for biometric recognition devices, which reduces the cost.

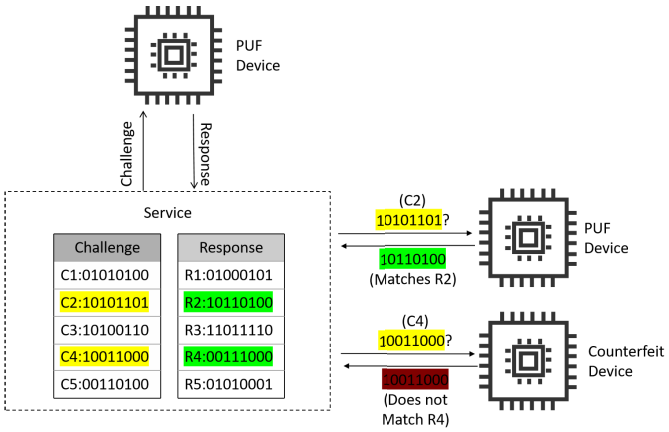

Fig. 1. CRP generation and authentication.

PUF exhibits essential security properties including unclonability, unpredictability, and inherent randomness. These characteristics prevent attackers from reliably deriving or replicating the associated confidential information, thereby significantly enhancing the overall security of the system.

B. Fuzzy Extractor

In this article, since the response of PUF is susceptible to environmental changes during actual deployment, a fuzzy extractor is introduced to correct the bit error problem of CRP. The fuzzy extractor consists of two parts. The generation part takes the response R of PUF as input and outputs a key K and public auxiliary data P. In the reproduction part, using the public auxiliary data P and the new noisy measurement value R' as inputs, the original R is restored, and then the key K is generated from the recovered R. This mechanism enables the fuzzy extractor to effectively handle the influence of PUF caused by external environmental changes while ensuring security.

C. Logistic Map

The logistic map exhibits characteristics such as discreteness, high randomness, low computational cost, and sensitivity to initial conditions, rendering it highly suitable for authentication applications. Compared to alternative approaches like ECC and exponentiation operations, the logistic map not only consumes less computational energy but also provides enhanced system security. These advantages make it particularly advantageous for implementation in resource-constrained devices. Its sensitivity to initial conditions and system parameters introduces a high degree of unpredictability into the encryption process, thereby effectively resisting statistical analysis and differential attacks [31]. This section briefly introduces the formal definition of the logistic map and its relevant cryptographic properties.

The logistic map represents a classic nonlinear iterative system. Despite having only a single control parameter, it exhibits ideal chaotic properties—including high unpredictability and extreme sensitivity to initial conditions—that render it highly suitable for cryptographic applications. Its mathematical definition is given by the following equation:

$$x_{n+1} = r * x_n * (1 - x_n). \tag{2}$$

In the logistic map, x_n denotes the value at the nth iteration, typically confined to the interval (0, 1), while r is a control parameter within the range [0, 4] that governs the dynamic behavior of the system. The value x_{n+1}, representing the result of the subsequent iteration, is computed from the current state x_n and parameter r according to the defining equation.

However, the limited chaotic parameter range and low complexity of the classical logistic map restrict its security for cryptographic applications. To overcome these limitations, researchers have enhanced the original mapping by introducing additional parameters and initial values, as well as extending their valid ranges [32].

In this study, we propose an improved chaotic method, which is based on perturbing the underlying chaotic method and utilizing the generated chaotic sequence to implement a formula that is highly sensitive due to the use of the multiplicative inverse function. The proposed method is formally defined by the following equation:

$$x_{n+1} = \left(\frac{e^k}{e^{r * x_n * (1 - x_n)}} \right) \bmod 1. \tag{3}$$

The variable x_n denotes the current value in the sequence, confined to the interval [0, 1]. The control parameter r, defined over [0, 4], governs the dynamic behavior of the system. The

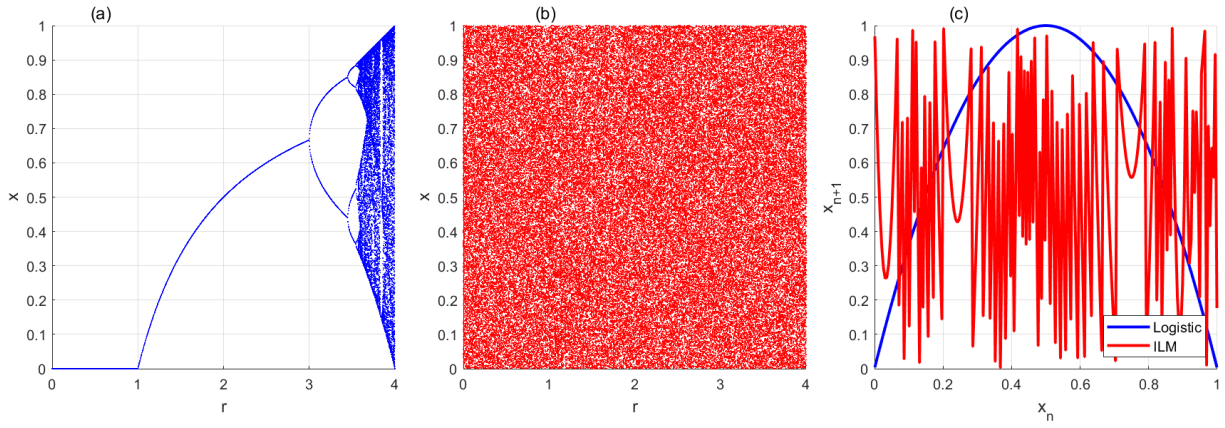

Fig. 2. Bifurcation diagram and iterative function graph. (a) Logistic map bifurcation diagram. (b) ILM bifurcation diagram. (c) Iterative function graph.

subsequent value x_{n+1} is derived from the current state x_n, and n represents the iteration index. A constant k is introduced to modulate the sensitivity and chaotic characteristics of the mapping. In ILM, the K value strikes a balance between chaotic complexity and computational efficiency. Although a larger K value can enhance the testing effectiveness of Lyapunov exponents (LEs) and entropy, it also increases the computational cost. The recommended range of the K value in this article is [5, 10]. Considering that while ensuring the lightweight nature of the computation, it should also possess sufficient chaotic characteristics to meet the security requirements of cryptography; in this article, K is set to 7.

The sensitivity to initial conditions and control parameters plays a decisive role in the emergence of chaotic behavior, particularly when these parameters vary significantly. Such sensitivity can drive the system to transition from an ordered to a chaotic state. When multiple functions are combined, their respective contributions to chaotic behavior generation may differ substantially. In particular, compared to the standard logistic map, the fractional function exhibits higher nonlinearity in its mathematical structure, leading to a stronger response to minor input perturbations and demonstrating a more pronounced effect in inducing chaotic dynamics.

D. Chaos Analysis

1) Bifurcation Diagram: The classical logistic map suffers from a narrow chaotic parameter range and numerous periodic windows, resulting in a nonuniform distribution of its chaotic sequences over the interval [0, 1], as illustrated in Fig. 2(a). In cryptographic applications, such periodic windows may reduce the effective key space, thereby increasing vulnerability to brute-force attacks. Expanding the range of chaotic parameters is therefore essential for enhancing security by enlarging the key space. The relationship between chaotic states and control parameters can be visualized using bifurcation diagrams, which depict the extent of chaotic behavior. As shown in Fig. 2(b), the ILM eliminates periodic windows entirely—regardless of the value of parameter r—and produces state variables that are uniformly distributed across [0, 1]. These results demonstrate that the proposed model not only broadens the chaotic parameter range but also completely suppresses periodic windows, outperforming the classical logistic map in both aspects.

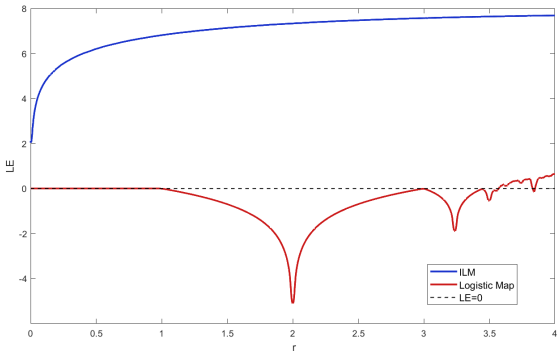

Fig. 3. Comparison of LEs of logistic map and ILM map.

2) Iterative Function Graph: To characterize the fundamental properties of chaotic maps and evaluate their behavioral complexity, iterative function graphs are employed to analyze their dynamic characteristics. These graphs provide an intuitive means of distinguishing between simple and complex dynamical systems. Fig. 2(c) displays the iterative function graphs of the classical logistic map and the proposed ILM, respectively. As observed, the logistic map exhibits a smooth, parabolic profile—a unimodal structure indicative of relatively simple dynamics that are more susceptible to analysis. In such cases, key parameters or initial conditions can be inferred with relative ease from trajectory data. In contrast, the ILM presents a multimodal, irregularly distributed curve in radial space. This complex structure results in highly unpredictable behavior, enhancing its resistance to parameter estimation attacks based on trajectory analysis.

3) Lyapunov Exponent: The LE offers a quantitative measure of dynamical system stability [33], [34]. A system is considered stable if all its LEs are negative, whereas the presence of at least one positive LE indicates unstable or chaotic behavior. Fig. 3 compares the LE spectra of the classical logistic map and the proposed ILM. The logistic map

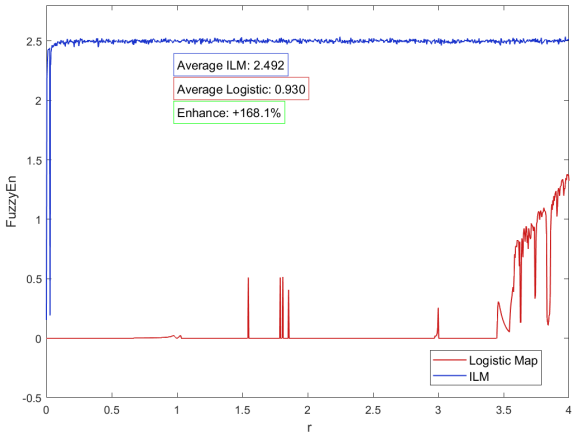

Fig. 4. Fuzzy entropy comparison chart.

exhibits positive LE values—and thus chaotic behavior—only within a specific, narrow parameter range, consistent with the chaotic regions identified in its bifurcation diagram. In sharp contrast, the ILM maintains positive LE values across a significantly broader span of control parameters. This demonstrates that the ILM sustains chaotic characteristics over an extended operational range, highlighting its enhanced utility for cryptographic applications.

4) Fuzzy Entropy: Highly complex systems often generate outputs devoid of discernible statistical patterns. In chaotic systems, substantial information is required to characterize their behavior, which is why they are generally described as complex. To quantitatively assess this complexity, we employ fuzzy entropy as a metric for evaluation.

Using identical parameters and initial conditions, the fuzzy entropy of both the classical and enhanced logistic maps was evaluated. The results, shown in Fig. 4, clearly indicate a higher fuzzy entropy value for the enhanced logistic map, reflecting its greater dynamical complexity. This elevated complexity makes behavioral prediction and pattern recognition substantially more challenging. For the fuzzy entropy calculation, a Gaussian membership function [35] was employed due to its computational efficiency and favorable mathematical properties, as defined in the following equation:

$$\theta \quad (\Delta_{\Lambda,\lambda}, r) = \exp\left(-\frac{\Delta_{\Lambda,\lambda}^{n_e}}{2r^2}\right). \tag{4}$$

Among them, r is a threshold parameter, $\Delta_{\Lambda,\lambda}$ represents the distance or difference between two sequences, and $\theta(\Delta_{\Lambda,\lambda}, r)$ represents the similarity between sequences Λ and λ.

E. Comparison and Discussion

ILM outperforms logistic mapping in all aspects of security and has better chaotic performance than logistic. To better demonstrate the performance of ILM, this section compares ILM with the improved logistic mapping proposed in other literature. Using LE and FuzzyEn as evaluation criteria, the sensitivity and complexity of ILM and other improved logistic mappings are compared. To ensure the fairness of the comparison, this article implements and tests the improved logistic mapping on the same device and platform, and calculates the average values of these indicators. Due to the fact that logistic mapping only has continuous chaotic states in the range [3.57, 4], for intuitive representation, this part of the calculation is taken and plotted as shown in Table II. It can be observed that ILM outperforms other chaotic mappings in these two representative indicators.

TABLE II
COMPARISON OF CHAOTIC MAPPING PERFORMANCE

Chaotic maps	LE	FuzzyEn
ILM	7.668	2.492
Logistic map	0.330	0.930
Enhanced Logistic Mapping [19]	6.428	2.191
CLM [32]	6.129	2.101
TM-DFSM [36]	1.387	1.421
LSC [37]	1.412	1.532
IST [38]	3.736	1.985

Based on the above test results, ILM outperforms logistic mapping and some improved chaotic mappings in terms of bifurcation characteristics, LE, and FuzzyEn measures. The results demonstrate that by integrating the multiplicative inverse function into the formula construction of ILM, not only can its parameter sensitivity be enhanced, but the generated sequence also significantly improves in cryptographic properties.

F. Adversarial Model

In this study, the Dolev–Yao (DY) model and the Canetti–Krawczyk (CK) model were employed to conduct a rigorous security assessment of the PUF-ILM protocol [27], [28], [39]. In addition, the oracle query mechanism of the real or random (ROR) model was combined to depict the capabilities of the attacker. The DY model grants the attacker $\mathcal{A}$ complete control over the public communication channel, allowing interception, tampering, replaying, or injecting any protocol messages, and obtaining parameters such as L_{RN_d} and PID_i transmitted in the channel. However, it is assumed that the attacker cannot directly crack the hash function, the unclonability of the PUF, or the chaotic mapping and other underlying cryptographic primitives. The CK model, on this basis, further allows the attacker to obtain long-term secrets such as $\{\mathrm{PID}_i, K, R_i\}$ stored by the device or gateway through the leakage of long-term keys, and to obtain specific session keys SK through the leakage of session keys, thereby evaluating the robustness of the protocol in terms of forward security, key leakage, and resistance to impersonation and other stronger threats. The ROR introduced can formally quantify the threat of the attacker to the semantic security of the cryptographic key.

IV. AUTHENTICATION SCHEME BASED ON PUF AND THE IMPROVED LOGISTIC MAPPING

This study designs an efficient authentication mechanism tailored for resource-constrained devices in the IoV. The proposed scheme incorporates a lightweight PUF to provide resilience against external physical attacks and ensure the

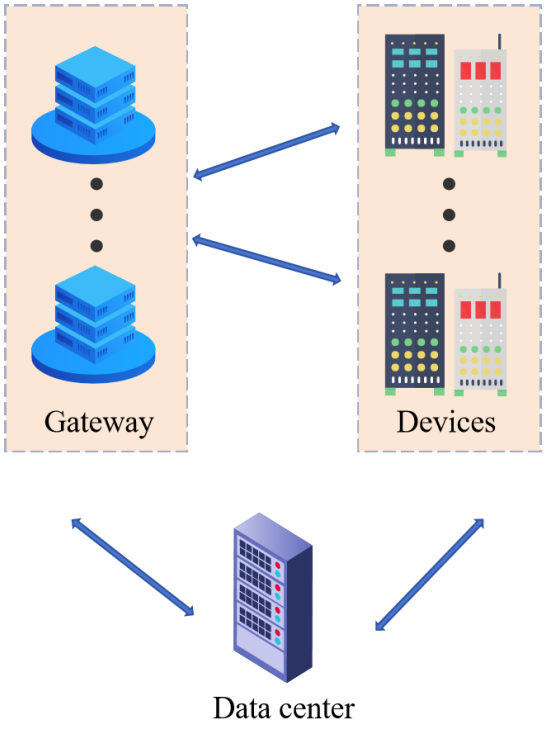

Fig. 5. System model.

integrity of device identities. Furthermore, the logistic chaotic map is introduced into the design owing to its lightweight nature, unpredictability, and high randomness. Its integration enhances both the confidentiality and integrity of information during transmission.

In the proposed scheme, all PUFs are assumed to operate under ideal conditions, satisfying key security properties such as randomness, unpredictability, and unclonability, and are unaffected by external interference. The notations used in the registration and mutual authentication phases of the scheme are summarized in Nomenclature.

A. System Model

Based on the architectures described in [16], [18], and [29], the authentication model in this scheme comprises three main entities: gateways, devices, and a DC. This framework enables mutual authentication between terminal devices and gateways, as illustrated in Fig. 5. The specific implementation details of the proposed scheme are elaborated below.

1) Gateway: As a core component of the authentication process, the gateway is responsible for forwarding authentication information and device-collected data to the DC or relevant databases.

2) Devices: These refer to resource-constrained units deployed across various facilities. All devices are assumed to be equipped with a PUF, which serves as a critical element throughout the authentication procedure.

3) Data Center: The DC manages the registration and authentication of legitimate devices. It supports devices by storing and aggregating substantial amounts of contextual data in databases, without actively participating in the real-time authentication process.

B. Registration Stage

The device registration phase is illustrated in Fig. 6. During this stage, both the device and the gateway register with the DC through a secure channel. The specific procedure consists of the following steps:

1) *Step 1:* D_i selects its own identity RID_i and temporary identity RID_{TM} and sends them to DC. GW_i selects its own identity $\text{RID}_{\text{GW}i}$ and sends it to DC.
2) *Step 2:* DC generates random numbers C_i, C_{TM}, r, RN_u, s, computes the pseudo-identities $\text{TID}_i = h(r \| \text{RID}_{\text{GW}_i})$, $\text{PID}_i = h(C_i \| \text{RID}_i)$, $\text{PID}_{\text{TM}} = h(C_{\text{TM}} \| \text{RID}_{\text{TM}})$, then derives the shared secret $W = h(\text{PID}_i \| \text{TID}_i \| s)$ and $K = \text{RN}_u \oplus W$, and finally sends $\{C_i, C_{\text{TM}}, \text{PID}_i, \text{PID}_{\text{TM}}, K\}$ to D_i and $\{W, \text{TID}_i\}$ to GW_i.
3) *Step 3:* D_i acquires the message and stores PID_i, PID_{TM}, K in the device. The device takes C_i and C_{TM} in the message as the input of PUF, calculates the response R_i and R_{TM}, and sends the message $\{R_i, R_{\text{TM}}\}$ to DC. GW_i securely stores the message $\{W, \text{TID}_i\}$ in the gateway memory.
4) *Step 4:* DC computes $L_{\text{TID}_i} = L_{\text{TID}_i}(x)$ and publicly reveals x, p, L_{TID_i}; store RID_{GWi}, RID_i, RID_{TM}. In addition, DC sends $\{(C_i, R_i, \text{PID}_i), (C_{\text{TM}}, R_{\text{TM}}, \text{PID}_{\text{TM}})\}$ to GW_i.
5) *Step 5:* GW_i updates its stored information to W, TID_i, (C_i, R_i, PID_i), $(C_{\text{TM}}, R_{\text{TM}}, \text{PID}_{\text{TM}})$.

C. Certification Stage

The certification stage is as follows: In this process, mutual authentication between the device and gateway is achieved using the authentication parameters and information obtained during registration, followed by the negotiation of a session key for subsequent secure communication. The detailed steps are outlined below.

1) *Step 1:* As shown in Algorithm 1. D_i generates a random number RN_d, computes $L_{\text{RN}_d} = L_{\text{RN}_d}(x)$, $L_{\text{RN}_d \cdot \text{TID}_i} = L_{\text{RN}_d}(L_{\text{TID}_i})$, $K^* = K \oplus L_{\text{RN}_d \cdot \text{TID}_i}$, and then creates the request authentication message $\{L_{\text{RN}_d}, \text{PID}_i, K^*\}$ and sends it to GW_i.
2) *Step 2:* As shown in Algorithm 2. Upon receiving the authentication request from D_i, GW_i first searches its database for PID_i; if PID_i is absent, GW_i rejects the request and D_i reinitiates authentication using PID_{TM}, while GW_i authenticates the devices with $(C_{\text{TM}}, R_{\text{TM}}, \text{PID}_{\text{TM}})$. Otherwise, GW_i retrieves (C_i, R_i) and generates random RN_s and timestamp T_s.GW_i computes $L_{\text{RN}_d \cdot \text{TID}_i} = L_{\text{TID}_i}(L_{\text{RN}_d})$, $\text{RN}_u = K^* \oplus L_{\text{RN}_d \cdot \text{TID}_i} \oplus W$, $L_{R_i \cdot \text{RN}_d \cdot \text{TID}_i} = L_{R_i}(L_{\text{RN}_d \cdot \text{TID}_i})$, $C_i^* = C_i \oplus L_{\text{RN}_d \cdot \text{TID}_i}$, $\text{RN}_s^* = \text{RN}_s \oplus L_{R_i \cdot \text{RN}_d \cdot \text{TID}_i}, R_i \oplus W$, $V_0 = (L_{R_i \cdot \text{RN}_d \cdot \text{TID}_i} \| \text{RN}_u \| \text{RN}_s \| T_s)$, then sends $\{C_i^*, \text{RN}_s^*, R_i \oplus W, V_0, T_s\}$ to D_i.
3) *Step 3:* As shown in Algorithm 3. D_i checks whether the transmission delay satisfies $|T - T_s| < \Delta t$; if $|T - T_s| \geq \Delta t$, the authentication terminates. D_i computes $W = R_i \oplus W \oplus R_i$ and $\text{RN}_u = K \oplus W$, then derives V_0'; if $V_0' = V_0$, authentication of D_i to GW_i succeeds;

Algorithm 1 Device Authentication Request (Generate M1)

Input: $\{PID_i, K, L_{TID_i}\}$
Output: $\{L_{RN_d}, PID_i, K^*\}$
procedure P-1(PID_i, K, L_{TID_i})
  generate random RN_d
  $L_{RN_d} \leftarrow L_{RN_d}(x)$
  $L_{RN_dTID_i} \leftarrow L_{RN_d}(L_{TID_i})$
  $K^* \leftarrow K \oplus L_{RN_dTID_i}$
  $M_1 \leftarrow \{L_{RN_d}, PID_i, K^*\}$
  send M_1 to GW_i
end procedure

Algorithm 2 Gateway Verification and Response (Generate M2)

Input: $\{M_1, W, PID_{TM}, (C_i, R_i, PID_i)\}$
Output: $\{C_i^*, RN_s^*, R_i \oplus W, V_0, T_s\}$
procedure P-2($M_1, W, TID_i, (C_i, R_i, PID_i)$)
  extract L_{RN_d}, PID_i, K^* from M_1
  if PID_i not found in database then
    use backup PID_{TM} and $(C_{TM}, R_{TM}, PID_{TM})$
    Verification phase halted if not found
  else
    retrieve (C_i, R_i) associated with PID_i
    generate random RN_s, timestamp T_s
    $L_{RN_dTID_i} \leftarrow L_{TID_i}(L_{RN_d})$
    $RN_u \leftarrow K^* \oplus L_{RN_dTID_i} \oplus W$
    $L_{R_iRN_dTID_i} \leftarrow L_{R_i}(L_{RN_dTID_i})$
    $C_i^* \leftarrow C_i \oplus L_{RN_dTID_i}$
    $RN_s^* \leftarrow RN_s \oplus L_{R_iRN_dTID_i} \oplus R_i \oplus W$
    $V_0 \leftarrow h(L_{R_iRN_dTID_i} \| RN_u \| RN_s \| T_s)$
    $M_2 \leftarrow \{C_i^*, RN_s^*, R_i \oplus W, V_0, T_s\}$
    send M_2 to D_i
  end if
end procedure

Algorithm 3 Device Validation and Session Key Generation (Generate M3)

Input: $\{M_2, R_i, K, W\}$
Output: $\{R_{i+1}^*, V_1, T_u\}$
procedure P-3(M_2, R_i, K, W)
  extract $C_i^*, RN_s^*, R_i \oplus W, V_0, T_s$ from M_2
  if $|T_{current} - T_s| \geq \Delta t$ then
    Verification phase halted
  else
    $W \leftarrow (R_i \oplus W) \oplus R_i$
    $RN_u \leftarrow K \oplus W$
    compute $V_0' = h(L_{R_iRN_dTID_i} \| RN_u \| RN_s \| T_s)$
    if $V_0' = V_0$ then
      generate timestamp T_u, random n
      $C_{i+1} \leftarrow h(C_i \| RN_u)$
      $R_{i+1} \leftarrow PUF(C_{i+1})$
      $PID_{i+1} \leftarrow h(RID_i \| R_i \| RN_s)$
      $SK \leftarrow h(RN_u \| R_{i+1} \| L_{R_iRN_dTID_i})$
      $V_1 \leftarrow h(RN_s \| SK \| T_u)$
      $RN_u' \leftarrow n$
      $R_{i+1}^* \leftarrow R_{i+1} \oplus RN_s$
      $K' \leftarrow RN_u' \oplus W$
      store PID_{i+1}, K'
      $M_3 \leftarrow \{R_{i+1}^*, V_1, T_u\}$
      send M_3 to GW_i
    else
      Verification phase halted
    end if
  end if
end procedure

otherwise, it fails. D_i generates a timestamp T_u and random number n for C_i, then computes $C_{i+1} = h(C_i \| \mathrm{RN}_u)$, $R_{i+1} = \mathrm{PUF}(C_{i+1})$, $\mathrm{PID}_{i+1} = h(\mathrm{RID}_i \| R_i \| \mathrm{RN}_s)$, $\mathrm{SK} = h(\mathrm{RN}_u \| R_{i+1} \| L_{R_i \cdot \mathrm{RN}_d \cdot \mathrm{TID}_i})$, $V_1 = h(\mathrm{RN}_s \| \mathrm{SK} \| T_u)$, sets $\mathrm{RN}_u' = n$, $R_{i+1}^* = R_{i+1} \oplus \mathrm{RN}_s$, $K' = \mathrm{RN}_u' \oplus W$, and sends the message $\{R_{i+1}^*, V_1, T_u\}$ while storing PID_{i+1} and K'.

4) *Step 4:* As shown in Algorithm 4. GW_i verifies $|T - T_u| < \Delta t$; if $|T - T_u| \geq \Delta t$ the authentication terminates. Otherwise, it computes $R_{i+1} = R_{i+1}^* \oplus \mathrm{RN}_s$ and $\mathrm{SK} = h(\mathrm{RN}_u \| R_{i+1} \| L_{R_i \cdot \mathrm{RN}_d \cdot \mathrm{TID}_i})$, so GW_i authentication succeeds. Finally, it GW_i calculates $C_{i+1} = h(C_i \| \mathrm{RN}_u)$, $\mathrm{PID}_{i+1} = h(\mathrm{PID}_i \| R_i \| \mathrm{RN}_s)$ and stores $(C_{i+1}, R_{i+1}, \mathrm{PID}_{i+1})$ in its gateway memory.

V. Safety Analysis

A. Informal Security Verification

1) Resistant to Cloning and Physical Attacks: PUF possesses inherent unclonability, ensuring that even if attackers gain physical access to device memory or hardware, they cannot replicate the PUF's output. Furthermore, the device stores only a pseudo-identity and the key K, preventing exposure of authentication-related sensitive parameters such as RN_u. As a result, attackers are unable to impersonate legitimate devices during authentication or extract device-sensitive information through physical means.

2) Anonymity and Nontraceability: Throughout the authentication process, all communication between the device and the gateway is conducted using pseudo-identities, which are updated upon completion of each authentication session. This mechanism ensures that attackers cannot obtain the true device identifiers RID_i and $\mathrm{RID}_{\mathrm{TM}}$ during data exchange. Consequently, the proposed scheme provides both anonymity and untraceability.

3) Two-Way Authentication: In this scheme, the device authenticates the gateway by verifying the validity of $V_0' \stackrel{?}{=} V_0$. The gateway verifies the device by verifying the validity of $V_1' \stackrel{?}{=} V_1$. Two-way authentication between the device and the gateway is achieved through the above two-step verification. Attackers who want to crack the secret values such as RN_u and RN_S contained in V_0 and V_1 will have to face the problem of chaotic mapping of discrete logarithms, which makes the cracking difficult. Moreover, RN_u and RN_s do not transmit in plaintext form in the channel, so attackers cannot obtain secret values to impersonate legitimate terminal devices and join the authentication.

Algorithm 4 Gateway Final Verification and Update

Input: $\{M_3, RN_s, RN_u, L_{R_i RN_d TID_i}\}$
Output: $\{SK, (C_{i+1}, R_{i+1}, PID_{i+1})\}$
procedure P-4($M_3, RN_s, RN_u, L_{R_i RN_d TID_i}$)
  extract R^*_{i+1}, V_1, T_u from M_3
  if $|T_{current} - T_u| \geq \Delta t$ then
    Verification phase halted
  else
    $R_{i+1} \leftarrow R^*_{i+1} \oplus RN_s$
    $SK \leftarrow h(RN_u \| R_{i+1} \| L_{R_i RN_d TID_i})$
    compute $V'_1 = h(RN_s \| SK \| T_u)$
    if $V'_1 = V_1$ then
      $C_{i+1} \leftarrow h(C_i \| RN_u)$
      $PID_{i+1} \leftarrow h(PID_i \| R_i \| RN_s)$
      store $(C_{i+1}, R_{i+1}, PID_{i+1})$
    else
      Verification phase halted
    end if
  end if
end procedure

4) Resistant to Replay and Tampering Attacks: The proposed scheme incorporates a timestamp mechanism to verify whether message transmission delays remain within acceptable limits. Timestamps are embedded in both V_0 and V_1, and the secret values contained therein are updated promptly after each authentication session. Any tampering with the timestamps by an attacker will result in immediate authentication failure. Furthermore, all message exchanges during authentication are protected using cryptographic hash functions, which significantly reduces the risk of interception or modification over insecure channels. Together, these measures provide effective resistance against replay and tampering attacks.

5) Anti-DoS Attack and Desynchronization Attack: When an attacker attempts to disrupt communication by flooding the device and gateway with excessive messages, both entities will first validate the transmission delay. Subsequently, the values of V_0 and V_1 are verified. If any of these checks fail, the authentication process is immediately terminated. Moreover, in the event of a communication interruption, the device can reinitiate an authentication request using its temporary pseudo-identity PID_{TM}, while the gateway authenticates the device based on the stored (C_{TM}, R_{TM}). As a result, the proposed scheme provides robust defense capabilities against both denial-of-service (DoS) and desynchronization attacks.

6) Resist Simulated Attacks: Any attempt by an adversary to impersonate a legitimate device or gateway is effectively prevented due to the lack of essential cryptographic elements. To impersonate a device, the attacker must generate valid authentication tokens, which requires knowledge of confidential key parameters—information that remains inaccessible. Similarly, impersonation of the gateway fails as the attacker lacks both the legitimate CRP and the correct encryption parameters. In both scenarios, the absence of these critical components renders identity forgery infeasible.

7) Forward/Backward Safety: In the proposed scheme, the session key is generated as $\text{SK} = h(\text{RN}_u \| R_{i+1} \| L_{R_i \cdot \text{RN}_d \cdot \text{TID}_i})$. Here, SK, R_{i+1}, and $L_{R_i \cdot \text{RN}_d \cdot \text{TID}_i}$ are updated after every authentication session. Even if an attacker acquires current device secrets and a subset of CRPs through unauthorized means, the continually refreshed session key prevents the adversary from tracing the device's communication data. As a result, the scheme ensures both forward and backward secrecy.

B. Resistant to Machine-Learning Modeling Attacks

In this scheme, although attackers may intercept CRP from insecure channels, they must first compute $L_{\text{RN}_d} \cdot L_{\text{TID}_i}$ to derive the challenge value C_i. This requires solving the discrete logarithm problem associated with the chaotic map, which is computationally infeasible. Furthermore, due to the one-way property of the hash function, an adversary cannot reverse-engineer the original response R_i from its hashed value. Without access to a sufficient volume of PUF-generated CRP, attackers cannot construct an accurate model of the PUF behavior. Therefore, the proposed scheme effectively resists machine-learning-based modeling attacks.

To quantitatively analyze the resistance of machine-learning models to attacks, this article simulates an attacker who can collect up to 10 000 challenge responses from public channels. In this test, we used MLP and SVM trained with 80% of the collected data. Firstly, without using ILM encryption, the prediction accuracy of MLP was as high as 95.3% and that of SVM was as high as 95.4%. However, when we encrypted and obfuscated the challenge responses using ILM, the accuracy dropped to 49.5% and 48.8%, respectively, which was close to random guessing. This confirms the reasoning in the previous part of this article, that ILM can effectively disrupt the learnability of challenge responses and mitigate the impact of machine-learning attacks. The simulation results are shown in Fig. 7.

C. Security Verification Based on ROR Model

The ROR model is a commonly used testing method in the formal security analysis of authentication and key exchange protocols. ROR can quantify the attacker's ability to crack the session key by providing a strict framework. In other words, it can determine whether the attacker can distinguish between a real or randomly generated SK. This model can confirm the confidentiality of the SK, the resistance of the protocol to eavesdropping, tampering, simulation, etc., and the overall security of the protocol. In the process of proving security, the attacker needs to distinguish between the real session key and an equivalent-length random string. The attacker's advantage is defined as the degree to which the probability of correct distinction deviates from random guessing. If this advantage can be ignored, it indicates that the protocol satisfies the semantic security of the session key, proving that it can resist various attacks such as eavesdropping and simulation.

1) Model and Definition: Before conducting a formal security verification of PUF-ILM, the basic definitions related to the ROR model are introduced first. Considering that the PUF-ILM protocol involves two types of participants, namely device D_i and gateway GW, and each participant runs a protocol instance denoted as $\Pi^S_{D_i}$ and Π^S_{GW}, where S is the

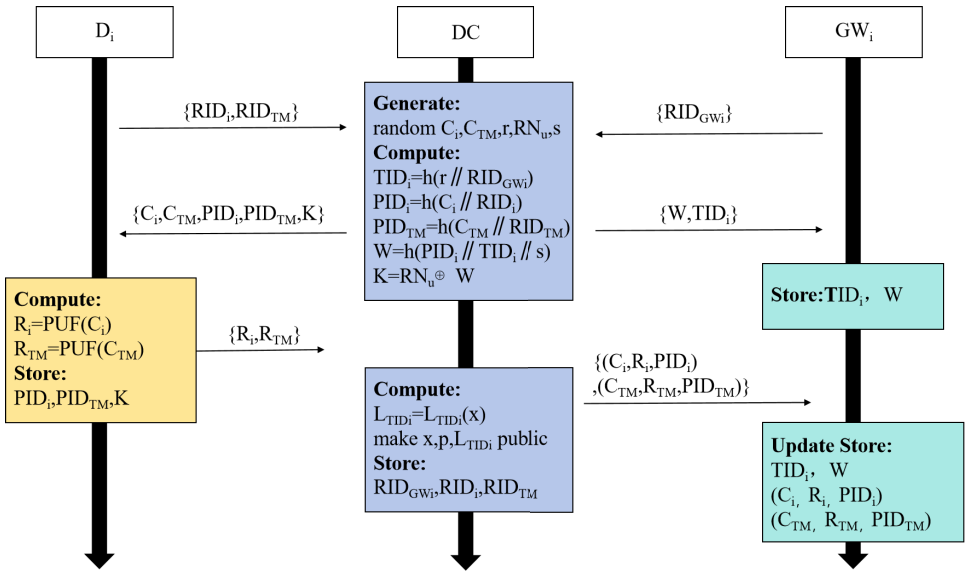

Fig. 6. Device registers with the gateway.

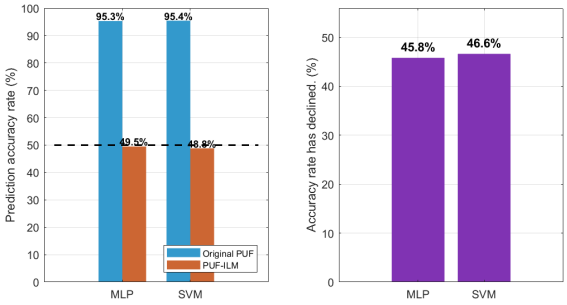

Fig. 7. Experiment on anti-machine-learning attacks.

session identifier, to make the proof more general, $\Pi_{U_1}^S$ and $\Pi_{U_2}^S$ will be used instead of $\Pi_{D_i}^S$ and Π_{GW}^S in the formal verification. The attacker $\mathcal{A}$ is a polynomial-time algorithm that can fully control the communication channel and can query the interaction with the protocol instance through the following oracle.

1) *Execute*($\Pi_{U_1}^{S_1}$, $\Pi_{U_2}^{S_2}$): Obtain all the messages generated by the execution of the protocol between instances $\Pi_{U_1}^{S_1}$ and $\Pi_{U_2}^{S_2}$.
2) *Send*(Π_U^S, m): Send the message m to the instance Π_U^S and return the response generated by this instance according to the protocol specifications.
3) *Reveal*(Π_U^S): If the session key has been established, return the session key of the instance Π_U^S.
4) *CorruptDevice*(D_i): Return the long-term secrets of device D_i, including the parameters $\{\text{PID}_i, K, R_i\}$ stored in the device.
5) *Test*(Π_U^S): This query can only be executed once. A random bit $b \in \{0, 1\}$ is selected. If $b = 1$, the actual session key of the instance Π_U^S is returned; if $b = 0$, a random string of the same length is returned.

Freshness condition: If the following conditions are met, it indicates that an instance Π_U^S is fresh.

1) The agreement has been successfully completed, and a session key has been established.
2) The session key of this instance was not leaked through the Reveal(Π_U^S) query.
3) The attacker did not perform CorruptDevice(D_i) on the devices involved in the session, meaning that the $\{\text{PID}_i, K, R_i\}$ stored in the devices was not retrieved by the attacker's query.

The attacker $\mathcal{A}$ objective is to win the game of querying Test(Π_U^S), that is, to guess the correct bit b. The definition of the attacker's advantage is

$$\mathcal{A}\text{dv}_{\mathcal{A}}^{\text{PUF-ILM}}(pt) = |2 \cdot \Pr[\mathcal{A}\text{wins}] - 1| \tag{5}$$

where pt represents the time during which the attacker was active.

2) Safety Assumption: Regarding the security analysis of PUF-ILM, this article makes the following hardness assumptions for cryptographic primitives.

1) *Hash function H:* Modeled as a random oracle, for any polynomial-time attacker, the advantage of distinguishing the hash output from a random string is negligible.
2) *PUF:* Suppose that PUF is unpredictable and unclonable, that is, given a series of CRPs (C_i, R_i), for a new challenge C^*, the advantage of predicting PUF(C^*) can be ignored, and the response of PUF has sufficient entropy.
3) *ILM:* Assuming that the discrete logarithm problem of chaotic mappings (CDLP) is difficult, for given $L_a(x)$ and $L_b(x)$, calculating $L_{ab}(x)$ is computationally infeasible.

3) Safety Theorem:

Theorem 1: Assuming that the PUF-ILM protocol operates under the random oracle model and that the PUF is unpredictable, the CDLP of ILM is computationally infeasible. Therefore, for any polynomial-time attacker $\mathcal{A}$, its advantage

satisfies

$$\mathcal{A}\mathrm{dv}_{\mathcal{A}}^{\text{PUF-ILM}}(pt) \le \frac{q_h^2}{2^{\ell_h+1}} + \frac{q_p^2}{2^{n+1}} + q_s \cdot \mathcal{A}\mathrm{dv}_{\mathcal{A}}^{\text{CDLP}}(pt) + \frac{q_s}{2^{\gamma}}. \quad (6)$$

Among them: q_h represents the number of queries to the random oracle, ℓ_h represents the length of the hash output, q_p represents the number of PUF queries, n is the length of the PUF response, q_s represents the number of Send queries, γ is the number of bits of the timestamp, and $\mathcal{A}\mathrm{dv}_{\mathcal{A}}^{\text{CDLP}}(\text{pt})$ represents the advantage in solving the CDLP problem.

4) Proof Outline: This part proves the theorem through a series of games. Let Succ_i be the event where the attacker wins in game G_i. The specific steps are as follows:

1) G_0*:* In this game, the attacker launches an attack on PUF-ILM. Therefore,
$$\mathcal{A}\mathrm{dv}_{\mathcal{A}}^{PUF\text{-ILM}}(pt) = \left|2 \cdot \Pr\left[\text{Succ}_0\right] - 1\right|. \quad (7)$$
2) G_1*:* In this game section, a simulated random oracle H is used. For each new hash query, a uniformly random response is selected and recorded. Since the hash function is modeled as a random oracle in the security assumption section, the attacker cannot distinguish between G_0 and G_1, except for hash collision cases. According to the birthday paradox, it can be concluded that
$$\left|\Pr\left[\text{Succ}_1\right] - \Pr\left[\text{Succ}_0\right]\right| \le \frac{q_h^2}{2^{\ell_h+1}}. \quad (8)$$
3) G_2*:* In this game, we simulate PUF queries. When the protocol requires a PUF response, we use random values instead. Due to the unpredictability of the PUF, the advantage that attackers have in distinguishing between a real PUF response and a random value can be disregarded. Therefore,
$$\left|\Pr\left[\text{Succ}_2\right] - \Pr\left[\text{Succ}_1\right]\right| \le \frac{q_p^2}{2^{n+1}}. \quad (9)$$
4) G_3*:* In game G_3, the security of the chaotic mapping is handled. That is, when the protocol needs to calculate $L_{\text{RN}_d\text{TID}_i}$ or $L_{R_i\text{RN}_d\text{TID}_i}$, random values are used instead, unless the attacker can solve the CDLP problem. Through these, we can obtain
$$\left|\Pr\left[\text{Succ}_3\right] - \Pr\left[\text{Succ}_2\right]\right| \le q_s \cdot \mathcal{A}\mathrm{dv}_{\mathcal{A}}^{\text{CDLP}}(pt). \quad (10)$$
5) G_4*:* In this section, we consider the validity of the timestamps, as attackers may launch attacks by replaying old messages. Since each message contains a timestamp and the recipient will check the freshness of the timestamp, that is, whether it is within Δt, the replay attack can be detected. For each send query, the probability that the attacker successfully fakes a fresh timestamp is at most $1/2\gamma$, therefore,
$$\left|\Pr\left[\text{Succ}_4\right] - \Pr\left[\text{Succ}_3\right]\right| \le \frac{q_s}{2^{\gamma}}. \quad (11)$$

In game G_4, all session keys are random values and have no relation to the protocol execution. Therefore, attackers have no advantage in guessing or testing bit b, that is,

$$\Pr\left[\text{Succ}_4\right] = \frac{1}{2}. \quad (12)$$

TABLE III
COMPARISON OF SECURITY FEATURES

	[18]	[40]	[41]	[42]	[43]	PUF-ILM
Resistant physical attacks	✓	✓	✓	✓	✓	✓
Anonymity	✓	✓	✓	✓	✓	✓
Non-traceability	✓	✓	✓	✓	✓	✓
Two-way authentication	✓	✓	✓	✓	✓	✓
Resistant replay attack	✓	✓	✓	✓	✓	✓
Resistant ML attack	×	×	×	×	×	✓
Resistant DoS attack	✓	✓	×	×	×	✓
Resistant desync attack	×	✓	×	✓	×	✓
Resistant MITM attack	✓	✓	✓	✓	✓	✓
Resistant simulated attack	✓	✓	✓	✓	✓	✓
Forward/backward safety	✓	✓	✓	✓	✓	✓

Based on all the above games, we make the following deductions:

$$\left|\Pr\left[\text{Succ}_0\right] - \frac{1}{2}\right| \le \frac{q_h^2}{2^{\ell_h+1}} + \frac{q_p^2}{2^{n+1}} + q_s \cdot \mathcal{A}\mathrm{dv}_{\mathcal{A}}^{\text{CDLP}}(pt) + \frac{q_s}{2^{\gamma}}. \quad (13)$$

Based on (6) and (13), we can infer that

$$\mathcal{A}\mathrm{dv}_{\mathcal{A}}^{\text{PUF-ILM}}(pt) = \left|2 \cdot \Pr\left[\text{Succ}_0\right] - 1\right| \le \frac{q_h^2}{2^{\ell}} + \frac{q_p^2}{2^{n}} + 2q_s \cdot \mathcal{A}\mathrm{dv}_{\mathcal{A}}^{\text{CDLP}}(pt) + \frac{q_s}{2^{\gamma-1}}. \quad (14)$$

Since q_h, q_p, and q_s are all polynomially bounded and $\mathcal{A}\mathrm{dv}_{\mathcal{A}}^{\text{CDLP}}(\text{pt})$ can be ignored, therefore $\mathcal{A}\mathrm{dv}_{\mathcal{A}}^{\text{PUF-ILM}}(\text{pt})$ can also be ignored. Thus, the security verification of PUF-ILM under the ROR model is proved, and it is secure.

VI. PERFORMANCE ANALYSIS

The proposed scheme described in Section IV was implemented on a PC platform using MATLAB, with extensive simulation experiments conducted under configured conditions. The experimental platform features an AMD Ryzen 9 7940HS processor, Windows 11 operating system, and 32 GB of RAM. In these simulations, an ideal PUF model was employed, thereby excluding the influence of environmental factors such as temperature-induced noise from consideration. This section presents a comparative analysis between the proposed scheme and existing approaches in terms of security attributes and computational efficiency, demonstrating the advantages of our method in authentication performance.

A. Comparison of Safety Features

Table III presents a comparison of the security features between this scheme and the existing ones. Wang and Mu [18], Mahmood et al. [40], and Irshad et al. [41] all employ encryption mechanisms but do not encrypt or obfuscate the input and output of the mapping. Attackers can obtain CRP through attack methods, leading to machine-learning modeling attacks. In this scheme, the leakage of CRP can be effectively prevented, and the resistance to machine-learning modeling attacks is enhanced. Wang and Mu [18] and Yu et al. [42]

TABLE IV
COMPARISON OF COMMUNICATION COST AND TOTAL TIME ACROSS DIFFERENT SCHEMES

Scheme	Communication cost (bit)	Total time (ms)
[18]	1952	$8T_h + 4T_L + T_{\text{ENC}} + T_{\text{Dec}} + 11T_{\text{PUF}} + 1T_{\text{FE,Rep}} = 21.53$
[40]	1568	$29T_h + 11T_{\text{ENC}} + T_{\text{Dec}} + T_{\text{FE,Rep}} = 10.57$
[41]	2048	$14T_h + 6T_L + 6T_{\text{ENC}} + 6T_{\text{Dec}} = 22.81$
[42]	1888	$8T_h + 3T_L + 11T_{\text{PUF}} = 11.05$
[43]	3296	$36T_h + 4T_{\text{PUF}} + 27T_{\text{ENC}} + 27T_{\text{Dec}} = 12.10$
PUF-ILM	1521	$13T_h + 5T_L + 2T_{\text{PUF}} + 1T_{\text{Rep}} = 10.43$

introduce mechanisms such as request frequency control and abnormal traffic detection, enabling attackers to send a large number of forged requests, consuming a significant amount of system resources and causing service disruptions. In this scheme, the introduction of V_0 and V_1 to verify the transmission delay can effectively prevent DoS attacks. In the scheme given in [18], attackers can send information to the server by forging identities, interrupting the authentication between the device and the server, and thus may be subject to desynchronization attacks. In this scheme, a pseudo-identity mechanism is established to resynchronize the device, enabling it to resist desynchronization attacks. In the schemes blacklisted in [40] and [43], attackers can predict or forge authentication responses by constructing mathematical models or simulating system behaviors, making it easy to model PUF responses and leading to the leakage of confidential information. In this scheme, the parameters of the session key SK are updated in real time, which can effectively resist simulated attacks.

B. Comparison of Computational Costs

Define T_h, T_{PUF}, T_L, T_{Enc}, T_{Dec}, T_{FE}, T_{Rep} as the time for executing the hash function, the time for the PUF response, the time for executing the chaotic mapping, the time for executing the encryption algorithm, the time for executing the decryption algorithm, and the time for restoring the fuzzy extractor, respectively. The performance comparison of each scheme is shown in Table IV.

The table presents a comparison of the computational costs between the scheme proposed in this article and those proposed in the cited literature. It can be seen from the overall time in the table that [18], [40] used resource-intensive elliptic curve point multiplication operations in their proposed schemes, resulting in computational costs of 21.53 and 10.57 ms, respectively. The schemes in [41] and [42] involve a large number of chaotic mapping operations, resulting in higher computational costs when compared with those in [18] and the schemes in this article. The fuzzy extractor function was used in the scheme proposed in [43], resulting in a computational cost of 12.1 ms at the controller node end. The scheme proposed in this article only relies on hash functions and logical mappings, with a total computational cost of 10.43 ms. Compared with the schemes proposed in other literature, the scheme proposed in this article significantly reduces the computational cost. Therefore, the scheme proposed in this article is suitable for lightweight devices with limited resources.

On the other hand, the communication costs between the scheme proposed in this article and other schemes are compared. The communication cost of the scheme proposed in this article is 1521 bits, which is slightly higher than that in [40], but significantly lower than that of the schemes proposed in other literature. Moreover, the computational costs of [18] and [41] are relatively high, and they are vulnerable to machine learning and physical attacks. By comparing all the schemes, the one proposed in this article not only maintains security but also reduces computing time and communication costs, making it suitable for resource-constrained lightweight devices.

VII. CONCLUSION

This article presents a lightweight device authentication scheme that integrates a PUF with an ILM, enabling mutual authentication and session key negotiation between devices and gateways. The proposed solution satisfies eleven security attributes, including resistance to cloning attacks, untraceability, mutual authentication, and robustness against machine-learning attacks. With a communication cost of 1521 bits and a computational cost of only 10.43 ms, the scheme offers significant advantages over existing approaches in both security and efficiency. It achieves stronger security properties such as two-way authentication and machine-learning resistance while maintaining lower computational and communication overhead, making it suitable for practical deployment in resource-constrained environments.

Future work may focus on migrating the authentication framework from simulation to embedded hardware platforms, enabling comprehensive evaluation of its performance and reliability under real-world conditions.

REFERENCES

[1] K. Abboud, H. A. Omar, and W. Zhuang, "Interworking of DSRC and cellular network technologies for V2X communications: A survey," *IEEE Trans. Veh. Technol.*, vol. 65, no. 12, pp. 9457–9470, Dec.2016.
[2] C.-M. Chen, Z. Li, A. K. Das, S. A. Chaudhry, and P. Lorenz, "Provably secure authentication scheme for fog computing-enabled intelligent social Internet of Vehicles," *IEEE Trans. Veh. Technol.*, vol. 73, no. 9, pp. 13600–13610, Sep.2024.
[3] C. Lai, J. Ma, X. Wang, H. Zhou, and D. Zheng, "A novel authentication and key agreement scheme for in-vehicle networks," *IEEE Trans. Veh. Technol.*, vol. 74, no. 6, pp. 9630–9644, Jun.2025.
[4] M. Tanveer, A. Aldosary, S.-U.-D. Khokhar, A. K. Das, S. A. Aldossari, and S. A. Chaudhry, "PAF-IoD: PUF-enabled authentication framework for the Internet of Drones," *IEEE Trans. Veh. Technol.*, vol. 73, no. 7, pp. 9560–9574, Jul.2024.
[5] S. M. Awais et al., "PUF-based privacy-preserving simultaneous authentication among multiple vehicles in VANET," *IEEE Trans. Veh. Technol.*, vol. 73, no. 5, pp. 6727–6739, May2024.

[6] H. Jiang, G. Wan, Y. Wei, and J. Li, "ECU authentication method based on PUF for in-vehicle networks," in *Proc. SIES*, Jan. 2024, pp. 99–103.
[7] X. Zhang, H. Wu, X. Tao, Z. Wei, C. Wang, and H. Li, "PUF-based lightweight group authentication for massive IoT access with insecure channel," *IEEE Internet Things J.*, vol. 12, no. 14, pp. 26968–26983, Jul.2025.
[8] A. Rullo et al., "PUF-based authentication-oriented architecture for identification tags," *IEEE Trans. Dependable Secure Comput.*, vol. 22, no. 1, pp. 66–83, Jan.2025.
[9] X. Luo, Y. Liu, H.-H. Chen, and Q. Guo, "Physical layer security in intelligently connected vehicle networks," *IEEE Netw.*, vol. 34, no. 5, pp. 232–239, Sep.2020.
[10] A. Farraj and E. Hammad, "A physical-layer security cooperative framework for mitigating interference and eavesdropping attacks in Internet of Things environments," *Sensors*, vol. 24, no. 16, p. 5171, Aug.2024.
[11] F. Wang, J. Cui, Q. Zhang, D. He, and H. Zhong, "Blockchain-based secure cross-domain data sharing for edge-assisted industrial Internet of Things," *IEEE Trans. Inf. Forensics Security*, vol. 19, pp. 3892–3905, 2024.
[12] Y. Liu and Y. Zhao, "A blockchain-enabled framework for vehicular data sensing: Enhancing information freshness," *IEEE Trans. Veh. Technol.*, vol. 73, no. 11, pp. 17416–17429, Nov.2024.
[13] E. Huaranga-Junco, S. González-Gerpe, M. Castillo-Cara, A. Cimmino, and R. García-Castro, "From cloud and fog computing to federated-fog computing: A comparative analysis of computational resources in real-time IoT applications based on semantic interoperability," *Future Gener. Comput. Syst.*, vol. 159, pp. 134–150, Oct.2024.
[14] F. Faraji, A. Javadpour, A. K. Sangaiah, and H. Zavieh, "A solution for resource allocation through complex systems in fog computing for the Internet of Things," *Computing*, vol. 106, no. 7, pp. 2107–2131, Jul.2024.
[15] A. Irshad, A. Aljaedi, Z. Bassfar, S. S. Jamal, M. Usman, and S. A. Chaudhry, "FA-SMW: Fog-driven anonymous lightweight access control for smart medical wearables," *IEEE Internet Things J.*, vol. 12, no. 4, pp. 4275–4285, Feb.2025.
[16] J. Cui, J. Yu, H. Zhong, L. Wei, and L. Liu, "Chaotic map-based authentication scheme using physical unclonable function for Internet of Autonomous Vehicle," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 3, pp. 3167–3181, Mar.2023.
[17] S. A. Majmaie, N. P. Bhatta, P. P. Kharat, and F. Amsaad, "PUF-based hardware security for trusted Internet of Drones: Challenges and future directions," in *Proc. SATC*, Jan. 2025, pp. 1–7.
[18] H. Wang and H. Mu, "A lightweight v2r authentication protocol based on puf and Chebyshev chaotic map," *J. Comput.*, vol. 34, no. 2, pp. 99–112, 2023.
[19] M. Alawida, J. S. Teh, A. Mehmood, A. Shoufan, and W. H. Alshoura, "A chaos-based block cipher based on an enhanced logistic map and simultaneous confusion-diffusion operations," *J. King Saud Univ.-Comput. Inf. Sci.*, vol. 34, no. 10, pp. 8136–8151, Nov.2022.
[20] A. K. Singh, A. Nayyar, and A. Garg, "A secure elliptic curve based anonymous authentication and key establishment mechanism for IoT and cloud," *Multimedia Tools Appl.*, vol. 82, no. 15, pp. 22525–22576, Jun.2023.
[21] X. Lu and W. Song, "Improved trajectory data encryption method for Internet of Vehicles using GAN-based chaotic logistic algorithm," *Alexandria Eng. J.*, vol. 114, pp. 719–727, Feb.2025.
[22] B. Kim, S. Yoon, Y. Kang, and D. Choi, "PUF based IoT device authentication scheme," in *Proc. ICTC*, Oct. 2019, pp. 1460–1462.
[23] Y. Nozaki and M. Yoshikawa, "Secret sharing schemes based secure authentication for physical unclonable function," in *Proc. ICCCS*, Feb. 2019, pp. 445–449.
[24] Z. Siddiqui, J. Gao, and M. Khurram Khan, "An improved lightweight PUF–PKI digital certificate authentication scheme for the Internet of Things," *IEEE Internet Things J.*, vol. 9, no. 20, pp. 19744–19756, Oct.2022.
[25] N. W. Tun and M. Mambo, "Secure PUF-based authentication systems," *Sensors*, vol. 24, no. 16, p. 5295, Aug.2024.
[26] X. Ding, X. Wang, Y. Xie, and F. Li, "A lightweight anonymous authentication protocol for resource-constrained devices in Internet of Things," *IEEE Internet Things J.*, vol. 9, no. 3, pp. 1818–1829, Feb.2022.
[27] M. Tanveer, A. G. Alharbi, and S. A. Aldossari, "RePUF-IoT: Reconfigurable PUF-based authentication protocol for IoT-driven healthcare systems," *IEEE Internet Things J.*, vol. 12, no. 22, pp. 47575–47587, Nov.2025.
[28] M. Tanveer, K. Toor, A. G. Alharbi, and S. R. Hassan, "SecTwin: A secure and efficient authentication mechanism for vehicular digital twins," *J. Inf. Secur. Appl.*, vol. 95, Dec.2025, Art. no. 104292.
[29] Z. Huang et al., "Improve SAC in PUFs: Metric, analysis, algorithm, and application," *IEEE Internet Things J.*, vol. 12, no. 16, pp. 34258–34272, Aug.2025.
[30] P. Vijayakumar, A. S. Rajasekaran, M. Azees, D. Ramasamy, and M. Karuppiah, "Probably secure PUF-based anonymous mutual and batch authentication for inter-vehicular communications in VANET," *IEEE Trans. Veh. Technol.*, early access, 2025, doi: 10.1109/TVT.2025.3600097.
[31] S. Chen, S. Feng, W. Fu, and Y. Zhang, "Logistic map: Stability and entrance to chaos," *J. Phys., Conf. Ser.*, vol. 2014, no. 1, Sep. 2021, Art. no. 012009.
[32] M. Riaz et al., "Secure and fast image encryption algorithm based on modified logistic map," *Information*, vol. 15, no. 3, p. 172, Mar.2024.
[33] I. V. Alexandrova and A. I. Belov, "Synthesis of discretized Lyapunov functional method and the Lyapunov matrix approach for linear time delay systems," *Automatica*, vol. 171, Jan.2025, Art. no. 111793.
[34] L. Zhang, W. Yu, and S. Gao, "Chaos of exponential logistic map," *Discrete Dyn. Nature Soc.*, vol. 2025, no. 1, Jan.2025, Art. no. 6620626.
[35] H. Azami, P. Li, S. E. Arnold, J. Escudero, and A. Humeau-Heurtier, "Fuzzy entropy metrics for the analysis of biomedical signals: Assessment and comparison," *IEEE Access*, vol. 7, pp. 104833–104847, 2019.
[36] M. Alawida, J. S. Teh, A. Samsudin, and W. H. Alshoura, "An image encryption scheme based on hybridizing digital chaos and finite state machine," *Signal Process.*, vol. 164, pp. 249–266, Nov.2019.
[37] Z. Hua, Y. Zhou, and H. Huang, "Cosine-transform-based chaotic system for image encryption," *Inf. Sci.*, vol. 480, pp. 403–419, Apr.2019.
[38] R. Soni, M. K. Thukral, and N. Kanwar, "A relative investigation of one-dimensional chaotic maps intended for light-weight cryptography in smart grid," *e-Prime-Adv. Electr. Eng., Electron. Energy*, vol. 7, Mar.2024, Art. no. 100421.
[39] A. Aldosary et al., "A secure authentication framework for consumer mobile crowdsourcing networks," *IEEE Trans. Consum. Electron.*, vol. 71, no. 2, pp. 4430–4442, May2025.
[40] K. Mahmood, Z. Ghaffar, M. Farooq, K. Yahya, A. K. Das, and S. A. Chaudhry, "A security enhanced chaotic-map-based authentication protocol for Internet of Drones," *IEEE Internet Things J.*, vol. 11, no. 12, pp. 22301–22309, Jun.2024.
[41] A. Irshad, G. A. Mallah, M. Bilal, S. A. Chaudhry, M. Shafiq, and H. Song, "SUSIC: A secure user access control mechanism for SDN-enabled IIoT and cyber–physical systems," *IEEE Internet Things J.*, vol. 10, no. 18, pp. 16504–16515, Sep.2023.
[42] S. Yu, N. Jho, and Y. Park, "Lightweight three-factor-based privacy-preserving authentication scheme for IoT-enabled smart homes," *IEEE Access*, vol. 9, pp. 126186–126197, 2021.
[43] Q. Xie and Y. Yao, "PUF and chaotic map-based authentication protocol for underwater acoustic networks," *Appl. Sci.*, vol. 14, no. 13, p. 5400, Jun.2024.

Sajjad Hussain Chauhdary (Senior Member, IEEE) received the Ph.D. degree from Korea University, Seoul, South Korea, in 2013.

He was appointed as an Associate Professor at the College of Computer Science and Engineering (CCSE), University of Jeddah, Jeddah, Saudi Arabia, from 2016 to 2024. Prior to his academic career, he spent five years as a Senior Research Engineer at LG/LSIS Company Ltd., and the Advanced Technology Research and Development Center, Anyang, South Korea. He is currently a Professor at the School of Information Engineering, Huzhou University, Huzhou, China. He is also the Director of the Intelligent Cyber-Systems Laboratory, Huzhou University. He led numerous impactful industrial and academic research projects funded by various governmental and cooperative organizations. He has been actively engaged in standardization efforts, contributing his expertise to major organizations, such as SAE International (standard J2831/1-5), ZigBee Alliance (SEP 2.0), and ISO/IEC (15118).

Dr. Chauhdary was recognized with the "Best Research Award" in 2012 and the "Best Project Award" in 2014.

Tengfei Ma is currently pursuing the master's degree with the School of Information Engineering, Huzhou University, Huzhou, China.

He is a member of the Intelligent Cyber-System Laboratory, Huzhou University. His research work focuses on issues related to cybersecurity.

Linhua Jiang received the B.Eng. degree from Shanghai Jiao Tong University, Shanghai, China, in 1999, the M.S. degree from the Catholic University of Leuven, Leuven, Belgium, in 2004, and the Ph.D. degree from Leiden University, Leiden, The Netherlands, in 2009.

He is currently a Professor at the School of Information Engineering, Huzhou University, Huzhou, China. He has published more than 100 scientific articles and conference papers. His current research interests include computer networks, cyber-physical systems, and parallel computing.

Farrukh Aslam Khan (Senior Member, IEEE) received the M.S. degree in computer system engineering from the GIK Institute of Engineering Sciences and Technology, Topi, Pakistan, in 2003, and the Ph.D. degree in computer engineering from Jeju National University, Jeju, South Korea, in 2007.

He is a Professor of cyber security at the Center of Excellence in Information Assurance (CoEIA), King Saud University, Riyadh, Saudi Arabia. He has over 25 years of teaching and research experience from various institutions. He also received professional training from Massachusetts Institute of Technology (MIT), Cambridge, MA, USA; New York University, New York, NY, USA; IBM, USA, and other institutions. He has supervised/co-supervised six Ph.D. students and 20 M.S. thesis students. He has co-organized several international conferences and workshops and has delivered many keynote and invited speeches. He has published over 145 research articles in refereed international journals and conferences.

Prof. Khan is a fellow of British Computer Society (BCS). He is on the editorial board of several prestigious international journals.

Ashok Kumar Das (Senior Member, IEEE) received the M.Sc. degree in mathematics, the M.Tech. degree in computer science and data processing, and the Ph.D. degree in computer science and engineering from IIT Kharagpur, Kharagpur, India, in 1998, 2000, and 2008, respectively.

He is currently a full Professor with the Center for Security, Theory and Algorithmic Research, IIIT, Hyderabad, India. He is a distinguished Adjunct Professor with the Department of Computer Science and Engineering, College of Informatics, Korea University, Seoul, South Korea. He was also a visiting Research Professor with the Virginia Modeling, Analysis and Simulation Center, Old Dominion University, Suffolk, VA, USA. He has authored over 530 papers in international journals and conferences in the above areas, including over 455 reputed journal papers. His Google Scholar h-index is 99 and i10-index is 368 with over 30,700 citations. His research interests include cryptography, system and network security, blockchain, security in the Internet of Things (IoT), Internet of Vehicles (IoV), Internet of Drones (IoD), smart grids, smart city, cloud/fog computing, intrusion detection, AI/ML security, quantum, and post-quantum cryptography.

Dr. Das was a recipient of the Institute Silver Medal from IIT Kharagpur. He has been listed in the Web of Science (Clarivate^{TM}) Highly Cited Researcher 2022 and 2023 in recognition of his exceptional research performance. He is/was on the editorial board of IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, IEEE SYSTEMS JOURNAL, *Journal of Network and Computer Applications* (Elsevier), *Computer Communications* (Elsevier), *International Journal of Communication Systems* (Wiley), *Journal of Cloud Computing* (Springer), *Cyber Security and Applications* (Elsevier), *Alexandria Engineering Journal* (Elsevier), *IET Communications*, *KSII Transactions on Internet and Information Systems*, and *International Journal of Communication Systems* (Wiley). He also served as one of the Technical Program Committee Chairs of the first International Congress on Blockchain and Applications (BLOCKCHAIN'19), Avila, Spain, June 2019, International Conference on Applied Soft Computing and Communication Networks (ACN'20), October 2020, Chennai, India, second International Congress on Blockchain and Applications (BLOCKCHAIN'20), L'Aquila, Italy, October 2020, and International Conference on Applied Soft Computing and Communication Networks (ACN'23), December 2023, Bangalore, India.

Shehzad Ashraf Chaudhry (Senior Member, IEEE) received the master's and Ph.D. degrees (Hons.) from International Islamic University Islamabad, Islamabad, Pakistan, in 2009 and 2016, respectively.

He is currently a Professor of cybersecurity engineering at the Department of Computer Science and Information Technology, College of Engineering, Abu Dhabi University, Abu Dhabi, United Arab Emirates. He is also affiliated with Department of Software Engineering, Nisantasi University, Istanbul, Türkiye. He has authored over 200 scientific publications in international journals and conference proceedings, including more than 180 articles indexed in Web of Science journals. He is a Leading Researcher in cybersecurity, and his research has been featured in leading magazines, journals, and conferences, including several IEEE Magazines, Transactions, and Journals, in addition to his featured articles in Elsevier and Springer journals. He is the inventor of two patents, with additional patent applications currently filed. With an H-index of 55, an i10-index of 140, and an accumulated impact factor exceeding 700, he work has been cited over 8400 times. He supervised over 40 graduate students, guiding them in advanced research across diverse areas. His current research interests include lightweight cryptography, elliptic curve cryptography, multimedia security, e-payment systems, MANETs, SIP authentication, smart grid security, the IoT and cloud infrastructure security, and next-generation networks.

Prof. Chaudhry has delivered numerous keynote speeches, moderated and participated in several panel discussions, and received multiple awards for best research papers. Over several years, he has been recognized among the world's leading computer scientists by Research.com and has also been listed among the rising stars of computer science. From 2020 to 2025, he consistently ranked among the Top 2% of computer scientists globally, according to Stanford University's annual report. He was a recipient of the Gold Medal for achieving 4.0/4.0 CGPA in his master's. In recognition of his research contributions, Pakistan Council for Science and Technology awarded him the prestigious Research Productivity Award, affirming his position among the most productive computer scientists in Pakistan.