Computers, Materials & Continua

Tech Science Press

Doi:10.32604/cmc.2025.058802

ARTICLE

Real-Time Identity Authentication Scheme Based on Dynamic Credentials for Power AIGC System

Feng Wei*, Zhao Chen, Yin Wang, Dongqing Liu, Xun Zhang and Zhao Zhou

State Grid Gansu Electric Power Research Institute, Lanzhou, 730000, China

* Corresponding Author: Feng Wei. Email: weifeng2407@163.com

Received: 21 September 2024; Accepted: 13 December 2024; Published: 06 March 2025

ABSTRACT: The integration of artificial intelligence (AI) with advanced power technologies is transforming energy system management, particularly through real-time data monitoring and intelligent decision-making driven by Artificial Intelligence Generated Content (AIGC). However, the openness of power system channels and the resource-constrained nature of power sensors have led to new challenges for the secure transmission of power data and decision instructions. Although traditional public key cryptographic primitives can offer high security, the substantial key management and computational overhead associated with these primitives make them unsuitable for power systems. To ensure the real-time and security of power data and command transmission, we propose a lightweight identity authentication scheme tailored for power AIGC systems. The scheme utilizes lightweight symmetric encryption algorithms, minimizing the resource overhead on power sensors. Additionally, it incorporates a dynamic credential update mechanism, which can realize the rotation and update of temporary credentials to ensure anonymity and security. We rigorously validate the security of the scheme using the Real-or-Random (ROR) model and AVISPA simulation, and the results show that our scheme can resist various active and passive attacks. Finally, performance comparisons and NS3 simulation results demonstrate that our proposed scheme offers enhanced security features with lower overhead, making it more suitable for power AIGC systems compared to existing solutions.

KEYWORDS: Cyber security; identity authentication; dynamic credential update; AIGC

1 Introduction

Smart grids are designed to improve the efficiency of energy distribution by using advanced sensors, communication technologies, and automated controls. However, the sheer volume and velocity of data generated by these systems pose significant challenges for traditional data processing, transmission methods, and data security [1]. The real-time transmission of Artificial Intelligence (AI)-generated data offers a solution by providing a representation of grid status and performance metrics. This approach not only facilitates faster decision-making but also enhances the ability of grid operators to monitor and respond to anomalies in real time. Of course, the secure transmission of real-time data is a prerequisite for ensuring the accuracy of decision-making. Therefore, in order to achieve secure real-time transmission of power monitoring data and Artificial Intelligence Generated Content (AIGC) data, implementing advanced encryption and authentication protocols is essential to prevent unauthorized access and ensure the integrity of the transmitted information [2].

In the era of digital transformation, the integration of AI with smart grid technologies has emerged as a powerful paradigm, revolutionizing the way we manage and optimize energy systems [3]. One of the

most compelling advancements in this field is the real-time data transmission scheme for AIGC, which plays a crucial role in enhancing the efficiency and reliability of smart grids [4]. Particularly with the recent development of large language models, AIGC has become a key player in decision-making within the field of data analysis and processing. As energy grids become increasingly complex and interconnected, the need for rapid, accurate, and secure data exchange has never been more critical. This real-time data transmission scheme aims to address these challenges by leveraging AI-generated data to provide a more intuitive and dynamic view of grid operations, while also incorporating robust data security measures.

Furthermore, the integration of AI in the real-time data transmission process introduces a new level of sophistication and adaptability, along with the need for enhanced security. AI algorithms can analyze and interpret complex data streams, generating images that highlight critical information and trends [5]. This capability is particularly valuable in dynamic and evolving grid environments where traditional methods may fall short. For instance, AI-generated data can dynamically reflect changes in grid load, generation, and distribution, providing operators with actionable insights and predictive analytics that support proactive management and optimization. Ensuring that these AI-generated data are securely transmitted and stored requires the implementation of robust cybersecurity measures to protect against data breaches and tampering [6].

With the continuous development of smart grid technology, the integration of real-time data security transmission and AIGC will play a pivotal role in shaping the future of energy management. Ensuring the resilience and security of power AIGC systems has become a central focus of current research. Therefore, schemes based on public key cryptographic primitives have been widely proposed. While these schemes offer high security, their heavy key management and computational overhead make them unsuitable for resource-constrained Internet of Things (IoT) devices, such as smart meters. In contrast, authentication and Key agreement protocols and physical layer key generation schemes based on symmetric encryption primitives are also being optimized. These schemes rely on one-time session keys, negotiated in secret, to achieve efficient data transmission. However, due to the heterogeneity of devices and the presence of channel noise in smart grids, generating stable physical layer keys remains a challenge. Therefore, to ensure the secure integration of AIGC and power data, it is crucial to design an efficient and secure lightweight identity authentication and scheme specifically tailored for power AIGC systems.

2 Related Work

Considering the security and performance requirements of smart grids, numerous schemes for real-time data collection and secure transmission have been proposed.

In 2015, Liu et al. [7] proposed a lightweight communication protocol for secure two-way communication in grids. The scheme employs bitwise Exclusive OR (XOR) for encryption and Lagrange interpolation for authentication, allowing for real time message verification. In 2017, Velusamy et al. [8] designed a probability-based trust calculation method to address security challenges in smart grid communication networks (SGCN), which are vulnerable to packet-dropping attacks. In 2018, Wu et al. [9] introduced an effective Identity-Based Encryption with Equality Test (IBEET) framework for smart grids, aiming to balance customer privacy with power system optimization. Their scheme utilizes bilinear pairing to eliminate the time-consuming HashToPoint function and restricts trapdoors to specific keywords, thereby preventing privacy leakage. In 2018, Nangrani et al. [10] designed a novel interleaved performance index for assessing the dynamic security of smart grid networks, addressing the unpredictable dynamics of power flow on transmission lines. Their approach combines the Lyapunov Exponent to quantify chaos with a conventional megawatt performance index for overload monitoring, resulting in the Interleaved Mega Watt-Lyapunov Exponent performance index. In 2019, Jolfaei et al. [11] addressed the vulnerability of phasor measurement

units (PMUs) in smart grids. They proposed a streamlined and secure integrity protection algorithm that ensures the safety of PMU data, demonstrating resilience against ciphertext-only and known or chosen plaintext attacks. Their method outperforms existing solutions in terms of speed while meeting strict timing requirements, making it suitable for power protection applications and emerging anomaly detection scenarios involving rapid message exchanges. In 2020, Wang et al. [12] introduced a robust and efficient authentication protocol that integrates blockchain technology, Elliptic Curve Cryptography (ECC), and a dynamic Join-and-Exit protocol, and batch verification to enhance security for smart meters and utility management centers. In 2021, Tur et al. [13] proposed a design that enhances the reliability of the current grid model by incorporating chaotic codes into communication instructions. Their case study, which involves transmitting and encoding instructions four times daily, demonstrates that the proposed method achieves necessary reserve capacity and robust chaotic encryption. In 2022, Sasikum et al. [14] proposed an improved Delegated Proof of Stake (DPoS) consensus mechanism that facilitates real-time data transmission by enabling nodes to efficiently reach consensus for block generation and securely store information in trading nodes. In the same year, Kebotogetse et al. [15] designed a streamlined Concealed Based Security Scheme that enhances data transmission security through authentication while minimizing computational overhead and energy consumption. Compared to the advanced metering infrastructure (AMI) data communication framework, which does not incorporate authentication.

In addition, with the gradual maturity of AI technology, AI-based intelligent monitoring and security solutions for smart grids are developing rapidly. In 2018, Medved et al. [16] designed a novel demand response scheduling method using an approximate Q-learning (AQL) algorithm for aggregators to optimize the operation schedules of flexible active resources. Their simulations conducted on a practical low-voltage grid model show that, while the economic approach yields the highest profit but results in the highest number of schedule violations, and the energy allocation strategy improves the voltage profile, however, it leads to reduced profits, the AQL approach balances economic performance and minimal schedule violations, validating their hypothesis. In 2020, Hansan et al. [17] addressed the challenges of real-time communication and precise synchronization in smart grid applications, which are essential for accurate monitoring, measurement, and control. To tackle these challenges, they proposed an AI-based synchronization scheme using a backpropagation neural network for timing estimation and error correction. In 2021, Barja-Martinez et al. [18] revealed interdependencies between these services, suggesting they can be offered as bundled solutions to stakeholders. They highlight the growing application of deep learning for time series prediction, unsupervised learning techniques for customer segmentation and non-technical loss detection, and reinforcement learning for energy management systems. In 2022, Wang et al. [19] proposed a novel approach using hyperdimensional computing (HDC) to detect anomalies in real-time directly from raw meter data, eliminating the need for extensive pre-processing. The method employs an associative memory for classifying hypervectors, which enhances robustness to data imbalance and includes a retraining mechanism to enhance accuracy further. In the same year, Khan et al. [20] reviewed the role of AI and machine learning in Demand Response (DR), highlighting their effectiveness in optimizing user engagement and managing complex tasks. They discuss various AI approaches and commercial applications for DR in different countries, along with the integration of blockchain technology. To address the real-time secure communication requirements between aggregators (AGs) and smart meters (SMs) in smart grids, in 2023, Wang et al. [21] proposed an efficient and provably secure identity authentication and key agreement scheme based on extended Chebyshev chaotic mapping. This scheme preserves the anonymity of smart meters and achieves perfect forward security, effectively resisting common threats such as replay attacks and identity forgery. In the same year, Ayub et al. [22] proposed a privacy-preserving identity authentication protocol for smart grid consumer centers that leverages blockchain authentication to enhance resistance to potential

attacks and ensure the real-time integrity of response data. Additionally, they incorporated Physically Unclonable Functions (PUFs) to guard against physical attacks. In 2024, Benrebbouh et al. [23] proposed a security-enhanced identity authentication protocol leveraging blockchain technology. This protocol builds on the existing smart grid authentication architecture, integrating blockchain's security mechanisms to ensure secure communication among various IoT devices.

3 System Model

This section defines the data transmission model and threat model for the real-time data transmission scheme of AIGC in smart grid, and elaborates on the functions of the participating entities and the capabilities of adversaries.

3.1 The Power AIGC System Model

The smart grid system model primarily includes three types of entities: data consumers, intelligent gateway nodes (GWN), and data generation devices. As shown in Fig. 1, the smart grid includes power generation, transmission, transformation, distribution, and consumption, with secure data transmission accompanying the entire power flow. In addition, AI technology has gradually become the core support for smart grid data decision-making and analysis, as exemplified by AIGC in the Fig. 1.

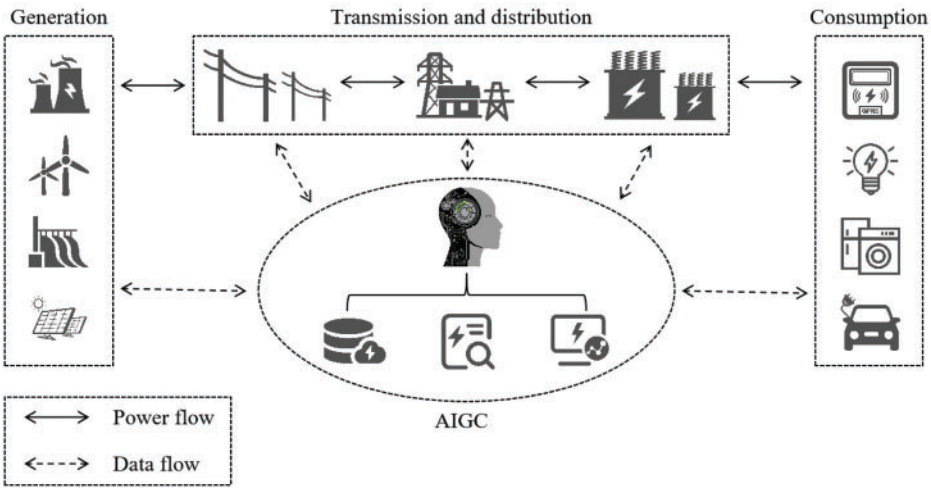

Figure 1: The architecture of power AIGC system

The data generation device is responsible for collecting and providing real-time data, including but not limited to grid data and monitoring images. The intelligent gateway functions as both an identity authentication intermediary and a data intermediary between generation devices and consumers, the data consumers can access grid data in real time through the intelligent gateway. Providing secure real-time data transmission in the power system is difficult due to the resource limitations of generation devices and the vulnerability of deployed devices [24]. Moreover, refer to the work of [25–27], the communication energy of power generation device is usually positively correlated with the communication distance between entities. Therefore, we choose the intelligent gateway to serve as the intermediary to balance the security of communication and the energy consumption.

3.2 Threat Model

This section adopts the attack capabilities defined by the Dolev-Yao (DY) model as the threat model for security analysis. Consequently, we assume that an adversary in the smart power data transmission system possesses the following basic capabilities:

- The adversary can intercept, modify, delete, and replay data transmitted through the public channel.
- An adversary may employ side-channel attacks to extract secret parameters stored within consumer devices. Similarly, grid terminals may also be compromised, allowing attackers to access and retrieve secret parameters.
- The adversary may include a legitimate user who acts maliciously. However, the adversary cannot access the AIGC model parameters or training data.

4 Our Proposed Scheme

This section proposes a secure identity authentication and key agreement scheme for power AIGC system, the specific authentication steps and update steps are shown in Fig. 2. The scheme facilitates both identity authentication and the generation of one-time symmetric keys, ensuring the integrity and efficiency of data transmission within the smart power system. Additionally, it is important to note that existing schemes typically require synchronization of the clocks of consumers, intelligent gateways, and data generation devices. To address this, we incorporate a system timestamp into the scheme to mitigate replay attacks.

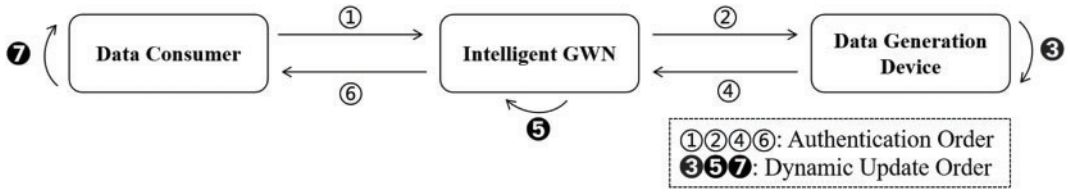

Figure 2: The steps of our proposed protocol

4.1 Initialization Phase

Before deploying, the System Administrator (SA) must initialize the data consumer, intelligent gateway, and data generation device in offline mode.

*Step*1: The SA assigns ID_j to each data generation device and stores ID_j in the non-volatile memory (NVM).

*Step*2: The SA generates random numbers $\{MK\}$ as the authentication master key.

*Step*3: The intelligent gateway stores the master key $\{MK\}$ in its database, and retains all the $\{ID_j\}$ values of the data generation devices.

4.2 Data Consumer Registration Phase

During the execution of this registration phase, the data consumer C_i can complete offline registration via the secure channel.

*Step*1: At first, C_i inputs ID_i, PW_i and biometrics BIO_i, compute $(\sigma_i, \tau_i) = Gen\,(BIO_i)$. In addition, C_i retrieves the random numbers R_i and current timestamp T_1. Upon the completion of information input, C_i computes $DR_i = R_i \oplus h\,((ID_i \oplus PW_i) \parallel \sigma_i)$ and $V_1 = h(\sigma_i \parallel ID_i \parallel PW_i)$.

*Step*2: C_i transmits $\{R_i, T_1\}$ to the intelligent gateway.

*Step*3: After receiving $\{R_i, T_1\}$, the intelligent gateway verify T_1. If T_1 is fresh, the intelligent gateway continues to compute $PR_i = R_i \oplus MK$. Finally, the intelligent gateway stores $\{PR_i\}$, and C_i stores $\{V_1, DR_i, \tau_i\}$.

4.3 Data Generation Device Registration Phase

Similarly, this phase is also conducted through a offline and secure channels. The registration phases are described below:

*Step*1: The data generation device gets identity ID_j, and retrieves a random nounce R_j, and time T_2. The data generation device transmits $\{ID_j, R_j, T_3\}$ to the intelligent gateway.

*Step*2: Upon receiving $\{ID_j, R_j, T_3\}$, it checks the freshness of message. If T_3 is fresh, the intelligent gateway computes $DIR_j = h(R_j \parallel ID_j)$ and $PTC_j = DIR_j \oplus R_j$. Then, the intelligent gateway transmits $\{PTC_j\}$ to device.

*Step*3: Finally, the gateway stores $\{ID_j, R_j\}$ in the database table, and the device stores PTC_j into NVM.

4.4 Login Phase

After the legal data consumer C_i completes the registration, it needs to log in to verify its identity. The login phase is illustrated in Fig. 3.

*Step*1: C_i inputs ID_i, PW_i and BIO_i, then, C_i computes $(\sigma_i, \tau_i) = Gen(BIO_i)$, and $V_1^* = h(\sigma_i \parallel PW_i \parallel ID_i)$.

*Step*2: C_i checks $V_1^* = V_1$? If they are equal, C_i completes the login phase. Otherwise, the C_i refuses the request.

4.5 Authentication and Key Agreement Phase

The entities in our scheme complete mutual authentication, allowing the data consumer and the device generates a session key SK for secure encrypted communication. This process is depicted in Fig. 3.

*Step*1: C_i computes $R_i = DR_i \oplus h((ID_i \oplus PW_i) \parallel \sigma_i)$. Then, SC inputs target $\{SD_j, ID_{IGWN}\}$. C_i retrieves target device ID_j, the timestamp TS_1 and generates a random number R_u. C_i computes $TC_i = h(R_i \parallel TS_1)$, $DR_u = R_u \oplus h(TC_i \parallel TS_1)$, $DID_j = ID_j \oplus h(TC_i \parallel R_u)$ and $Q_1 = h(R_u \parallel DID_j \parallel TC_i \parallel DR_u \parallel TS_1)$.

*Step*2: C_i sends $m_1 = \{Q_1, DR_u, DID_j, TS_1\}$ to the intelligent gateway.

*Step*3: Upon receiving m_1, the intelligent gateway checks TS_1. If it is freshness, it computes $R_i = PR_i \oplus MK$, $TC_i = h(R_i \parallel TS_1)$, $R_u = DR_u \oplus h(TC_i \parallel TS_1)$, $ID_j = DID_j \oplus h(TC_i \parallel R_u)$ and $Q_1^* = h(R_u \parallel DID_j \parallel TC_i \parallel DR_u \parallel TS_1)$.

*Step*4: The intelligent gateway checks $Q_1^* = Q_1$? If it is valid, it retrieves R_j and the current timestemp TS_2. Then, it computes $TC_j = h(R_j \parallel TS_2)$, $DIR_j = h(R_j \parallel ID_j)$, $DDR_u = R_u \oplus h(TC_j \parallel TS_2 \parallel ID_j)$ and $Q_2 = h(ID_j \parallel DDR_u \parallel TC_j \parallel DIR_j \parallel TS_2)$.

*Step*5: The intelligent gateway sends $m_2 = \{Q_2, DIR_j, DDR_u, TS_2\}$ to the data generation device.

*Step*6: Upon receiving m_2, the device checks TS_2. If it is freshness, the device computes $R_j = PTC_j \oplus DIR_j$, $TC_j = h(R_j \parallel TS_2)$, $R_u = DDR_u \oplus h(TC_j \parallel TS_2 \parallel ID_j)$ and $Q_2^* = h(ID_j \parallel DDR_u \parallel TC_j \parallel DIR_j \parallel TS_2)$. Then, the device checks $Q_2^* = Q_2$? If it is equal, intelligent device generates R_s and timestamp TS_3, and computes $SK = h(R_u \parallel R_s)$, $DR_s = R_s \oplus h(TC_j \parallel ID_j \parallel TS_3)$, $Q_3 = h(R_s \parallel DR_s \parallel ID_j \parallel R_u \parallel TC_j \parallel TS_3)$.

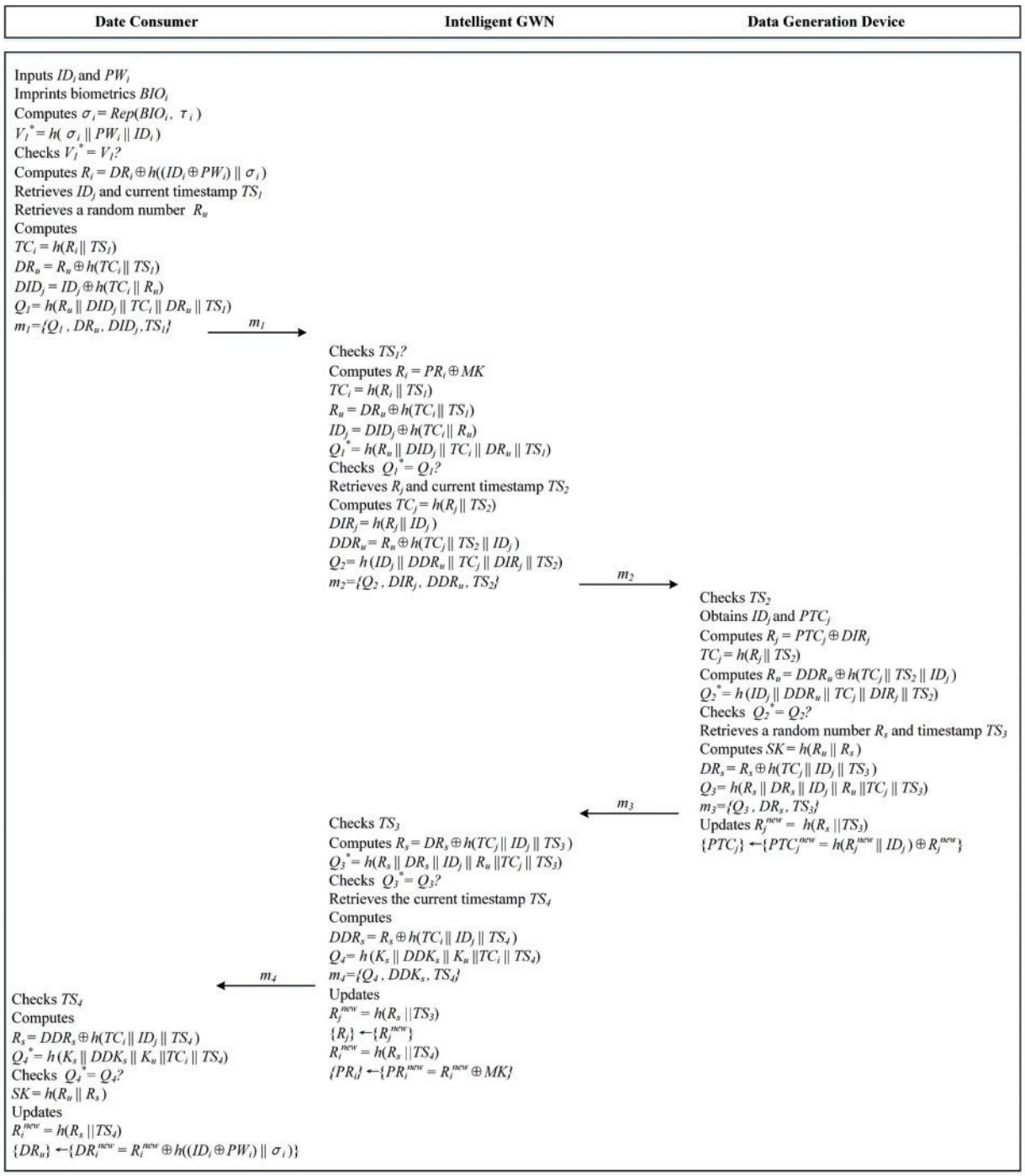

Figure 3: Login, authentication and key agreement, dynamic credential update phases

*Step*7: The device sends $m_3 = \{Q_3, DR_s, TS_3\}$ to the intelligent gateway.

*Step*8: Upon receiving m_3, the gateway checks TS_3, if it is freshness, gateway computes $R_s = DR_s \oplus h(TC_j \| ID_j \| TS_3)$, $Q_3^* = h(R_s \| DR_s \| ID_j \| R_u \| TC_j \| TS_3)$ and checks $Q_3^* = Q_3$? If it is valid, gateway computes $DDR_s = R_s \oplus h(TC_j \| ID_j \| TS_4)$ and $Q_4 = h(K_s \| DDK_s \| K_u \| TC_i \| TS_4)$.

*Step*9: The gateway sends $m_4 = \{Q_4, DDK_s, TS_4\}$ to C_i.

*Step*10: Upon receiving m_4, C_i checks TS_4. If it is freshness, C_i computes R_s and checks $Q_4^* = h(K_s \parallel DDK_s \parallel K_u \parallel TC_i \parallel TS_4)$. If it is valid, C_i computes $SK = h(R_u \parallel R_s)$.

4.6 Dynamic Credential Update Phase

After the *SK* negotiation is completed, the credentials are dynamically updated. The details of the credential update phases are shown in Fig. 3.

*Step*1: The gateway computes $R_i^{new} = h(R_s \parallel TS_4)$, $PR_i^{new} = R_i^{new} \oplus MK$, and updates PR_u with PR_u^{new}. Similarly, C_i computes R_i^{new} and DR_u^{new}.

*Step*2: The device computes $R_j^{new} = h(R_s \parallel TS_3)$, $PTC_j^{new} = h(R_j^{new} \parallel ID_j) \oplus R_j^{new}$, and updates PTC_j with PTC_j^{new}. Similarly, the gateway computes R_j^{new}, and updates R_j with R_j^{new}.

4.7 Password Update Phase

The legitimate C_i can independently update passwords.

*Step*1: C_i inputs ID_i, PW_i, BIO_i to compute V_1^* and R_i.

*Step*2: C_i checks $V_1^* = V_1$? If it is equal, C_i inputs new password PW_i^{new}. Then, C_i computes V_1^{new}, DR_i^{new}, and updates V_1 and DR_i.

5 Security Analysis

5.1 Formal Security Analysis

5.1.1 ROR Model

The security of data transmission relies on the security of encryption keys. Therefore, we use the widely accepted ROR model to illustrate the security of *SK* in this scheme and provide the following primitives related to the ROR model. We set the semantic security of our scheme as follows.

Semantic security. We define the advantages of an adversary successfully attacking the scheme to compute the session key as $Adv_{\mathscr{A}}^{P}(t) = |2\Pr[succ] - 1|$. t represents the polynomial time, and *succ* represents the event in which $\mathscr{A}$ performs a $Test\,(\Pi^t)$ query on some fresh instances and correctly guesses the value.

The proof of our scheme is as follows:

Theorem 1. Suppose the adversary $\mathscr{A}$ attempts to compromise our protocol P within polynomial time t. The following parameters are defined:

- $|\text{Hash}|$: The range of the hash function.
- q_{send}: The number of send queries.
- q_{hash}: The number of hash queries.
- $|D|$: The size of the password dictionary.
- l: The bit length of the biometric secret key.

Based on these definitions, the advantage in compromising the session key *SK* can be estimated as

$$Adv_{\mathscr{A}}^{P}(t) \le \frac{q_{hash}^2}{|Hash|} + \frac{q_{send}}{|D| \cdot 2^{l-1}} \tag{1}$$

Proof. To prove $Theorem1$, we design the following games G_i $(0 \le i \le 4)$. In addition, we denote $Succ_{G_i}$ as the probability of winning the G_i by $\mathscr{A}$ guessing the correct bit c. Meanwhile, the advantage in winning the G_i is represented as $Adv_{G_i} = Pr[Succ_{G_i}]$. The detailed analysis of every game G_i $(0 \le i \le 3)$ are analyzed as follows:

Game G_0: game G_0 is considered an actual attack performed by the adversary against our scheme. The bit c is chosen randomly by the adversary before game G_0 begins. According to the definition of semantic security provided earlier, it follows that

$$Adv^{P}_{\mathscr{A}}(t) = |2Adv_{G_0} - 1| \tag{2}$$

Game G_1: In this game G_1, the adversary can launch an eavesdropping attack by intercepting all the messages through the $Execute$ query during the authentication. The adversary can then perform the $Reveal(\Pi^t)$ and $Test(\Pi^t)$ queries to determine whether the output corresponds to SK or a random number. However, the intercepted messages m_1, m_2, m_3, m_4 do not enhance the probability of deriving the session key SK. Therefore, it follows that

$$Adv_{G_1} = Adv_{G_0} \tag{3}$$

Game G_2: In contrast to the previous game, game G_2 includes both send and hash queries. Additionally, game G_2 models an active attack where the adversary $\mathscr{A}$ attempts to convince participants to receive fabricated information. Although $\mathscr{A}$ can repeatedly initiate hash queries, the messages m_1, m_2, m_3, m_4 are associated with random numbers, current timestamps, and temporary identity credentials. As a result, when $\mathscr{A}$ makes send queries, the probability of collision is negligible. It follows that

$$|Adv_{G_2} - Adv_{G_1}| \leq \frac{q^2_{hash}}{2 \cdot |Hash|} \tag{4}$$

Game G_3: G_3 using $CorruptSmartcard(\Pi^{t_1}_U)$ query, an adversary $\mathscr{A}$ can obtain the credentials whice stored in the NVM. To guess the correct ID_i and PW_i, $\mathscr{A}$ requires both the temporary credential TC_i and biometric information. In addition, we assume that the system allows a limited number of incorrect password entries. Therefore, it also follows that

$$|Adv_{G_3} - Adv_{G_2}| \leq \frac{q_{send}}{|D| \cdot 2^l} \tag{5}$$

After $\mathscr{A}$ sends the $Test(\Pi^t)$ query, guessing bit c can win the game. Therefore, it is obvious that

$$Adv_{G_4} = \frac{1}{2} \tag{6}$$

According to (2), (3) and (6), we can obtain the following relation:

$$\frac{1}{2}Adv^{P}_{\mathscr{A}}(t) = \left|Adv_{G_0} - \frac{1}{2}\right| = |Adv_{G_1} - Adv_{G_4}| \tag{7}$$

Similarly, according to (4), (5), (7) and the triangular inequality, we can obtain the following relation:

$$\begin{aligned} \frac{1}{2}Adv^{P}_{\mathscr{A}}(t) &\leq |Adv_{G_1} - Adv_{G_2}| + |Adv_{G_2} - Adv_{G_4}| \\ &\leq \frac{q^2_{hash}}{2 \cdot |Hash|} + \frac{q_{send}}{|D| \cdot 2^l} + Adv^{CMP}_{\mathscr{A}}(t) \end{aligned} \tag{8}$$

Finally, multiply the two sides of (8) by factoring 2 and simplifying it, we can obtain the desired result

$$Adv_{\mathscr{A}}^{P}(t) \leq \frac{q_{hash}^{2}}{|Hash|} + \frac{q_{send}}{|D| \cdot 2^{l-1}} \tag{9}$$

5.1.2 AVISPA Simulation

AVISPA utilizes a formal simulation language known as HLPSL to precisely define protocol behaviors, data structures, cryptographic elements, and the abilities of attackers. It offers four verification backends, with OFMC and CL-AtSe being the most commonly applied in protocol certification research. These two models are particularly useful for verifying whether *SK* is securely negotiated and determining if the scheme can resist both passive and active attacks. The outcomes from these models are presented in Fig. 4, demonstrating that the scheme is secure and effectively defends against various common attacks.

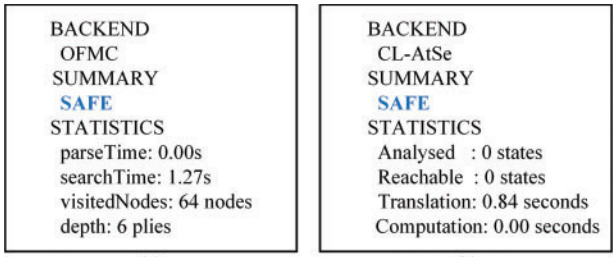

Figure 4: (a) OFMC (b) CL-AtSe

5.2 Informal Security Analysis

In this section, we examine the security of the proposed scheme and compare it with other related approaches [25–27]. The detailed analysis is presented below.

5.2.1 Replay Attack

A replay attack occurs when an adversary retransmits previously intercepted packets to the same target entity with the intention of deceiving it. Consequently, we suppose that an adversary can intercept messages and attempt to launch replay attacks against the entities. However, all entities verify Q_1, Q_2, Q_3, Q_4 and TS_1, TS_2, TS_3, TS_4. Additionally, core parameters are dynamically updated after the session key (SK) is generated. Therefore, the scheme introduced in this paper can effectively counter replay attacks.

5.2.2 Man-in-the-Middle Attack

Similarly, an adversary might intercept information m_1, m_2, m_3, m_4. However, these messages are encrypted using a hash function and are dynamically updated. If the adversary attempts to use or modify the intercepted information to launch an attack, it will result in authentication failure. Thus, the scheme introduced in this paper effectively mitigates man-in-the-middle attacks.

5.2.3 Online Guessing Attack

An online guessing attack involves an attacker attempting to crack target information by repeatedly trying different parameter combinations. An adversary might attempt to launch online guessing attacks as follows:

- The adversary can obtain DR_u and DID_j from m_1, DIR_j and DDR_u from m_2, DR_s from m_3, and DDR_s from m_4 to compute the session key.
- To obtain R_u and R_s, the adversary would need TC_i, TC_j, and ID_j. However, this information is transmitted after being encrypted by a hash function, making it impossible for the adversary to obtain two unknown parameters simultaneously through guessing attacks.

Thus, the adversary cannot successfully extract information through online guessing attacks against the proposed scheme in this paper.

5.2.4 Offline Guessing Attack

Offline guessing attacks are typically combined with device loss attacks. After gaining access to storage information, the attacker attempts to obtain core parameters by making repeated guesses. First, while the adversary can access the information stored on the device, they cannot directly obtain sensitive information such as ID_i and PW_i, as this data is encrypted using a hash function. Additionally, according to the threat model settings, we assume that an adversary might obtain DR_i and V_1. Nonetheless, the adversary is unable to access any useful information by launching an offline guessing attack. Thus, the scheme presented in this paper can effectively defends against stolen smartcard attacks and offline guessing attacks.

5.2.5 Tracking Attack

A tracking attack occurs when an adversary analyzes parameter information intercepted through a public channel and uses identity identifiers and fixed constants to track the sending entity. According to our analysis of online guessing attacks, we observe that messages are dynamic in each authentication process due to the inclusion of random values and timestamps. Because of these dynamic parameters, the adversary cannot reliably track entities in the network. Therefore, the scheme presented in this paper is resistant to tracking attacks.

5.2.6 D-DOS Attack

A Distributed Denial of Service attack takes place when an attacker exploits a network of compromised computers transmit a substantial quantity of requests to a target in a short time frame. This overwhelming traffic drains the target's computational resources or network capacity, preventing it from delivering normal services. In extreme scenarios, the target system may crash or stop functioning altogether. We assume that the adversary has the ability to intercept messages and initiate DDoS attacks against the device. Upon receiving a simulation request, the device first confirms the validity of the timestamp's freshness. If the timestamp fails to meet the synchronized clock's threshold, the request is automatically rejected. As a result, the presented scheme is capable of mitigating such attacks effectively.

5.2.7 Forward Security

Each communicating entity retrieves a random number during every authentication, and these random numbers are used to compute the session key (SK). Consequently, the SK changes dynamically and randomly throughout the mutual authentication process. Additionally, when the device joins or leaves the smart grid system, no entity can access the previous or subsequent SK. Therefore, the scheme proposed in this paper effectively meets the forward security requirements.

5.2.8 Security Comparison

This section provides a comparison between the security and functionality of the presented scheme and related works [25–27]. A detailed comparison is outlined in Table 1.

Table 1: Security and functionality comparison

Attack method	[25]	[26]	[27]	Ours
Dynamic credential update	N	N	N	Y
Mutual authentication	Y	Y	Y	Y
Replay attack	N	Y	Y	Y
Man-in-the-middle attack	N	N	Y	Y
Online guessing attack	N	Y	Y	Y
Offline guessing attack	Y	N	Y	Y
Tracking attack	Y	N	N	Y
D-DOS attack	N	N	Y	Y
Forward security	Y	Y	Y	Y

6 Performance Analysis

This section assesses the computation, communication, and storage overheads associated with the proposed framework for intelligent endpoints. Additionally, we compare these aspects with those of advanced, relevant schemes [25–27] in the same field. The details of the comparison are described below.

6.1 Analysis Basis

This section assumes that the running time of our scheme is equal to that of an Intel Xeon CPU (2.60 GHz, 8 GB RAM) [27]. Additionally, the following parameters are assumed: a 32-bit timestamp; identity, secret number, and random number each of 160 bits; a hash function output of 160 bits; and an ECC point multiplication output of 320 bits. Furthermore, the ciphertext length following symmetric encryption is assumed to match the total size of the plaintext. The execution times for these computations are summarized in Table 2.

Table 2: The running time of several computation

Notation	Definition	Time
T_H	The Hash function	0.0004 ms
T_P	Elliptic curve point multiplication	7.3529 ms
T_R	The operation of Rep	0.4420 ms
T_S	Symmetric encryption/decryption	0.1303 ms

6.2 Computation Overheads

This section compares the computation overheads of [25–27]. Table 3 shows the computation overheads of our scheme and [25–27]. It is not difficult to find that our computational cost is better than [25,27].

Table 3: Computation overheads (ms)

Scheme	C_i	*Gateway*	*Device*	Time
[25]	$8T_H + T_R + T_S$	$12T_H + T_S$	$5T_H$	0.7126
[26]	$10T_H + T_R$	$7T_H$	$7T_H + 2T_S$	0.4516
[27]	$13T_H + T_R$	$14T_H$	$12T_H$	0.4576
Ours	$11T_H + T_R$	$14T_H$	$8T_H$	0.4544

6.3 Communication Overheads

This section compares the communication overheads of our scheme with those reported in [25–27]. As illustrated in Table 4, our scheme exhibits lower communication overhead compared to the other schemes.

Table 4: Communication overheads (bits)

	C_i		*Gateway*		*Device*		Total bits
	Trans	Receive	Trans	Receive	Trans	Receive	
[25]	832	320	992	1184	352	672	2176
[26]	672	672	1824	1472	800	1152	3296
[27]	672	544	1568	1184	512	1024	2752
Ours	512	352	832	832	352	512	1696

6.4 Storage Overhead

Referencing the analysis above, this section compares the storage overheads of our scheme with those in [25–27]. Table 5 demonstrates that our scheme requires less storage overhead than the other schemes. Furthermore, it offers superior security and additional functional features, as outlined in Table 3.

Table 5: Storage overheads (bits)

Scheme	C_i	*Gateway*	*Device*	Total
[25]	1120	800	480	2400
[26]	640	480	320	1440
[27]	800	480	480	1760
Ours	480	640	320	1440

6.5 NS3 Simulation

In this section, we use the NS3 simulation tool [28] to simulate our scheme alongside [25–27]. We analyze the impact of end-to-end delay and network throughput, two critical network performance parameters. The simulation experiments are conducted on the Ubuntu 16.04.7. In the simulation setup, users are distributed within a square area centered around an gateway, allowing for free movement. The devices are distributed along a circular radial. Additionally, the simulation time is 1600 s and all entities communicate using the 2.4 GHz IEEE 802.11a Wi-Fi standard. The simulation details are provided in Table 6.

Table 6: NS3 parameters

Parameters	Description	
Scenarios	**No. of C_i**	**No. of *Device***
1	5	10
2	5	20
3	5	30
4	5	40
5	5	50
Mobility	Random (0–3 m/s)	

6.5.1 End-to-End Delay Analysis

End-to-end delay is a critical metric for assessing network real-time performance. It is calculated as the average time required for a message to travel from the sender to the receiver. The simulation results for end-to-end delay are shown in Fig. 5. It is evident that the end-to-end delay of our proposed scheme is lower compared to the schemes in [25–27], primarily due to our design, which incorporates smaller message sizes during the authentication phase.

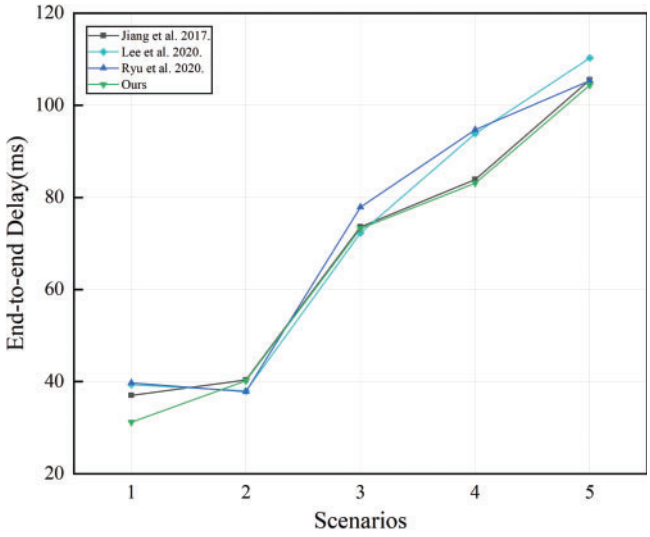

Figure 5: Comparison of end-to-end delay with related works [25–27]

6.5.2 Network Throughput

Network throughput refers to the number of bits transmitted per unit of time. Fig. 6 shows that the throughput of the proposed scheme is lower than that of the schemes presented in [25–27]. This lower throughput is attributed to our scheme's use of smaller messages during the authentication process. Moreover, it is important to note that our scheme offers additional functionality features and improved security compared to the related schemes.

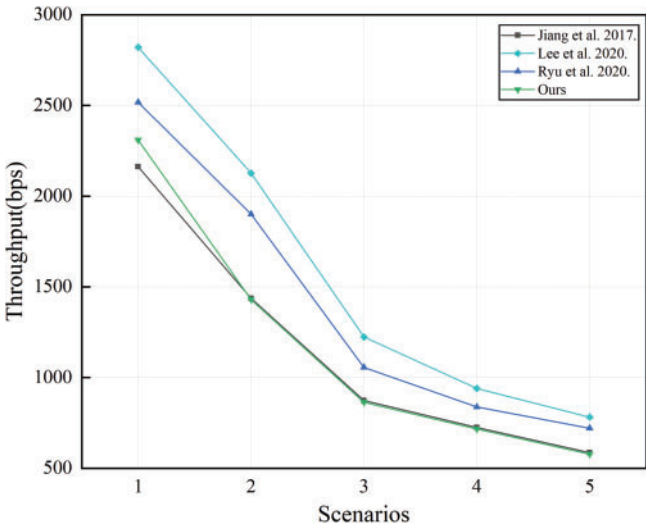

Figure 6: Comparison of network throughput with related works [25–27]

7 Conclusion

In this paper, we proposed a real-time identity authentication scheme based on dynamic credentials for power AIGC systems. The scheme includes a dynamic credential update phase that facilitates the continuous change of session keys, thereby enhancing the availability and security of the power AIGC system. We compare the security and performance of our scheme with several related authentication schemes, with the results indicating that our scheme offers superior security with minimal performance overhead. Finally, we employ the NS3 simulator to assess the network performance of our proposed scheme in comparison to other existing schemes. The simulation results indicate that our scheme is particularly well-suited for integration within power AIGC system.

Acknowledgement: The authors are very grateful to the anonymous reviewers for their detailed comments and suggestions.

Funding Statement: Not applicable.

Author Contributions: The authors confirm contribution to the paper as follows: study conception and design: Feng Wei, Zhao Chen; data collection: Yin Wang; analysis and interpretation of results: Dongqing Liu, Xun Zhang; draft manuscript preparation: Feng Wei, Zhao Chen, Zhao Zhou. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: The datasets generated and/or analyzed during the current study are not publicly available due to personal privacy reasons but are available from the corresponding author on reasonable request.

Ethics Approval: Not applicable.

Conflicts of Interest: The authors declare no conflicts of interest to report regarding the present study.

References

1. Chong ATY, Mahmoud MA, Lim F-C, Kasim H. A review of smart grid technology, components, and implementation. In: 2020 8th International Conference on Information Technology and Multimedia (ICIMU); 2020; IEEE. p. 166–9.

2. Moreno Escobar JJ, Morales Matamoros O, Tejeida Padilla R, Lina Reyes I, Quintana Espinosa H. A comprehensive review on smart grids: challenges and opportunities. Sensors. 2021;21(21):6978. doi:10.3390/s21216978.
3. Alsafran AS, Hassan A, Abusada F, Alaraj MM. Challenges and solutions for AI explainability in smart grid literature review. SSRN Electron J. 2024. doi:10.2139/ssrn.4807531.
4. Ayesha MNuman, Alhussein M, Baig MF, Aurangzeb K. Enhancing grid flexibility with coordinated battery storage and smart transmission technologies. J Energy Storage. 2024;100:113607. doi:10.1016/j.est.2024.113607.
5. Yan Y, Hu RQ, Das SK, Sharif H, Qian Y. An efficient security protocol for advanced metering infrastructure in smart grid. IEEE Netw. 2013;27(4):64–71. doi:10.1109/MNET.2013.6574667.
6. Shi Z, Yao W, Li Z, Zeng L, Zhao Y, Zhang R, et al. Artificial intelligence techniques for stability analysis and control in smart grids: method- ologies, applications, challenges and future directions. Appl Energy. 2020;278:115733. doi:10.1016/j.apenergy.2020.115733.
7. Liu Y, Cheng C, Gu T, Jiang T, Li X. A lightweight authenticated communication scheme for smart grid. IEEE Sens J. 2015;16(3):836–42. doi:10.1109/JSEN.2015.2489258.
8. Velusamy D, Pugalendhi G. An effective trust based defense mechanism to thwart malicious attack in smart grid communication network. In: 2017 IEEE International Conference on Intelligent Techniques in Control, Optimization and Signal Processing (INCOS); 2017; IEEE. p. 1–9.
9. Wu L, Zhang Y, Choo K-KR, He D. Efficient identity-based encryption scheme with equality test in smart city. IEEE Trans Sustain Comput. 2017;3(1):44–55. doi:10.1109/TSUSC.2017.2734110.
10. Nangrani S, Bhat S. Smart grid security assessment using intelligent technique based on novel chaotic performance index. J Intell Fuzzy Syst. 2018;34(3):1301–10. doi:10.3233/JIFS-169426.
11. Jolfaei A, Kant K. A lightweight integrity protection scheme for low latency smart grid applications. Comput Secur. 2019;86(1):471–83. doi:10.1016/j.cose.2018.09.014.
12. Wang W, Huang H, Zhang L, Su C. Secure and efficient mutual authentication protocol for smart grid under blockchain. Peer-to-Peer Netw Appl. 2021;14(5):2681–93. doi:10.1007/s12083-020-01020-2.
13. Tur MR, Ogras H. Transmission of frequency balance instructions and secure data sharing based on chaos encryption in smart grid-based energy systems applications. IEEE Access. 2021;9:27323–32. doi:10.1109/ACCESS.2021.3058106.
14. Sasikumar A, Ravi L, Kotecha K, Saini JR, Varadarajan V, Subramaniyaswamy V. Sustainable smart industry: a secure and energy efficient consensus mechanism for artificial intelligence enabled industrial internet of things. Comput Intell Neurosci. 2022;2022(1):1–12. doi:10.1155/2022/1419360.
15. Kebotogetse O, Samikannu R, Yahya A. A concealed based approach for secure transmission in advanced metering infrastructure. IEEE Access. 2022;10(4):84809–17. doi:10.1109/ACCESS.2022.3195240.
16. Medved T, Artač G, Gubina AF. The use of intelligent aggregator agents for advanced control of demand response. WIREs Energ Environ. 2018;7(3):e287. doi:10.1002/wene.287.
17. Hasan MK, Ahmed MM, Hashim AHA, Razzaque A, Islam S, Pandey B. A novel artificial intelligence based timing synchronization scheme for smart grid applications. Wirel Pers Commun. 2020;114(2):1067–84. doi:10.1007/s11277-020-07408-w.
18. Barja-Martinez S, Aragüés-Peñalba M, Munné-Collado Í, Lloret-Gallego P, Bullich-Massagué E, Villafafila-Robles R. Artificial intelligence techniques for enabling big data services in distribution networks: a review. Renew Sustain Energ Rev. 2021;150:111459. doi:10.1016/j.rser.2021.111459.
19. Wang X, Flores R, Brouwer J, Papaefthymiou M. Real-time detection of electrical load anomalies through hyperdimensional computing. Energy. 2022;261:125042. doi:10.1016/j.energy.2022.125042.
20. Khan MA, Saleh AM, Waseem M, Sajjad IA. Artificial intelligence enabled demand response: prospects and challenges in smart grid environment. IEEE Access. 2022;11(1):1477–505. doi:10.1109/ACCESS.2022.3231444.
21. Wang C, Li X, Ma M, Zhou T, Xu G, Xiong N, et al. PSAK: a provably secure authenticated key agreement scheme based on extended chebyshev chaotic maps for smart grid environments. Trans Emerg Telecomm Technol. 2023;34(5):1900. doi:10.1002/ett.4752.

22. Ayub MF, Li X, Mahmood K, Shamshad S, Saleem MA, Omar M. Secure consumer- centric demand response management in resilient smart grid as Industry 5.0 application with blockchain-based authentication. IEEE Trans Consum Electron. 2024;70(1):1370–9. doi:10.1109/TCE.2023.3320974.
23. Benrebbouh C, Mansouri H, Cherbal S, Pathan A-SK. Enhanced secure and efficient mutual authentication protocol in iot-based energy internet using blockchain. Peer-to-Peer Netw Appl. 2024;17(1):68–88. doi:10.1007/s12083-023-01580-z.
24. Guo F, Herrera L, Murawski R, Inoa E, Wang C-L, Beauchamp P, et al. Comprehensive real-time simulation of the smart grid. IEEE Trans Ind Appl. 2013;49(2):899–908. doi:10.1109/TIA.2013.2240642.
25. Jiang Q, Zeadally S, Ma J, He D. Lightweight three-factor authentication and key agreement protocol for internet-integrated wireless sensor networks. IEEE Access. 2017;5:3376–92. doi:10.1109/ACCESS.2017.2673239.
26. Lee H, Kang D, Ryu J, Won D, Kim H, Lee Y. A three-factor anonymous user authentication scheme for internet of things environments. J Inf Secur Appl. 2020;52:102494. doi:10.1016/j.jisa.2020.102494.
27. Ryu J, Kang D, Lee H, Kim H, Won D. A secure and lightweight three-factor-based authentication scheme for smart healthcare systems. Sensors. 2020;20(24):7136. doi:10.3390/s20247136.
28. Amare T, Adrah CM, Helvik BE. A method for performability study on wide area communication architectures for smart grid. In: 2019 7th International Conference on Smart Grid (icSmartGrid); 2019; IEEE. p. 64–73.