

A Two-way Interactive Secure Communication Model for Electric Energy Metering Data

Xu Chen^{1,*}, Chao Zhang¹, Fei Liang¹, Yu Yan¹, Baofeng Li², Xiaomeng Duan² and Yingjie Zhao²

¹State Grid Ningxia Marketing Service Center (State Grid Ningxia Metrology Center), Ningxia Yinchuan, 750000

²China Electric Power Research Institute, Beijing, 100192

Abstract

INTRODUCTION: As power market reforms deepen, traditional unidirectional protocols (e.g., IEC 102) fail to meet the secure, real-time, and bidirectional data exchange requirements of modern power grids, leaving systems vulnerable to eavesdropping and tampering.

OBJECTIVES: To ensure the confidentiality, integrity, and reliability of power data transmission by overcoming the pattern leakage vulnerabilities of traditional encryption, while satisfying the strict real-time and high-frequency demands of large-scale power systems.

METHODS: Two schemes are designed: a pure SM4 symmetric encryption scheme for high-frequency data, and an SM2-SM4 hybrid scheme for advanced authentication. To enhance security, a novel ECB-CBC hybrid encryption mode is introduced for SM4.

RESULTS: The proposed ECB-CBC hybrid mode effectively eliminates plaintext redundancy. Its Shannon entropy stabilizes at ~7.99 bits/byte (nearly touching the 8.0 theoretical ideal, vastly improving upon standard ECB's ~3.5 bits/byte). It also achieves an optimal inter-block avalanche effect of ~64 bits per block. The SM2-SM4 hybrid scheme's encryption time is only 15%-20% higher than that of pure SM4. Across 1-16 thread tests, the throughput of both SM4-based schemes grows linearly, outperforming RSA and fully homomorphic encryption (FHE) by several orders of magnitude.

CONCLUSION: The proposed ECB-CBC hybrid architecture overcomes standard mode vulnerabilities and achieves the macro-level Strict Avalanche Criterion (SAC), significantly enhancing resistance to network attacks. Compared to traditional asymmetric and homomorphic encryption, the SM4 and SM2-SM4 schemes strike an optimal balance between robust security and computational efficiency for high-concurrency power system applications.

Keywords: two-way interactive communication, identity authentication, access control

Received on 15 February 2026, accepted on 19 May 2026, published on 12 October 2026

Copyright © 2026 Xu Chen *et al.*, licensed to EAI. This is an open access article distributed under the terms of the [CC BY-NC-SA 4.0](https://creativecommons.org/licenses/by-nc-sa/4.0/), which permits copying, redistributing, remixing, transformation, and building upon the material in any medium so long as the original work is properly cited.

doi: 10.4108/ew.14632

*Corresponding author. Email: chenxu3809@163.com

1. Introduction

With the continuous deepening of the power marketization reform, especially the rapid development of emerging business models such as power spot trading [1], the power system has put forward unprecedentedly high requirements for the real-time, bidirectional, and security of data interaction. The electricity consumption information collection system [2] (hereinafter referred to as the

"consumption and collection system") serves as the core data infrastructure of the power system. The efficient, reliable, and secure communication between its master station (consumption and collection master station), dispatching master station, and other plant and station end equipment has become the key to supporting advanced applications of the smart grid and the stable operation of the power market.

However, the communication protocols [3] widely used in China's power system at present (such as those based on

the IEC 60870-5-102 standard) are mainly designed for one-way data collection (such as remote automatic meter reading), and they have inherent limitations in transmission format, interaction capability, and security mechanism. This one-way communication mode cannot meet the demand in the power market environment where the master station needs to issue control instructions, rate parameters, or real-time transaction signals to the terminal devices widely distributed on the user side through two-way interaction. This contradiction has led to significant deficiencies in the system's flexibility, real-time control, and business scalability. More importantly, traditional protocols lack built-in and powerful security mechanisms, which makes the key national infrastructure information of electrical energy data face serious security risks of being eavesdropped on, tampered with, and forged during transmission, and it is difficult to meet the mandatory requirements of national cybersecurity level protection and power security zoning.

At the level of security technology, although there have been in-depth studies on encryption algorithms (such as AES, ECC) and communication protocols [4] (such as IEC 61850, TLS), both at home and abroad, there are potential risks in the application of algorithms based on international standards in the field of critical information infrastructure in China. Although China's independently developed national cryptographic algorithms (SM2, SM3, SM4) have formed a standard system and been successfully applied in fields such as finance [5], their deep integration and efficient application in the complex heterogeneous environment of power consumption information collection systems, especially in achieving low-latency two-way secure communication on high-concurrency and resource-constrained factory and station terminal equipment, are still crucial. It still faces key technical challenges. Existing studies often have problems such as high computational overhead, high hardware requirements, or failure to systematically construct an end-to-end secure communication model from the station control layer to the master station layer.

To address the above issues, this paper proposes two bidirectional secure interactive encryption communication schemes suitable for electricity metering data. The main contributions of this paper are as follows:

- This paper presents an improved version of the SM4 algorithm, which enhances the reliability of the encryption results.
- An in-depth study was conducted on the application of national cryptographic algorithms (SM2, SM4) in communication protocols, and two application layer data encryption schemes suitable for different security levels and performance requirements were proposed.
- We conduct a comprehensive analysis and extensive experiments on the proposed solution. The analysis indicates strong scalability and security, while experimental data demonstrate favorable performance.

2. Related Works

In terms of encryption technology, in the secure communication protocol for electrical energy data, encryption technology is the core for ensuring the confidentiality, integrity, and authenticity of data. With the large-scale deployment of smart grids and Internet of Things (IoT) devices, for high-frequency, real-time, and distributed transmission of electrical energy data, encryption solutions need to take into account efficiency, lightness, and security. At PRESENT, the mainstream technologies include: symmetric encryption (such as AES [6] and lightweight PRESENT, SPECK) for efficient data encryption; Asymmetric encryption [7] (such as ECC) and identity-based encryption (IBE) are used for key management and identity authentication. In addition, homomorphic encryption supports ciphertext computation [8], providing a new approach for privacy protection in data aggregation and analysis. However, its computational cost remains a key challenge for practical application.

In the field of domestic electrical energy data security, national cryptographic algorithms [9] (SM series) have become the core of the technical system. SM2 (Asymmetric Encryption), SM3 (Hash Algorithm), and SM4 [10] (Symmetric Encryption) jointly form an independent cryptographic framework that conforms to national standards, gradually replacing internationally recognized algorithms in areas such as digital signatures, key exchange [11], and data encryption. In terms of power information security protection, the industry has successively proposed new ideas with network services as the objects of protection and carried out authentication and encryption practices based on technologies such as digital certificates and dynamic keys [12]. However, the existing methods generally have problems such as high computational overhead and reliance on dedicated hardware encryption devices. How to achieve a balance between security and efficiency remains a key challenge in current research.

In terms of network communication protocols, the CIGRE Joint Working Group (referred to as JWG) of the International Conference on Large Power Grids has carried out information system design, network security design, and other work in accordance with the technical specifications related to power information security [13]. WG D2.22 formed the technical manual "Handling of Information Security in Electric Power Enterprises" between 2006 and 2009 [14]. In addition, NIST has developed a "Smart Grid Cybersecurity" guidance manual, which describes the information security requirements of smart grids, information security protection strategies for smart grids, and the information security protection architecture for smart grids, among other contents [15].

In the secure communication of electrical energy data, the design of network protocols focuses on embedding multi-level security mechanisms while ensuring real-time performance and reliability. At the basic standard level, IEC 61850 enhances the tamper-proof and interoperability of communication in substations and monitoring systems

by introducing security layers such as TLS. At the network layer, IPsec, after being lightweight improved, is used to protect the communication of control systems such as SCADA, and is adapted to high real-time scenarios such as multicast. At the application layer, the lightweight protocols MQTT and CoAP are respectively combined with TLS/DTLS encryption to meet the dual requirements of resource constraints and data transmission security of IoT terminals, forming a systematic secure communication framework covering from the terminal to the master station.

In the power system, the 102 protocol standard for the transmission of electrical energy data between the plant station and the master station was formed by referring to the IEC 60870 5-102 protocol [16], and this protocol can already support the transmission of electric energy metering data. However, in the context of China's electricity market transactions, the 102 protocol only operates one-way data transmission and has limited transmission formats, which cannot meet the requirements issued by the electricity trading rules. Therefore, previously, in response to the special requirements of the power system, domestic research institutions first focused on data security [17], mainly considering encryption technology, data verification methods, etc.; Second, by studying the real-time performance and flexibility of communication protocols, mainly by integrating data compression algorithms, data caching and other technologies into the communication process, the transmission efficiency of data has been improved [18]; Thirdly, in terms of real-time performance, large-scale transmission and processing of time series data may have an impact on real-time performance. Although the existing communication models have taken real-time requirements into account, there may still be delay problems when dealing with large-scale time series data.

3. Preliminaries

3.1. SM2 Key Exchange Protocol

The SM2 key exchange protocol is founded on the Chinese national standard SM2 elliptic curve cryptographic algorithm. Its primary objective is to enable communicating entities over an insecure public channel to collaboratively establish a shared session key exclusively known to them, without the prerequisite of any pre-shared secrets. This procedure leverages the principles of asymmetric cryptography: by respectively utilizing their own private keys and their peer's public keys, both parties execute a series of specified elliptic curve point operations to independently derive the identical keying result. This negotiation mechanism guarantees that even if all exchanged messages during the process are intercepted, it remains computationally infeasible for an adversary to calculate the shared key. Typically, the derived key serves as a session key for symmetric encryption algorithms (such

as SM4) to facilitate efficient cryptographic protection for subsequent communications. Furthermore, since each negotiation execution yields a distinct key, the protocol inherently provides forward secrecy.

Taking an initiator A (e.g., a dispatching master station) and a responder B (e.g., an acquisition terminal) as an example, assuming both parties share global domain parameters and possess their own long-term public-private key pairs, the interaction workflow is as follows:

(1) Ephemeral Key Exchange: A and B independently generate ephemeral key pairs and mutually exchange their ephemeral public keys after validation.

(2) Shared Secret Computation: By mathematically combining their own long-term and ephemeral private keys with the counterpart's corresponding public keys, both parties leverage the algebraic properties of elliptic curves to independently calculate an identical shared secret point.

(3) Session Key Derivation: A and B input this shared point along with their identity information (ID) into a Key Derivation Function (KDF) to deduce the final symmetric session key. Consequently, both parties successfully conclude the key agreement without transmitting any plaintext key material.

3.2. SM4 Algorithm

The SM4 algorithm is a proprietary block cipher standard with independent intellectual property rights. It was promulgated by the National Cryptography Administration (GB/T 32907-2016) and has been incorporated into the international standard system (ISO/IEC 18033-3). As an efficient symmetric cryptographic scheme, SM4 not only ensures data confidentiality but also has significant advantages such as fast computation speed, high efficiency in software and hardware implementation, and low resource consumption. Its encryption process mainly consists of two modules: the key expansion algorithm and the 32-round iterative encryption algorithm. The decryption process is exactly the same as the encryption process, except that the order of the round keys is reversed (i.e., the round keys are used in reverse order). This symmetric structure design significantly facilitates the unified implementation of the algorithm in engineering software and hardware. The detailed working process is as follows:

(1) Key Expansion (Round Key Generation)

Let the input 128-bit initial encryption key be $MK = (MK_0, MK_1, MK_2, MK_3)$, where each MK_i is a 32-bit word. Introduce four 32-bit system parameters FK_i and 32 predefined constants CK_i . Initially, a concealment transformation is performed to generate intermediate keys K_i : $K_i = MK_i \oplus FK_i (i = 0, 1, 2, 3)$. Subsequently, a 32-round iterative expansion is executed to generate 32 round keys rk_i . For $i = 0, 1, \dots, 31$:

$$rk_i = K_{i+4} = K_i \oplus T'(K_{i+1} \oplus K_{i+2} \oplus K_{i+3} \oplus CK_i) \quad (1)$$

(2) 32-Round Encryption Iteration

Let the input 128-bit plaintext block be $X = (X_0, X_1, X_2, X_3)$, where each X_i is a 32-bit word. Utilizing the 32 generated round keys rk_i , 32 rounds of non-linear iterations are sequentially applied to the plaintext. For $i = 0, 1, \dots, 31$:

$$X_{i+4} = X_i \oplus T(X_{i+1} \oplus X_{i+2} \oplus X_{i+3} \oplus rk_i) \quad (2)$$

In each round, the first three words are XOR-ed with the current round key, input into the core function T for confusion and diffusion, and then XOR-ed with the fourth word to generate a new word.

(3) Reverse Transformation and Ciphertext Output

Following the 32-round iteration, an output data sequence $(X_{32}, X_{33}, X_{34}, X_{35})$ is obtained. To maintain complete structural consistency between encryption and decryption, the algorithm finally executes a reverse transformation to invert the word order.

The final output 128-bit ciphertext block Y is:

$$Y = (X_{35}, X_{34}, X_{33}, X_{32}) \quad (3)$$

3.3. Electronic Codebook

The Electronic Codebook (ECB) mode is the most basic and simplest operation mode in block ciphers. As shown in Figure 1, the plaintext message is first divided into independent data blocks, and the size of each data block is equal to the block length of the encryption algorithm. If the length of the last data block is less than the required length, a padding scheme will be applied. Subsequently, each plaintext block will be independently encrypted using the same encryption key to generate the corresponding ciphertext block. The mathematical formula can be expressed as follows: the encryption process is defined as $C_i = E_K(P_i)$, and the decryption process as $P_i = D_K(C_i)$. Here, P_i and C_i denote the i -th plaintext and ciphertext blocks, respectively, and K represents the secret key.

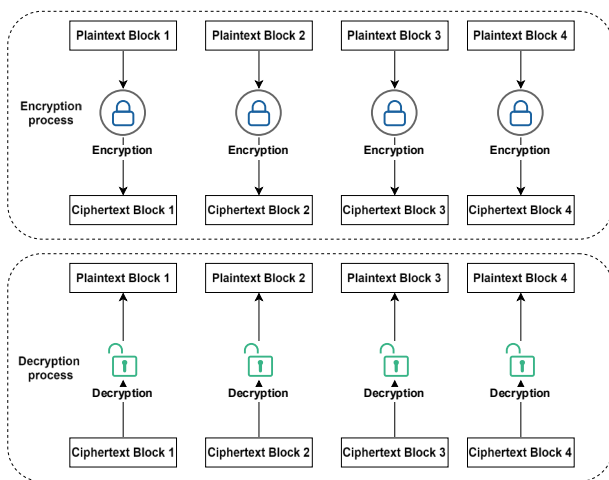


Figure 1. ECB model

The greatest advantage of the ECB mode is the independence of the grouped processing. This characteristic itself supports highly parallel computing and enhances the encryption and decryption throughput in software and hardware implementations. Moreover, this mode does not have error propagation; during transmission, bit flip errors in a single ciphertext block will only disrupt the decryption process of that specific block. However, since the same plaintext block always maps to the same ciphertext block, the ECB mode cannot conceal the statistical characteristics of the original data and its underlying pattern. Additionally, it is vulnerable to active attacks because the attacker can intercept, replay, or replace ciphertext blocks to compromise data integrity [19]. Therefore, in current practical applications, for regular data with lengths exceeding a single block or containing structured information, the ECB mode is no longer recommended for encryption purposes.

3.4. Cipher Block Chaining

As shown in Figure 2, the Cipher Block Chaining (CBC) mode is one of the most widely used and standardized working modes in modern cryptography, aiming to address the inherent security flaws of the ECB mode. Unlike the ECB mode, which processes each data block independently, the CBC mode introduces a feedback mechanism (i.e., a "chain-like" structure). Before encryption, each plaintext block is first subjected to an XOR operation with the previous ciphertext block. For the first plaintext block, since there is no preceding ciphertext, a randomly generated initialization vector (IV) is usually used for the operation. If the message length is not an integer multiple of the block length, a padding scheme is also required. The mathematical formulation can be expressed as follows: the encryption process is defined as $C_i = E_K(P_i \oplus C_{i-1})$ with $C_0 = IV$, and the decryption process as $P_i = D_K(C_i) \oplus C_{i-1}$.

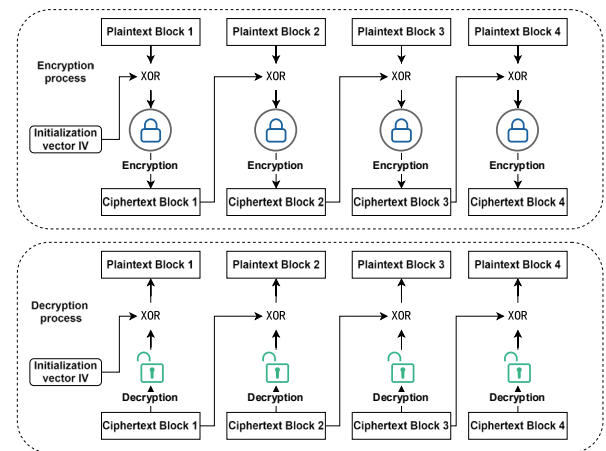


Figure 2. CBC model

The main advantage of the CBC mode lies in its chained mechanism. Each ciphertext block depends on all the preceding plaintext blocks, which enables the same plaintext block to be mapped to completely different ciphertext blocks due to the difference in their positions. This effectively conceals the statistical characteristics of the original data and provides semantic security. However, this mode also has inherent limitations: due to the sequential dependence on the order of the previous ciphertext outputs, the encryption process must be executed serially and cannot be accelerated in parallel; at the same time, this mode has a local error propagation characteristic - a bit flip error in a single ciphertext block during transmission will completely disrupt the decryption result of that block and cause bit flips in the corresponding bit positions of subsequent plaintext blocks, but the subsequent blocks are not affected [20]. Moreover, in practical applications, the CBC mode is usually combined with a message authentication code (MAC) to ensure data integrity, thereby resisting active threats such as padding oracle attacks.

4. System Design

The proposed bidirectional interactive secure communication model for electric energy metering data in this paper consists of three entities, which are elaborated as follows:

- **Power Plant:** The plant station end refers to the collective term for the physical sites located at the front end of the power network, mainly including power plants and substations.
- **Control Center:** The master station of the electricity information collection system is the "brain" and "data center" located at the back end. It centrally and remotely collects the electricity consumption data of all smart meters (on the user side) within the jurisdiction through the communication network, and conducts electricity consumption analysis, billing control, and fault monitoring.
- **Key Management Center:** This center generates, distributes, and periodically updates cryptographic keys via secure channels, thereby ensuring data confidentiality and integrity during transmission.

For different data transmission scenarios, this paper first proposes a mixed ECB-CBC mode designed to strengthen the overall security of the SM4 algorithm. Then, this paper designs two sets of data interaction schemes, namely the symmetric encryption scheme based on SM4 and the mixed encryption scheme based on SM2 and SM4.

4.1. Enhanced SM4 Algorithm

In practical applications, relying on a single encryption mode (like ECB or CBC) for SM4 frequently exposes the system to security vulnerabilities. In ECB mode,

independent block encryption means that identical plaintext invariably yields identical ciphertext blocks. This flaw exposes data structures, allowing adversaries to detect repetitive patterns via ciphertext analysis and subsequently launch replay or tampering attacks, thereby severely compromising the integrity of the system. Although CBC mode employs an initialization vector (IV) to create a chaining effect that effectively masks plaintext patterns, its security heavily depends on the randomness and secure management of this IV. If the IV lacks sufficient entropy or suffers a breach during transmission, the ciphertext may become predictable, potentially reducing CBC mode to a fragile state analogous to ECB. Consequently, both the intrinsic pattern leakage of ECB and the IV-related risks in CBC fail to meet the strict security protocols required for highly sensitive information, highlighting the need for an alternative approach.

The algorithmic workflow is illustrated in Figure 3. This paper investigates an enhanced SM4 algorithm merging ECB and CBC modes to establish a dual-layer encryption architecture. This structure optimizes computational efficiency while delivering robust security enhancements, thereby providing superior resilience against various attacks.

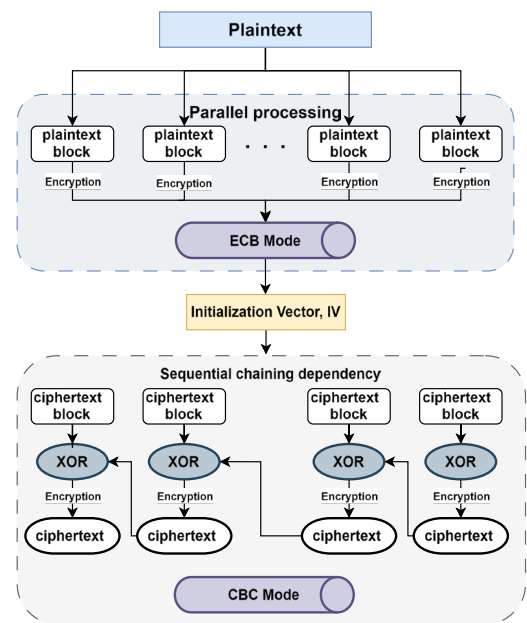


Figure 3. Enhanced SM4 algorithm process

In this design, initial encryption employs the ECB mode. Because ECB processes blocks autonomously without inter-block reliance, it supports parallel processing. This makes it highly suitable for rapidly handling massive datasets, maintaining high operational efficiency of the algorithm.

After the initial pass, CBC mode is applied to the generated ciphertext. By performing an XOR operation

with the preceding block, CBC introduces a chaining dependency across the ciphertext. This structural link elevates randomness and obscures the direct plaintext-ciphertext mapping inherent to ECB, ultimately fortifying the system's security.

This hybrid approach successfully merges the strengths of both modes while mitigating their individual weaknesses through a dual-layer structure. ECB provides rapid processing, whereas CBC contributes attack resistance via structural dependency. Furthermore, the architecture permits dynamic tuning of the ECB-to-CBC ratio based on application needs, optimizing the trade-off between performance and protection.

In addition, executing an ECB pass prior to CBC minimizes the system's reliance on the absolute randomness of the initialization vector (IV). This simplifies IV management and adds another robust layer of cryptographic strength.

The execution process of the hybrid encryption algorithm proposed in this section is as follows:

(1) Data Partitioning and ECB Pre-encryption.

Let the original plaintext message be denoted as P . It is first partitioned into n independent blocks, each with a fixed length of 128 bits, represented as $P_1, P_2, \dots, P_n$. Appropriate padding is applied to the final block if its length is insufficient. In the first encryption tier, each plaintext block P_i is independently encrypted using the SM4 algorithm under a symmetric secret key K . This generates an intermediate sequence of initial ciphertext blocks, denoted as C'_i . The mathematical formulation for this stage is:

$$C'_i = E_{SM4_K}(P_i), i = 1, 2, \dots, n \quad (4)$$

(2) CBC Chaining and Secondary Encryption.

The intermediate ciphertext sequence is subsequently fed into the CBC encryption tier. A random 128-bit Initialization Vector (IV) is generated. For the first intermediate block C'_1 , it is XORed with the IV prior to being processed by the SM4 encryption function. For all subsequent blocks, the intermediate ciphertext C'_i is XORed with the immediately preceding final ciphertext block C_{i-1} , thereby establishing the necessary cryptographic dependency. The final ciphertext blocks C_i are generated as follows:

$$C_1 = E_{SM4_K}(C'_1 \oplus IV) \quad (5)$$

$$C_i = E_{SM4_K}(C'_i \oplus C_{i-1}), i = 2, 3, \dots, n \quad (6)$$

(3) Asymmetric Key Encapsulation.

To resolve the inherent key distribution vulnerabilities of symmetric cryptography in multi-party communication, the Elgamal asymmetric cryptosystem is integrated into the final stage. The symmetric key K (utilized in Steps 1 and 2) is treated as the plaintext for the Elgamal algorithm. Using the receiver's Elgamal public key, K is encrypted to produce an encapsulated cipher-key. Finally, the

encapsulated key and the final SM4 ciphertext sequence $C = \{C_1, C_2, \dots, C_n\}$ are transmitted together over the air-ground data link, ensuring both robust data confidentiality and secure key management.

4.2. Symmetric Encryption Scheme

Application layer data encryption is achieved through the SM4 symmetric encryption algorithm and is suitable for high-frequency data transmission scenarios. The sender encrypts the data with an SM4 symmetric key before transmission, while the receiver decrypts it with the same key. The key is generated and distributed by an independent key management module, and is transmitted and updated regularly through a secure channel to ensure the confidentiality and integrity of the data during transmission. The specific technical route is shown in Figure 4.

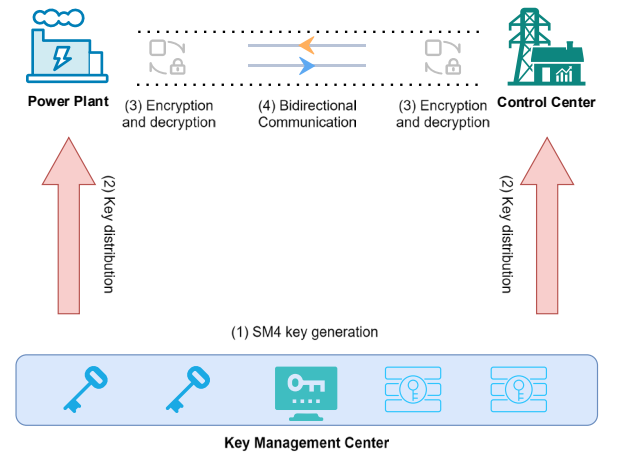


Figure 4. SM4 symmetric encryption scheme

In the algorithm flow of this scheme, the core symbols involved and their definitions are as follows: Let K be the SM4 symmetric key generated and distributed by an independent key management module, which is transmitted and updated regularly through a secure channel; M and C respectively represent the original plaintext data and the encrypted ciphertext data during the communication process. The encryption and decryption process is characterized by $E_K(\cdot)$ and $D_K(\cdot)$, that is, the SM4 encryption algorithm and decryption algorithm using the key K .

The detailed algorithm process is as follows:

- **SM4 Key Generation:** The key management module generates a secure SM4 symmetric key K .

$$K \leftarrow \text{KeyGen}() \quad (7)$$

- **Key Distribution:** The key management module securely distributes the key K to the sender and receiver through a secure channel.

$$Send K \rightarrow Sender, Send K \rightarrow Receiver$$

- **Encryption:** The sender encrypts the plaintext data M with the key K to obtain the ciphertext C .

$$C = EK(M) \quad (8)$$

- **Bidirectional Interaction:** The sender transmits the ciphertext C to the receiver through the communication network.
- **Decryption:** After receiving the ciphertext C , the receiving end decrypts it using the same key K to restore the plaintext M .

$$M = DK(C) \quad (9)$$

Based on the graphical architecture, this solution realizes the full life cycle control of symmetric keys through a centralized key management module. Combined with end-to-end identity authentication and encrypted transmission, it builds a complete and reliable data security protection system.

4.3. Symmetric Encryption Scheme

To elevate application-layer data protection, a hybrid framework integrating SM2 and SM4 is implemented. In this architecture, communicating nodes rely on the asymmetric SM2 protocol to execute digital signature verification and securely negotiate a shared symmetric key. This generated key subsequently drives the SM4 algorithm to encrypt the actual data payload. Upon receipt, the destination node retrieves the symmetric key via SM2 decryption, which then allows for the decoding of the ciphertext. By pairing the rigorous key management of public-key cryptography with the computational speed of symmetric ciphers, this approach delivers the robust safeguards required for transmitting highly sensitive information. The specific technical route is shown in Figure 5.

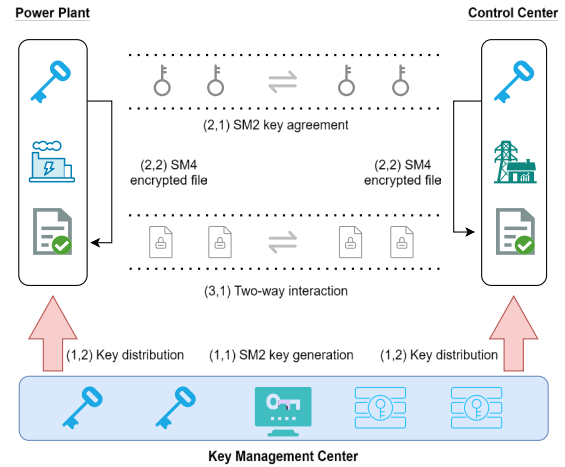


Figure 5. SM2-SM4 hybrid encryption scheme.

In the algorithm flow of Scheme Two, the symbol definitions involved are shown in Table 1.

Table 1. Symbol Definition

Symbol	Explanation
(SK_s, PK_s)	The SM2 key pair for the sender
(SK_r, PK_r)	The receiving end SM2 key pair
(sk_s, Ps)	temporary key pairs for the sender
(skr, Pr)	temporary key pairs for the receiver
K_s	The temporary SM4 symmetric session key generated by the sender.
M	Plaintext application data to be transmitted
C_{K_s}	The ciphertext obtained after encrypting K_s with the public key PK_r of the receiving end
C_M	The ciphertext obtained after encrypting M with the symmetric key K_s .
IDs, IDr	identity identifiers for both parties
SK	The shared key generated through negotiation
$KeyAgr(\cdot)$	SM2 key agreement function
$KDF(\cdot)$	key derivation function
$DSK(\cdot)$	The SM2 asymmetric decryption algorithm using the private key SK
$EncK(\cdot)/DecK(\cdot)$	SM4 encryption and decryption algorithms

The core process of this algorithm can be divided into three stages: the first stage: key exchange and identity authentication; the second stage: data encryption and transmission; the third stage: data reception and verification. Its complete interaction logic is as follows:

- **SM2 Key Generation:** Each of the communicating parties generates a temporary SM2 key pair.

$$(sks, Ps) \leftarrow TempKeyGen() \quad (10)$$

$$(skr, Pr) \leftarrow TempKeyGen() \quad (11)$$

- **Key Distribution:** Each of the communicating parties generates a temporary SM2 key pair, namely (Ps, IDs) and (Pr, IDr) . Furthermore, both parties must obtain each other's long-term public keys, PKr and PKs , in a prior or the current interaction.
- **Key Agreement:** Using their respective long-term private keys, ephemeral private keys, as well as the other party's long-term public keys, ephemeral public keys, and IDs, both parties independently compute the shared secret key SK.

The sender computes:

$$SK = KeyAgr(IDs, IDr, SKs, sks, PKr, Pr) \quad (12)$$

The receiver computes:

$$SK' = KeyAgr(IDr, IDs, SKr, skr, PKs, Ps) \quad (13)$$

- **Key Derivation:** Both parties use KDF to derive the session key for symmetric encryption from the shared key SK. L represents the key length.

$$Ks = KDF(SK, "SM4", L) \quad (14)$$

- **Two-way Interaction:** The communication between both parties is encrypted using Ks.

$$CM = EncKs(M) \quad (15)$$

$$M = DecKs(CM) \quad (16)$$

5. Theoretical Analysis

5.1. Proof of reversibility for the improved SM4 algorithm

Assume the plaintext data is padded and divided into n blocks of equal length, denoted as $P = \{P_1, P_2, \dots, P_n\}$. Let E_k and D_k represent the SM4 encryption and decryption functions using key k , respectively, and let IV be the random initialization vector.

Deduction of the Encryption Process:

- **Phase 1 (Initial ECB Encryption):** Each plaintext block is encrypted independently to generate the initial ciphertext block C'_i :

$$C'_i = E_k(P_i) (1 \leq i \leq n) \quad (17)$$

- **Phase 2 (Chained CBC Encryption):** The initial ciphertext blocks are subjected to XOR operations and secondary encryption:

For the 1st block:

$$C_1 = E_k(C'_1 \oplus IV) \quad (18)$$

For the i -th block ($i > 1$):

$$C_i = E_k(C'_i \oplus C_{i-1}) \quad (19)$$

The final output is the ciphertext sequence

$$C = \{C_1, C_2, \dots, C_n\}.$$

Deduction of the Decryption Process:

Upon receiving the ciphertext sequence C , the receiver performs the reverse operations:

- **Phase 1 (Reverse CBC):** Since SM4 is a deterministic symmetric encryption algorithm, $D_k(E_k(X)) = X$ always holds. For the 1st block:

$$C'_1 = D_k(C_1) \oplus IV \quad (20)$$

For the i -th block ($i > 1$):

$$C'_i = D_k(C_i) \oplus C_{i-1} \quad (21)$$

This step perfectly recovers all initial ciphertext blocks C'_i .

- **Phase 2 (Reverse ECB):** The recovered initial ciphertext blocks are decrypted independently:

$$P_i = D_k(C'_i) (1 \leq i \leq n) \quad (22)$$

Conclusion: Through mathematical deduction, the decryption process completely reverses and cancels out the XOR and non-linear transformation operations of the encryption process without any information loss. Therefore, the improved algorithm forms a strict logical closed loop and possesses absolute correctness.

5.2. Security analysis

The advantage of Scheme One lies in its efficient asymmetric encryption architecture. This scheme achieves the full lifecycle security management of SM4 session keys through the key management center, combined with end-to-end data encryption transmission. It provides support for high-frequency data in smart grids that balance efficiency and confidentiality, and is particularly suitable for business scenarios with high real-time requirements.

Scheme Two adopts the SM2 key agreement mechanism, which natively completes two-way identity authentication while establishing the session key. It organically integrates key distribution, identity

verification, and data encryption, and builds an end-to-end secure channel with forward security, which can effectively resist eavesdropping, tampering, replay, and man-in-the-middle attacks. It provides high-level security guarantees for sensitive data, such as control instructions and user privacy.

5.3. Correctness analysis

The correctness of Scheme One is guaranteed by a strict key management process and standard encryption and decryption algorithms. The scheme generates and securely distributes the same SM4 symmetric key to the key storage modules of the sender and receiver through an independent key management module, ensuring the consistency and synchronization of the keys for both encryption and decryption. The sender encrypts the data with this key and then transmits it, while the receiver decrypts it with the same key. This process strictly follows the SM4 algorithm specification. It can be proved that as long as the key remains consistent and the algorithm implementation is correct, the decryption result will definitely be exactly the same as the original plaintext data.

Scheme Two first uses the strictly proven SM2 key agreement protocol to enable both communicating parties to collaboratively calculate the same session key while undergoing identity authentication. The correctness of this process is guaranteed by the mathematical basis of elliptic curve cryptography. Subsequently, both parties conducted SM4-encrypted communication using the symmetric key agreed upon through negotiation. This not only inherited the efficiency of symmetric encryption but also solved the key distribution problem through asymmetric encryption. The addition of digital signatures and verification processes ensures the verifiability of data sources and the integrity of the transmission process.

6. Analysis of experimental results

We conducted simulation experiments on the proposed scheme. The experiments were run in a Windows system with an AMD Ryzen 75800H processor with Radeon Graphics, 16GB of RAM, and a 64-bit system type. We conducted ten experiments for each piece of data respectively. Finally, take the average value. The programming language used is Golang.

6.1. Diffusivity and confusability tests

To evaluate the confusion properties, we measured the Shannon entropy of ciphertexts generated from highly redundant plaintexts (e.g., files with uniform data patterns) across different sequence lengths. As illustrated in Figure 6, the conventional SM4-ECB mode completely fails to mask data redundancy; its entropy remains abnormally low (around 3.5 bits/byte), as identical plaintext blocks

deterministically yield identical ciphertext blocks, leaving it vulnerable to pattern recognition attacks.

In stark contrast, the proposed ECB-CBC hybrid mode demonstrates exceptional confusion capabilities. By introducing chaining dependencies in its secondary phase, the hybrid mode effectively disrupts any plaintext redundancy. Regardless of the number of encrypted blocks, the Shannon entropy of our proposed scheme consistently stabilizes at approximately 7.99 bits/byte, virtually touching the theoretical ideal limit of 8.0. This performance is entirely comparable to the standard SM4-CBC and SM4-GCM modes, validating that the hybrid architecture successfully overcomes the inherent pattern leakage vulnerability of standard ECB while maintaining optimal data randomness.

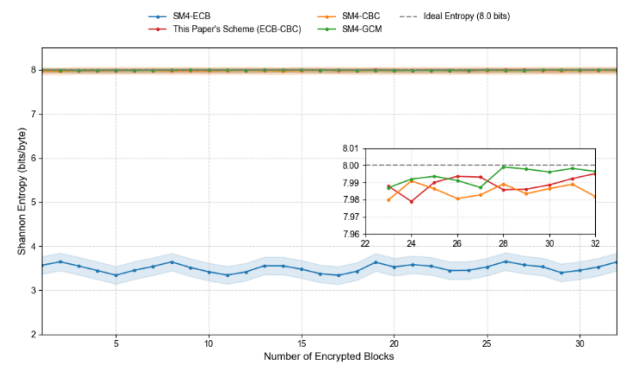


Figure 6. Confusion performance comparison based on Shannon entropy

Diffusion performance is strictly evaluated using the inter-block avalanche effect. We flipped a single bit in the first plaintext block and recorded the resulting bit changes across subsequent ciphertext blocks. For the 128-bit SM4 cipher, the theoretical ideal avalanche value per block is 64 bits.

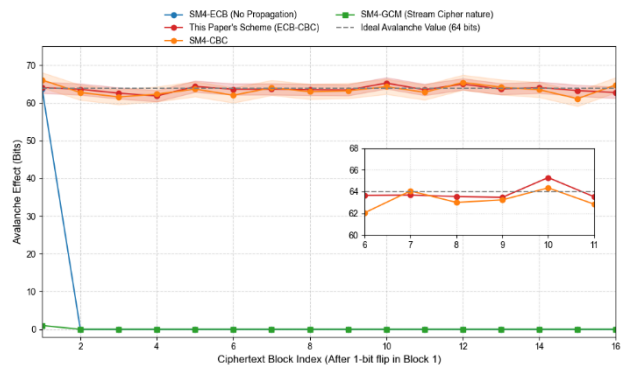


Figure 7. Diffusion performance comparison based on the inter-block avalanche effect

As shown in Figure 7, the differences among various operation modes are presented. The SM4-GCM mode is

essentially a stream cipher (based on the CTR structure), and a 1-bit change is strictly limited to the corresponding ciphertext bit position, exhibiting zero block inter-diffusion characteristics. Similarly, the SM4-ECB mode processes each data block independently - the first group achieves a 64-bit avalanche effect, but subsequent groups are completely unaffected (0-bit flipping).

Conversely, the ECB-CBC hybrid mode proposed in this paper inherits and optimizes the chained feedback mechanism. The single-bit flip of the initial group is rapidly propagated through the XOR operation in the secondary CBC stage, causing a continuous and stable approximately 64-bit avalanche effect in all subsequent ciphertext blocks. This proves that the proposed scheme achieves the optimal strict avalanche criterion (SAC) at the macro level, effectively resisting differential cryptanalysis while also taking into account the computational efficiency advantage brought by the ECB initial stage.

6.2. Encryption and decryption performance tests

This section evaluates the encryption time costs of the SM4 scheme proposed in this paper, the hybrid encryption scheme combining SM2 and SM4, and the homomorphic encryption scheme [8]. The results are shown in Figure 8.

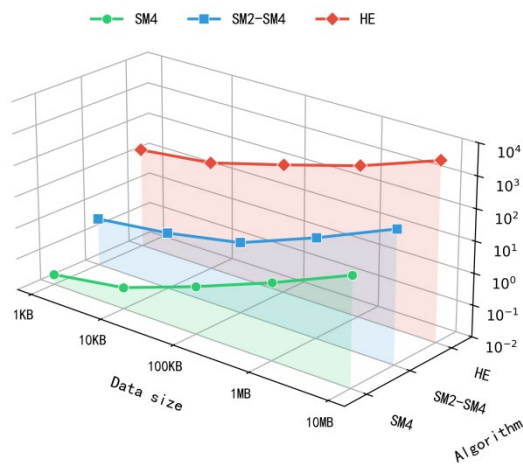


Figure 8. Comparison of encryption time cost

The experimental results reveal significant variations in processing speeds among the schemes. Because SM4 is a highly efficient symmetric cipher, its processing time scales linearly with dataset size, yielding the fastest overall performance. The SM2-SM4 hybrid approach adopts SM2 for key exchange to improve key management. While this makes it roughly 15%-20% slower than standalone SM4, it remains considerably faster than fully homomorphic encryption (FHE). Although FHE enables direct computation on ciphertexts, its massive computational overhead makes it orders of magnitude slower than the

others, even though the rate of slowdown levels off slightly with larger datasets. Ultimately, these findings dictate their use cases: SM4 is essential for tasks demanding strict real-time processing, like large-scale data transfers; the hybrid SM2-SM4 provides a practical trade-off for secure communications; and FHE trades speed for advanced functionality in privacy-preserving scenarios (e.g., secure multi-party computation), which currently limits its broader practical application.

This paper further conducts a comparative analysis of the throughput of the proposed SM4 symmetric encryption scheme, the SM2-SM4 hybrid encryption scheme, the RSA scheme [21], and the homomorphic encryption scheme [8]. The experimental results are shown in the figure. In general, under different concurrent thread scales, the throughput of each encryption scheme varies significantly.

As shown in Figure 9, for all thread scales (from 1T to 16T), the throughput of the encryption scheme shows a very significant performance difference. Overall, the SM4 symmetric encryption scheme maintains the highest throughput in all tests, and its performance shows an approximately linear growth trend as the concurrent thread scale increases. This is mainly because SM4, as a symmetric algorithm, has low computational complexity, does not require a complex key exchange process, and is easy to perform multi-thread parallel processing, thus being able to fully utilize computing resources.

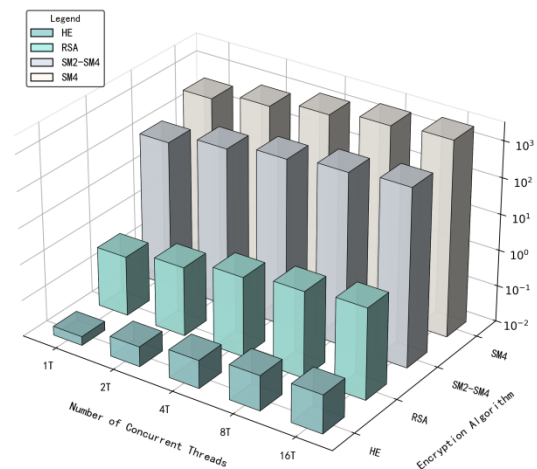


Figure 9. Throughput comparison

By comparison, while the SM2-SM4 hybrid architecture yields a slightly lower throughput than the standalone SM4 setup, it vastly outperforms both the RSA and homomorphic models. The rationale lies in its design: it delegates bulk data encryption to the low-overhead SM4 algorithm, reserving the more demanding SM2 protocol strictly for initial key negotiation. Consequently, the framework successfully optimizes both computational speed and cryptographic strength. Furthermore, although multi-threading consistently boosts throughput, the

inherent mathematical weight of SM2 dictates a gentler scaling curve relative to purely symmetric systems.

Conversely, RSA demonstrates inherently sluggish processing speeds with marginal gains from parallel threads. This bottleneck stems directly from its reliance on massive integer modular exponentiation. Such computationally dense operations resist meaningful acceleration via standard parallelization, fundamentally capping RSA's viability in high-concurrency environments.

Homomorphic encryption registers the lowest throughput among the evaluated protocols. The necessity to compute directly on ciphertexts imposes massive computational burdens, driving overall performance far below conventional benchmarks. Ultimately, while this paradigm offers unparalleled data privacy preservation, its severe latency constraints currently preclude widespread deployment in real-time, high-volume scenarios.

7. Conclusion

Driven by ongoing power market reforms, legacy communication protocols in electricity metering systems increasingly struggle with unidirectional data flow, inadequate security architectures, and high computational overhead when integrating national cryptographic standards. In response, this research introduces a bidirectional, secure communication framework tailored specifically for metering data. To overcome the deployment hurdles of national ciphers on resource-constrained and heterogeneous terminals, we formulate two distinct application-layer encryption strategies utilizing SM2 and SM4. These configurations are designed to accommodate varying security thresholds and operational constraints. Furthermore, the study engineers an optimized variant of the SM4 algorithm. This modification bolsters ciphertext robustness and processing efficiency, ultimately establishing high-intensity, end-to-end data shielding between the substation control layer and the master station. Subsequent research will focus on scaling this architecture, optimizing its deployment across broader distributed energy networks and edge computing environments.

Acknowledgements.

This work was supported by the Science and Technology Project of State Grid Ningxia Electric Power Co., Ltd. (Grant No. 5229YX24000H).

References

- [1] Lin B, Wei B. Power market reform incentivizes artificial intelligence investment: Evidence from China's electricity spot trading market pilot. *Energy Policy*. 2026;214: 115235.
- [2] Lai S, Wang J, Wang Z, Huang S, Wang H, Hu Y, et al. Key Technologies for Data Collection, Modeling, and Sharing of Carbon Emissions from Electricity Consumption Based on Blockchain. *International Conference on Smart Applications and Sustainability in the Artificial Intelligence of Things*: Springer; 2024. 453-462.
- [3] Pamulaparthi B, Macdonald D. Incorporating communication protocols for substation automation. *Switchgear Design, Operation, and Maintenance Using Industry Standards*: Elsevier; 2025. p. 135-172.
- [4] Ayello M, Lopes Y. Battery energy storage systems associated with transmission lines: implementation proposal with IEC 61850 standard and feasibility case study. *Electric Power Systems Research*. 2025;241: 111382.
- [5] Shingari N, Mago B. The importance of data encryption in ensuring the confidentiality and security of financial records of medical health. *2024 IEEE International Conference on Interdisciplinary Approaches in Technology and Management for Social Innovation (IATMSI)*: IEEE; 2024. 1-6.
- [6] Shukla D, Chakrabarti S, Sharma A. Blockchain-based cyber-security enhancement of cyber-physical power system through symmetric encryption mechanism. *International Journal of Electrical Power & Energy Systems*. 2024;155: 109631.
- [7] Zhao R, Lu J, Yu Z, Zeng K. A synchronous compression and encryption method for massive electricity consumption data privacy preserving. *Frontiers in Energy Research*. 2025;12: 1444505.
- [8] Zhang Y, Lu W, Yu Q, Zhang S, Li W, Liang K. Power Data Federated Learning Privacy Policy Based on Optimized Homomorphic Encryption. *2024 IEEE 6th International Conference on Power, Intelligent Computing and Systems (ICPICS)*: IEEE; 2024. 624-629.
- [9] Zheng Y, Wang X, Wen X, Tian M. System Using Computer Combined Data Encryption Technology in the Security Management of Electricity Bills. *International Conference on Innovative Computing*: Springer; 2024. 366-373.
- [10] Song Y, Li H, Chen Y. Hardware Implementation of SM4 Encryption Algorithm with Hybrid Stochastic Computing. *International Conference on Mobile Internet Security*; Singapore: Springer; 2023. 66-77.
- [11] Ayub MF, Li X, Mahmood K, Alenazi MJ, Das AK, Wang G. Provably secure efficient key-exchange protocol for intelligent supply line surveillance in smart grids. *IEEE Internet of Things Journal*. 2025;12(12): 1784-21792.
- [12] Hussain SS, Aftab MA, Farooq SM, Latif A, Konstantinou C, Abido MA. A public key based quantum secure digital signature scheme for securing IEC 61850 R-GOOSE and R-SV messages. *IEEE Transactions on Industry Applications*. 2025;61(3): 5135-5147.
- [13] Piètre-Cambacédès L, Bouissou M. Beyond attack trees: dynamic security modeling with Boolean logic Driven Markov Processes (BDMP). *2010 European Dependable Computing Conference*: IEEE; 2010. 199-208.
- [14] Somme stad T, Ekstedt M, Holm H. The cyber security modeling language: A tool for assessing the vulnerability of enterprise system architectures. *IEEE Systems Journal*. 2012;7(3): 363-373.
- [15] Schneier B. Attack trees. *Dr Dobbs's journal*. 1999;24(12): 21-29.
- [16] Bai Y, Hou Y, Fang D, He X, Zhu C. A remote real-time on-line monitoring and control system for large-scale wind farms. *2010 International Conference on Electrical and Control Engineering*: IEEE; 2010. 3220-3223.
- [17] Aytekin A, Coşkun A, Dursun M. Evolving Maturity Models for Electric Power System Cybersecurity: A Case-Driven Framework Gap Analysis. *Applied Sciences*. 2025;16(1): 177.

- [18] Dai H, Chen J, Ni Y, Chen H, Yu Y, Ji X, et al. Research on improving the efficiency of wireless networking in the power system. *Journal of Physics: Conference Series: IOP Publishing*; 2024. 012100.
- [19] Mahajan P. A study of encryption algorithms AES, DES and RSA for security. *Global journal of computer science and technology*. 2013;13(E15): 32-40.
- [20] Yau AK, Paterson KG, Mitchell CJ. Padding oracle attacks on CBC-mode encryption with secret and random IVs. *International Workshop on Fast Software Encryption: Springer*; 2005. 299-319.
- [21] Valsan V, Keerthan K, Devnath N, Ajithkumar A, Sasikumar A. Securing Sustainable Energy Trading: An RSA-Encrypted IoT Solution for Smart Meter Data Transmission. 2024 *International Conference on Computational Intelligence and Computing Applications (ICCICA)*: IEEE; 2024. 187-192.