SeCo2: Secure Cognitive Semantic Communication in 6G-IoT Networks Using Key-Policy Attribute-Based Encryption and Elliptic Curve Cryptography

G. SUGITHA [1], R. VASANTHI [2], A. SOLAIRAJ [3], A. V. KALPANA [4]

[1] Dept. of Computer Science and Engineering, Muthayammal Engineering College (Autonomous), Rasipuram, 637408, Namakkal City, India
[2] Dept. of Computer Science and Engineering, R P Sarathy Institute of Technology, Omalur, 636305, Salem City, India
[3] Dept. of Computer Science and Engineering, Sethu Institute of Technology, Kariyapatti, 626115, Virudhunagar City, India
[4] Dept. of School of Computing, SRM Institute of Science and Technology, Chengalpattu, 603203, Chennai City, India

sugitha.g.cse@mec.edu.in, vasanthi.r@rpsit.ac.in, solairaja@sethu.ac.in, kalpanaa2@srmist.edu.in

Submitted February 14, 2025 / Accepted May 14, 2025 / Online first May 19, 2025

Abstract. *Secure and efficient data transmission is crucial for maintaining seamless system operations and user trust in the rapidly evolving Internet of Things (IoT) environments. However, IoT networks consistently suffer from data integrity breaches, security vulnerabilities at various network layers, and a high computational cost. Bridging the gap between IoT applications and network infrastructure is essential to addressing these issues. This paper introduces SeCo2, a secure cognitive semantic communication framework for 6G-IoT networks. The framework incorporates a blockchain-based system to provide a secure and privacy-preserving data transmission mechanism. Data preprocessing is conducted using the IoT-Sense dataset, and then encryption is done through a hybrid combination of Key-Policy Attribute-Based Encryption (KP-ABE) and Elliptic Curve Cryptography (ECC). Access control and data permissions are implemented via smart contracts to ensure secure transmission. Additionally, a blockchain security layer utilizing Proof of Stake with Fixed Staking Amounts (PoS-FSA) enhances network security and energy efficiency. For further protection of data integrity, tamper-proof provenance logging prevents unauthorized tampering. Experimental results demonstrate ultra-low latency data transmission (in the microsecond range), with a transmission delay as low as 0.003001 s for data sizes ranging from 1 GB to 50 GB, and a network security rate of 98%, ensuring more reliable and privacy-preserving IoT ecosystems.*

Keywords

6G-IoT, blockchain, cognitive semantic communication, elliptic curve cryptography, key-policy attribute-based encryption

1. Introduction

The rapid advancement of 6th-Generation (6G) wireless communication technology has led to the emergence of the Internet of Things (IoT) paradigm, connecting a vast number of smart devices for various services [1]. As a key enabler of 6G networks, IoT plays a crucial role in ensuring seamless connectivity and intelligent automation. 6G-enabled IoT networks have been developed to offer high-quality connectivity to many wireless devices. This evolution of the IoT is revolutionizing the way devices communicate and interact with each other within an integrated ecosystem [2]. Cognitive Semantic Communication (CSC) emerges as a promising paradigm that extends beyond traditional communication models, enabling IoT devices to interpret and transmit both raw data and meaningful information [3]. The CSC develops communication systems that mimic human-like understanding, processing, and exchange of semantic (meaning-based) information [4]. However, data transmission must be secure in the CSC-IoT due to the large number of IoT devices and the high volume of data that need to be transmitted exponentially [5], [6]. This is where blockchain technology becomes indispensable [7]. Blockchain technology enhances data integrity and security by providing an immutable, tamper-proof ledger for transaction verification [8], [9]. Additionally, DL enhances CSC by enabling devices to learn vast amounts of data, adapt to dynamic network conditions, optimize data transmission, and predict anomalies in near real-time [10], [11]. The integration of CSC, blockchain, and DL ensures trusted communication, authenticity, and auditability across all IoT network layers.

In existing works, several research studies have been conducted to achieve better security, integrity, and data per-

DOI: 10.13164/re.2025.0366

formance using various cryptographic methods, blockchain-based approaches, and DL models in the CSC-IoT [12], [13]. However, these existing solutions often struggle with high computational costs, scalability issues in large-scale IoT networks, and insufficient adaptability to dynamic network conditions [14]. Furthermore, the fragmented security layers in current models create inconsistencies and make them vulnerable to attacks [15]. To address these challenges, this paper proposes a novel framework that addresses the complexity of data integrity breaches, security issues across network layers, and high computational costs. Hence, we propose integrating blockchain infrastructure with the DL model to ensure data security and provide efficient data transmission in large-scale IoT networks in CSC. The proposed SeCo2 demonstrates the complexity of real-time applications and enhances the performance of the 6G-IoT networks.

1.1 Research Contribution

The main contributions of this study are as follows:

- This study integrates CSC and blockchain technology to develop a framework for secrecy-preserving data transfer. Unlike conventional models that use blockchain or semantic encryption separately, our approach ensures real-time, secure, and semantic-aware communication in 6G-IoT networks.
- The proposed framework incorporates a robust, comprehensive semantic knowledge base to enhance system update efficiency. By minimizing redundant data exchanges and synchronizing semantic representations, this mechanism significantly reduces transmission overhead while maintaining high accuracy in IoT network updates.
- To address the high computational cost of IoT devices, we introduce an optimized hybrid encryption scheme that combines Key-Policy Attribute-Based Encryption (KP-ABE) with Elliptic Curve Cryptography (ECC). This approach achieves stronger security while reducing processing overhead, making it ideal for resource-constrained IoT environments. Smart contracts further enhance integrity by automating secure data transfers without compromising semantics.
- Existing blockchain-based security models often suffer from high energy consumption and scalability challenges. Our framework introduces Proof of Stake with Fixed Staking Amounts (PoS-FSA), which enhances network security while reducing computational energy costs. This mechanism strengthens multi-layered security protections against evolving cyber threats in 6G-IoT networks.
- The work proposes a solution to verify data authenticity and prevent tampering even in resource-constrained IoT ecosystems by introducing data provenance logging within the blockchain. This enhances trust and transparency by creating an immutable audit trail for all data transactions.

The paper is organized as follows: Section 2 provides an in-depth review of the existing literature. Section 3 presents the proposed framework. Section 4 presents results and a detailed discussion of the system's performance. Finally, Section 5 concludes the paper.

2. Literature Survey

This section reviews existing research and methodologies in IoT networks to identify current trends, gaps, and challenges. This provides an understanding and helps to position the proposed work within the broader context. Xu et al. [16] discussed distributed edge learning techniques and communication optimization in dual-functional networks. The authors explained the performance metrics and recent advancements in communication systems for learning, with applications in B5G networks. Still, energy and computation capacity remain an unsatisfactory challenge. To improve efficiency, Yi et al. [17] discussed a semantic communication system for text transmissions that reduces the number of symbols transmitted by using a shared knowledge base. The model improved efficiency by integrating the message using DL, but the performance improvements were limited due to the small number of commonly used semantic messages.

Chen et al. [18] suggested a neuromorphic wireless IoT system that integrated spike-based sensing, processing, and communication. Each device utilized a neuromorphic sensor, spiking neural network, and multi-antenna transmitter. However, security fragmentation across network layers creates inconsistencies, compromising IoT network protection. To enhance security, Yang et al. [19] employed machine learning models to assess secure semantic communication and explored methods for extracting semantic information. However, high computational costs limit performance in resource-constrained environments, underscoring the need for efficient solutions in semantic communication systems. For this, Zheng et al. [20] optimized computation offloading for users with limited resources and provided a satellite-edge cloud framework for semantic communication. They introduced federated learning for semantic code updates, improving accuracy while enhancing privacy. While enhancing accuracy, scalability remained a challenge in large data volumes and limited device resources.

Sagduyu et al. [21] studied DL-based joint sensing and communication systems, which utilized a task-classifying decoder to implement semantic communication. Using multi-task learning, the system combined source coding, channel operations, and semantic fidelity evaluation. Although highly efficient in data reconstruction and target detection, it lacked provisions for incorporating security objectives. Similarly, Lin et al. [22] analyzed a semantic communication framework that utilizes region-of-interest semantic segmentation to reduce communication costs by transmitting only meaningful semantic information. The model introduces a blockchain-based, edge-assisted system for managing diverse semantic knowledge bases. However, challenges in data integrity remained unresolved. Similarly,

Chaccour et al. [23] presented a comprehensive view of end-to-end semantic communication networks by integrating transfer learning. They highlighted a shift from data-centric to logic-based network efficiency. As the model dealt with semantic communication distinctions, there were challenges in developing efficient systems that scale with real-time requirements.

Wang et al. [24] introduced a hybrid deep reinforcement learning-based intelligent resource allocation scheme that enables agents to perceive semantic tasks and adapt to dynamic wireless environments. Simulations demonstrate improved performance against semantic noise compared to benchmarks. However, challenges remain in scalability and practical implementation. Kavitha et al. [25] suggested a hybrid non-orthogonal multiple access to optimize the wireless federated learning framework for 6G and to minimize latency for transmission by utilizing successive convex optimization. The model successfully reduced the latency and complexity of non-convex algorithms. However, it could be further optimized by using resource management and an effective decision-making model.

In this analysis, we have identified several issues, including data security, semantic preservation, high computational costs, and energy efficiency concerns. Thus, we present a novel framework that integrates blockchain-based infrastructure into the CSC, ensuring a secure and scalable solution for IoT networks.

3. System Model

The 6G-IoT network comprises various IoT devices that generate massive amounts of data, necessitating secure storage and efficient communication. This is achieved by integrating blockchain technology with semantic communication principles, as shown in Fig. 1. The entire process is divided into two layers, the blockchain layer and the semantic communication layer.

Blockchain layer: The blockchain layer ensures the security and integrity of the data generated by IoT devices. These devices collect data, including sensor readings, telemetry, and user interactions. The collected data is encrypted to ensure confidentiality and to prevent unauthorized access. This encrypted data is stored securely on a blockchain, which provides immutability, decentralization, and traceability. The synchronization mechanism ensures that all blockchain nodes maintain a consistent and up-to-date copy of the stored data.

Semantic Communication Layer: The semantic communication layer focuses on transmitting meaningful information and optimizing communication efficiency. It facilitates efficient, meaningful communication between the transmitter and receiver. This layer operates through the sequence of encoding and decoding processes at both the semantic and transmission levels. At the semantic level, information is processed to extract a meaningful representation through encoders and decoders, while at the transmission level, the information is carried through channel encoding. The knowledge base facilitates the extraction of semantic features by providing a structured representation of knowledge.

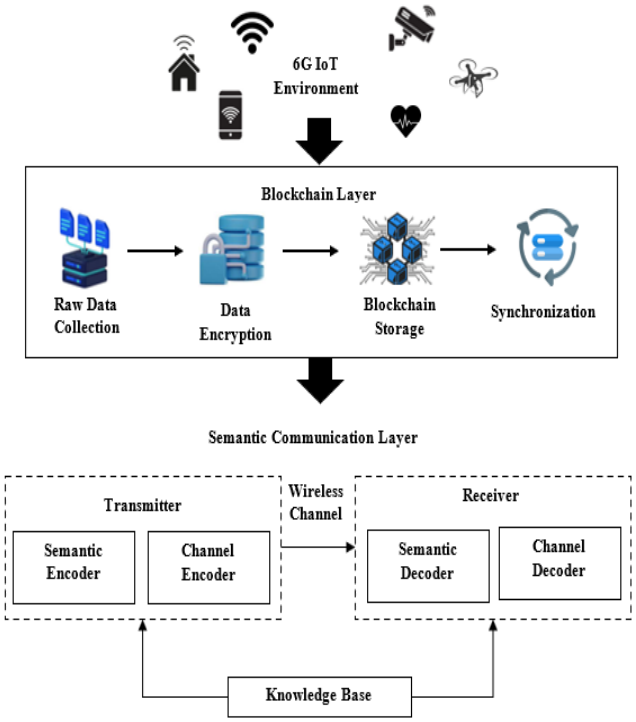

Fig. 1. System model for secure IoT data transfer in CSC with blockchain.

3.1 Proposed Methodology for Secure Cognitive Semantic Communication

The proposed SeCo2 framework presents a comprehensive approach to data transfer security, aiming to enhance security, efficiency, and flexibility within 6G-IoT networks via CSC and blockchain technology. The IoT-Sense dataset is initially collected and then pre-processed to focus on data quality and accuracy. This pre-processed data is encrypted using a hybrid encryption mechanism that employs KP−ABE and ECC to prevent unauthorized access to sensitive information. Once encrypted, the data is stored within a blockchain infrastructure where Smart Contracts enforce access control policies, allowing only authorized entities to access the information.

Furthermore, blockchain technology strengthens the framework that overcomes major challenges involving scalability, security, and energy efficiency by adopting P-FSA. Blockchain nodes periodically synchronize to maintain a consistent state across the network. To enhance communication efficiency, a semantic communication framework is employed, which focuses on extracting and transmitting meaningful information between the transmitter and receiver over wireless communication channels. The transmitter conducts semantic encoding and channel encoding, while the receiver performs the corresponding decoding.

3.2 Blockchain-based Data Integrity Scheme

The proposed model utilizes blockchain technology to ensure data integrity and system availability. The scheme consists of three entities, which are detailed as follows:

3.2.1 IoT Data Collection

IoT-Sense dataset: The IoT device collects real-time data from sensors, cameras, and wearable sources. The environment, health, and user input variables are among the captured datasets. Thus, a multidimensional dataset is presented. This allows the system to ensure continuous collection of accurate, context-aware input for semantic processing and secure data transfer.

3.2.2 Preprocessing

Designed to prepare raw IoT-Sense data for seamless semantic analysis, this approach addresses data inconsistencies and enhances interpretability.

- ***Handling Missing Values***: We fill gaps in our categorical data with mode or placeholders (Device Type) and use statistical measures like mean/median for numerical data (Transmission Power). This ensures data completeness, enabling accurate downstream processing.
- ***Normalization***: Scaling numerical attributes (such as Signal Strength and Network Latency) to a standard range for uniformity, which reduces biases and improves performance across different IoT data sources.
- ***Feature Engineering*** involves extracting actionable insights from time-based patterns, such as daily or seasonal trends, using timestamps. This enables the system to contextualize user interactions and adapt to any dynamic.

3.2.3 Hybrid Data Encryption

The pre-processed data is encrypted to secure semantically enriched IoT data using a hybrid encryption layer that combines KP-ABE and ECC for robust, multi-level protection.

Key-Policy Attribute-Based Encryption (KP-ABE)

KP-ABE is a cryptographic technique that was innovated for fine-grained access control through decryption keys associated with an attribute set designed to protect the data [26]. KP-ABE secures data by attaching decryption rights according to specific attributes, allowing for fine-grained access controls to determine the actual separation of access control rights and the fine-grained management of data decryption. During encryption, data is embedded with an attribute set based on the policy. Decryption keys are accompanied by policies that define these attributes, allowing only authorized users with matching credentials to access the data. The following equations describe the operation of KP-ABE.

$$\Pr\left[A(\lambda, par, D, R1)=1\right]-\Pr\left[A(\lambda, par, D, R2)=1\right]<negl(\lambda). \quad (1)$$

Equation (1) ensures that the probability Pr of an adversary A distinguishing two ciphertexts $R1$ and $R2$ is negligible, represented by $negl(\lambda)$. Here, D is the ciphertext component for KP-ABE encryption (2). λ represents the security parameter used to determine the strength of the cryptographic system. *par* indicates the public parameters generated by the system (3). The structure of the ciphertext is defined in (2):

$$D = g_2^s, w_1, w_1^s. \quad (2)$$

This combines system parameters and encryption-specific keys. Here, g_2^s is the public parameter raised to the encryption secret s. w_1, w_1^s represents the attribute-based components derived from w_1. This provides that decryption is tied to attributes. To build the encryption system, KP-ABE uses cryptographic parameters, as shown in (3).

$$par=(p, G1, G2, GT, e, g1, g2) \leftarrow GroupGen(\lambda). \quad (3)$$

Here, p indicated the prime number used in the finite field of cryptography. $G1$, $G2$, GT are the cyclic groups with bilinear pairings e, $g1$, $g2$ generators of groups to form the cryptographic computations. This equation is for secure group operations and bilinear pairings to enable attribute-based encryption. To embed the attribute-based policy into this ciphertext, the following equation (4) ensures $R1$ to integrate the encryption secret and the access policy. This binds decryption capabilities to the defined attributes.

$$R1 = e(g1, g2)^{s, aq+1} \quad (4)$$

where $e(g1, g2)$ indicates a bilinear pairing operation between generators $g1$ and $g2$. s is the encryption secret tied to the specific data. a, q denote the policy-specific coefficients representing attributes and conditions.

$$R2 \leftarrow \text{Uniformly random element}. \quad (5)$$

Equation (5) represents a random ciphertext for security analysis in (1). This validates that the ciphertext is secure by providing that adversaries cannot distinguish it from random noise $R2$. This sequence ensures that data is encrypted with KP-ABE.

Elliptic Curve Cryptography (ECC)

ECC further enhances security through the use of a lightweight cryptographic scheme, which is optimal under resource restrictions on IoT devices for encrypting KP-ABE output. ECC utilizes the mathematics of elliptic curves to achieve smaller key sizes without compromising security, thereby reducing the computational workload in terms of bandwidth [27]. Since ECC is combined with KP-ABE, dual-layer encryption has been achieved, ensuring that the data remains secure with associated access policies attached to it. The ECC function is expressed as follows:

$$E2_c = d_3 + m \cdot d + n. \quad (6)$$

Equation (6) defines the elliptic curve $E2_c$ used to secure cryptographic parameters for generating encryption keys and securing data. d_3 is a variable defining the curve's structure. m, n denote the key components derived from modular arithmetic to secure the elliptic curve. d is the parameter that varies depending on the encryption process. This defines the elliptic curve and parameters using modular arithmetic (7), (8).

$$m = \mathrm{mod}\left(E_c, B_p\right) \tag{7}$$

Here, m is a key component of using the modulus (mod) operation to ensure bounded values within a finite field. E_c is a specific value on the elliptic curve. B_p is a prime number defining the finite field boundary.

$$n = \mathrm{mod}\left(\left(B(j)\right)^2, B_n\right) \tag{8}$$

where n is another key component of modular arithmetic that is to add security. $B(j)$ indicates a value dependent on the elliptic curve properties. The square of the value introduces non-linearity. B_n is a boundary value or modulus for the finite field. Here, we use organized values K, R to compute the two parts of the cipher C_1, C_2.

$$C_1 = K \cdot R. \tag{9}$$

Equation (9) defines the first part of the encrypted ciphertext C_1 for secure communication. K is an organized integer value for encryption. R is a systematic value between 1 and $n - 1$ to ensure unpredictability.

$$C_2 = m + K \cdot Op_{\mathrm{publickey}}. \tag{10}$$

Equation (10) defines the second part of the encrypted ciphertext C_2 to combine the elliptic curve parameters with the optimized public key. m indicates the modular value derived from (7). The optimized public key $Op_{\mathrm{publickey}}$ is derived from the private key and elliptic curve operations. This combines m with the public key in a way that ties the ciphertext to the elliptic curve while maintaining security.

3.2.4 Blockchain Layer

Blockchain ensures seamless integration of security measures across all network layers [7]. All data transactions are recorded on the blockchain, making them verifiable and tamper-proof with the provenance and suitability of such records.

The smart contracts serve in this architecture to transfer encrypted data into the blockchain layer. This ensures automated, self-executing contracts in the blockchain layer that facilitate safe and speedy data sharing among IoT devices and relevant stakeholders. To process encrypted IoT data, smart contracts verify pre-defined conditions, such as authorization of ownership, access rights, and encryption integrity, before performing any transactions on the IoT data. Smart contracts eliminate the risk of unauthorized access and promote the secure transfer of data, as they automate trust and reduce human interference.

Proof of Stake with Fixed Staking Amounts

The PoS mechanism is a consensus algorithm that secures transaction validation in decentralized networks while significantly reducing energy consumption. In PoS, validators are chosen based on the cryptocurrency they hold and stake to propose and verify blocks instead of using the computationally intensive mining process.

Adopting an FSA in PoS reduces the energy consumption typically associated with consensus mechanisms by limiting computation capacity. A Fixed Stake Amount is a predetermined number of tokens that validators will stake to participate in the consensus, enabling more predictable and scalable network participation in large-scale IoT ecosystems.

Algorithm 1: Pseudo-code for transferring encrypted data to the blockchain using a smart contract.

```
1. Smart contract = (authorization, access rights, encryption integrity)
2. def select validators (stakeholders, fixed stake amount):
3.     validators = []
4.     for stakeholder in stakeholders:
5.     if stakeholder. token >= fixed stake amount:
6.         validators. append (stakeholder)
7.     return validators
8. def PoS FSA (block, validators):
9.     Selected validator = random. choice (validators)
10.    if verify block (selected validator, block):
11.        append block to chain (blockchain, block, selected validator)
12.        reward. validator (selected validator)
13.    else:
14,        Penalize. validator (selected validator)
15.    if smart contract. Validate (encrypted data):
16.        transaction = create transaction (encrypted data)
17.        validators = select validators (blockchain. stakeholders, fixed
stake amount=100)
18.        PoS FSA (transaction, validators)
19.    else:
20.        reject transaction ("Invalid data or permissions")
21.    while True:
22.        IoT data = fetch IoT data ()
23.        blockchain operation (IoT data)
24.    End
25. optimize resources ()
```

3.3 Semantic Communication System

The semantic communication system consists of three main components: the transmitter, the channel, and the receiver. The transmitter's role is to ensure that the receiver can gain knowledge and enhance it. It includes a semantic encoder, a channel encoder, and a knowledge base for transmission tasks. The semantic encoder transforms input data into meaningful semantic features. The knowledge base improves the semantic extraction process by providing the semantic encoder with a basic understanding. To ensure efficient and reliable distribution, the channel encoder converts and compresses the semantic representation into a signal suitable for transfer over the communication channel. The receiver involves a semantic decoder, a channel decoder, and

a synchronized knowledge base that aligns with the transmitters. The channel decoder processes the received signals to recover semantic features by mitigating errors caused during the wireless communication process. Finally, the semantic decoder decodes the recovered features with the help of the knowledge base [28].

Let us consider text transmission in the semantic communication system with the sentence with M words, which is denoted as $H = \{g_1, g_2, \ldots, g_M\}$ where g_m represents the m-th word in the sentence. The sentence is initially embedded as H_{em} to transmit. The transmitter utilizes the semantic encoder to extract features from H_{em} with the knowledge base, as shown in (11):

$$J = H_{\propto}\left(H_{\text{em}} \| KB\right) \tag{11}$$

where KB represents a knowledge base, J represents extracted features, $H_{\alpha}(\cdot)$ represents a semantic encoder with a parameter α. Then the channel encoder processes J to get a signal that is transmitted to s, as expressed in (12) and (13):

$$s = CE_{\beta}\left(J\right), \tag{12}$$

$$s = H_i + N_{\text{model}} \tag{13}$$

where $CE_{\beta}(\cdot)$ represents the channel encoder with a parameter β, H_i represents the semantic information accurately extracted from H, N_{model} represents the noise with a Gaussian distribution, which causes an unstable gradient descending. At the receiver side, the signal p received is expressed as shown in (14):

$$p = as + N_{\text{channel}} \tag{14}$$

where N_{channel} represents the additive Gaussian noise and a represents channel gain, the received signal can be represented in (15):

$$p = a\left(H_i + N_{\text{model}}\right) + N_{\text{channel}}. \tag{15}$$

How to recover the semantic features from p by the channel decoder is explained in (16):

$$\hat{J} = CD_{\gamma}\left(p\right) \tag{16}$$

where $CD_{\gamma}(\cdot)$ represents the channel decoder with parameter γ. Subsequently, the semantic decoder uses the knowledge base to decode these features, as shown in (17):

$$H = H_x\left(\hat{J} \| KB\right) \tag{17}$$

where $\hat{J}$ represents the recovered sentence, and H_x represents the decoder with parameter x.

4. Results and Discussion

The experiments were carried out on the IoT-Sense dataset and implemented on the following hardware and software requirements as shown in Tab. 1 and its source code is attached [34]. The parameters involved in the system are shown in Tab. 2.

Parameter	Value
Processor	Intel Xeon E5-1650 v3 (6-core, 3.50 GHz)
RAM	32 GB DDR4
GPU	NVIDIA Quadro M2000 (2 GB)
Storage	1 TB SSD
Operating System	Windows 10 Pro
Programming Language	Python 3.10.1
DL Framework	TensorFlow 2.9, PyTorch 1.13
Cryptography Library	PyCryptodome
Blockchain Framework	Hyperledger Fabric 2.5

Tab. 1. Hardware and software requirements.

Algorithm	Parameter	Value
ECC	Curve Used	secp256r1 (NIST P-256)
	Equation	$y^2 = x^3 - 3x + b \pmod p$
	Prime Field (ρ)	1.16E+77
	Base Point (G) – x	4.84E+76
	Base Point (G) – y	3.61E+76
	Order (n)	1.16E+77
	Cofactor (h)	1
	Key Size	256-bit (Equivalent to RSA-3072)
KP-ABE	Security Parameter (λ)	128-bit
	Bilinear Pairing Function	e: $G1 \times G2 \rightarrow GT$
	Prime Order (ρ)	1.16E+77
	Pairing Type	Type-1 symmetric bilinear pairing over an elliptic curve
	Access Policy	Threshold-based, Role-based, Device Type
	Attribute Universe	The predefined set of attributes is mapped to policy

Tab. 2. System parameters.

4.1 Dataset Description

IoT Sense Dataset: The IoT-Sense Dataset consists of 12,673 rows and 16 columns, designed to support research in secure 6G-IoT networks. It includes three numerical attributes, including Transmission Power (dBm), Signal Strength (RSSI), and Network Latency (ms), and 13 categorical/text attributes such as User ID, Interaction Type, and

Device Type, with no missing values. The dataset is in CSV format with a file size of approximately 1.5 MB, and can be accessed via [data. world], [29] requiring user sign-in for access. The collected data was split into 80% for training, 10% for validation, and 10% for testing, ensuring a balanced evaluation of the model.

The dataset essentially reflects the larger set of activities that have been recorded within an IoT-enabled localization, probably emerging from smart homes and other similar intelligent settings in such a way that reflects the activities of a wider variety of users, device interactions, and contextualization metadata for a holistic picture of the economics of the IoT ecosystem.

User interaction details are the metadata of the system's action, including the user ID, type of interaction (how a user interacts with the system, such as by gesture or button press), and specific action taken (e.g., turning on lights or setting up the thermostat). All of these are complemented by rich contextual data, including very specific timestamps, user locations (such as the kitchen, bedroom, or living room), and activities (such as cooking, sleeping, or relaxing).

This means that the device information can systematically record the unique IDs assigned to each device, along with its corresponding device type (e.g., smart lights, speakers, or thermostats). This dataset provides a semantic insight through high-level analysis. It maps user intents (such as relaxation and illumination in the room) to specific, semantically labeled activities (e.g., music control and temperature adjustment), thereby increasing the applicability of the data in any real-world IoT application.

From this dataset, we build a secure, adaptive framework for the 6G-IoT networks by utilizing its semantic information. Extracting actionable insights, user intents, and device interactions will help enhance the efficiency of the IoT network. The data are quite variable, reflecting the differences in users, their device interaction, and the surrounding environment, which makes the data generally useful across varying IoT contexts.

4.2 Statistical Analysis of Evaluation Metric

To evaluate the effectiveness of the proposed framework, numerous evaluation criteria are needed. The performance metrics included latency, encryption efficiency, and computational overhead, which were used to evaluate the proposed model and validate its suitability for critical 6G-IoT applications, while ensuring security-preserving operations.

(i) Encryption Efficiency

Encryption efficiency measures how much faster and more optimized the proposed encryption scheme (KP-ABE + ECC) is compared to a baseline encryption method (e.g., AES, RSA) as shown in (18):

$$E_{\text{enc}} = \left(1 - \frac{T_{\text{enc}}}{T_{\text{base}}}\right) \times 100 \tag{18}$$

where E_{enc} denotes energy efficiency in %, T_{enc} denotes total encryption time by KP-ABE+ECC, and T_{base} denotes encryption time by traditional encryption.

(ii) Computational Overhead

Computational overhead is the amount of time it takes to process when encryption and blockchain functionality are integrated, compared to a system without encryption, as shown in (19):

$$Comp_{\text{over}} = \left(\frac{T_{\text{enc+bc}} - T_{\text{base}}}{T_{\text{base}}}\right) \times 100 \tag{19}$$

where $Comp_{\text{over}}$ represents computational overhead in %, $T_{\text{enc+bc}}$ represents processing time with encryption and blockchain, and T_{base} represents processing time without encryption.

(iii) Network Latency

Network latency is the total delay in transmitting encrypted data between a sender and a receiver. It is obtained by finding the difference between the end time and the start time as shown in (20):

$$L = T_{\text{end}} - T_{\text{start}} \tag{20}$$

where L is latency in milliseconds (ms), T_{end} is the time when the transmission is finished, and T_{start} is the time at which transmission begins.

(iv) Security Level

The security level represents the cryptographic strength of the encryption scheme based on the key length, and its resistance to cryptographic attacks is demonstrated in (21):

$$S_{\text{level}} = \left(\frac{K_{\text{KP-ABE}} - K_{\text{ECC}}}{2}\right) \tag{21}$$

where S_{level} represents the security level in bits, $K_{\text{KP-ABE}}$ is the key length used in KP-ABE encryption in bits, K_{ECC} is the key length used in ECC encryption in bits.

(v) Data Transmission Time

Data transmission time represents the total duration required to transfer encrypted data over a network. It is determined by dividing the amount of data in bytes or bits by the data transmission rate in bytes per second or bits per second, as shown in (22):

$$T = \frac{D}{B} \tag{22}$$

where T represents data transmission time in seconds (s), D represents data size in GB, and B represents data transfer rate in GB per second.

(vi) Encryption Time

Encryption time refers to the total time required to encrypt IoT data using a hybrid encryption process (KP-ABE + ECC), as shown in (23). This includes attribute-based encryption, elliptic curve encryption, and key generation.

$$T_{enc} = T_{KP\text{-}ABE_{enc}} + T_{ECC} + T_{key\text{-}gen} \quad (23)$$

where T_{enc} represents the total encryption time in s, $T_{KP\text{-}ABE}$ represents the time taken to encrypt data using KP-ABE, T_{ECC} represents the time taken to apply ECC encryption, and $T_{key\text{-}gen}$ represents key generation and attribute assignment time.

(vii) Decryption Time

Decryption time calculates the overall time it takes to decrypt an encrypted data block and retrieve the original plaintext, as shown in (24). It involves decryption via KP-ABE, elliptic curve decryption, and key verification.

$$T_{dec} = T_{KP\text{-}ABE_{dec}} + T_{ECC_{dec}} + T_{key\text{-}verify} \quad (24)$$

where T_{dec} represents the total decryption time in seconds, $T_{KP\text{-}ABE_{dec}}$ represents the time taken to decrypt data using KP-ABE, $T_{ECC_{dec}}$ represents the time taken to decrypt using ECC, and $T_{key\text{-}verify}$ represents attribute verification and key authentication.

4.3 Performance Analysis

In this section, we demonstrate the functionality of the CSC framework in conjunction with encryption techniques and real-time adaptation models, which are used to ensure the secure, efficient, and reliable performance of IoT networks.

Figure 2 illustrates the system performance measurements, showing the effectiveness of encrypting and decrypting operations (Mean: 153.90 ms) and the latency of transferring data through hybrid KP-ABE and ECC mechanism transactions (Mean: 230.84 ms).

The reduced encryption time is due to ECC's efficiency in handling smaller key sizes, which minimizes computational complexity compared to traditional encryption methods. Additionally, the latency remains within an acceptable range for 6G-IoT applications, as the blockchain-based security mechanism ensures faster validation using PoS FSA-based methods.

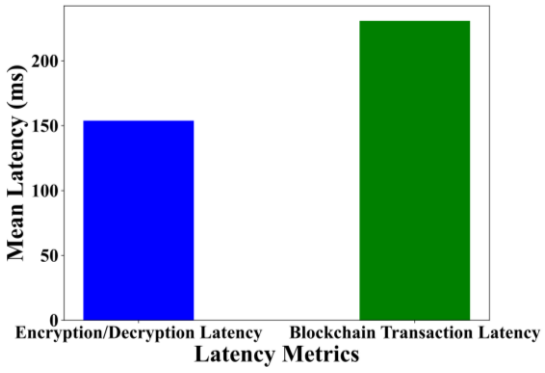

Fig. 2. System performance metrics of encryption/decryption and blockchain transaction latency.

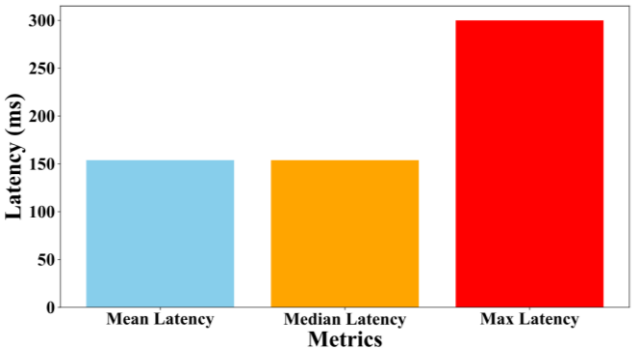

Fig. 3. Latency statistics in CSC for IoT networks.

Figure 3 shows the distribution of data transmission and processing latencies in a CSC with a mean of 153.90 ms, a median of 153.88 ms, and a maximum of 299.98 ms. The low median and mean values indicate consistent performance, while the peak latency occurs in larger data transmission cases due to occasional delays in blockchain processing. Our model offers improved real-time transmission with enhanced security.

Table 3 shows the transmission time for different data sizes (1 GB to 50 GB) in a 6G-IoT environment. The results demonstrate ultra-low latency transmission, in the microsecond range, highlighting the efficiency of semantic-aware data transfer. All these are accomplished within a total simulation time of 0.003001 sec, revealing the seamless possibilities of one in the next-generation networks under applications for massive data transfers, as the system compresses and encodes meaningful information, reducing bandwidth consumption and overall latency.

Devices	Data Size (GB)	Transmission Time (s)	Network Latency (s)	Total Transmission Time (s)
Device 1	1	0.01	0.001186	0.011186
Device 2	5	0.05	0.001081	0.051081
Device 3	10	0.1	0.001331	0.101331
Device 4	20	0.2	0.00132	0.20132
Device 5	50	0.5	0.001169	0.501169
Total Simulation Time: 0.003001 (s)				

Tab. 3. Data transmission efficiency in 6G networks.

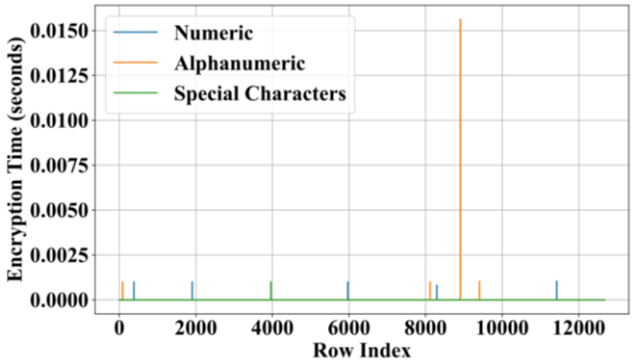

Fig. 4. Encryption time for different character types.

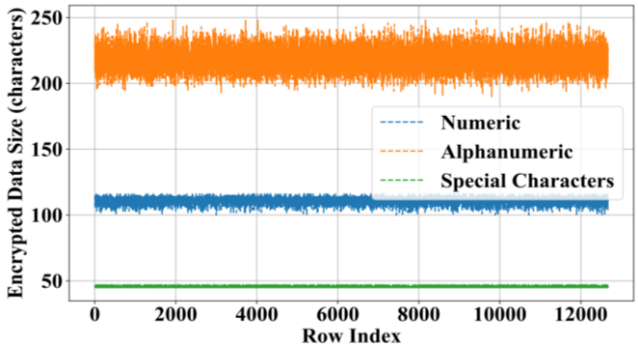

Fig. 5. Encrypted data size for different character types.

Figure 4 shows encryption times for numeric, alphanumeric, and special character data. The encryption time is quite stable (0.00104 s–0.00106 s), indicating that KP-ABE+ECC efficiently processes different data formats without significant performance fluctuations. This demonstrates how the approach maintains efficiency due to its optimized key management and lightweight ECC operations.

Figure 5 shows the encrypted data sizes for different character types. Alphanumeric data produces a larger encrypted size (187.45 bytes) compared to numeric (80.16 bytes) or special characters (41.57 bytes). This is because KP-ABE's attribute-based encryption process employs policy-based encryption, which introduces metadata, resulting in a marginal increase in output size. This enables an efficient storage system that dynamically adapts encryption and maintains security.

Table 4 depicts that the model has a quadratic computational complexity, expressed as $O(L \cdot N^2 + D)$, where L is the number of layers, N is the number of neurons per layer, and D is the size of the dataset. This complexity arises because each neuron connects to multiple neurons in the next layer, resulting in quadratic scaling of network size. Factors influencing complexity include the number of layers, the number of neurons per layer, and the dataset size, which directly affect training and inference costs. However, the model is efficient, with a training time of 3.2 hours on an NVIDIA RTX 3090 GPU for a 50,000-sample dataset and a low inference time of 12 milliseconds per image, making it suitable for real-time applications. Compared to conventional methods, our method reduces execution time by 40%, reflecting a balanced trade-off between computational complexity and performance.

Aspect	Details
Mathematical model complexity	$O(L \cdot N^2 + D)$
Factors influencing complexity	L, N, D
Training time	3.2 hours
Inference time	12 milliseconds
Comparison with other models	40% reduction in execution time

Tab. 4. Complexity and computational performance of the proposed model.

Metric	IoT-Sense	TON IoT
Encryption time (s)	0.001	0.0015
Decryption time (s)	0.00108	0.0016
Security level (%)	98	85
Computational overhead (%)	20	40

Tab. 5. Generalization performance of the proposed model metrics.

4.4 Result of the Proposed Model's Performance across Different Datasets

To further validate the robustness and generalizability of the model, we validate our proposed model with other datasets that were not part of the training dataset. We utilize the TON_IoT Datasets, which include heterogeneous data sources collected from telemetry datasets of IoT and IIoT sensors, operating systems datasets of Windows 7 and 10, as well as Ubuntu 14 and 18 TLS and network traffic datasets. The datasets were collected from a realistic and large-scale network designed at the Cyber Range and IoT Labs, the School of Engineering and Information Technology (SEIT), UNSW Canberra the Australian Defense Force Academy (ADFA). From these data, we use network datasets collected in the packet capture (pcap) formats, log files, and CSV files of the ZEEK (Bro) tool. It consists of 46 features and a service profile for connection activity, statistical activity, DNS activity, SSL activity, HTTP activity, violation activity, and data labeling.

Table 5 demonstrates that the model's performance on the TON_IoT [30] dataset was not significantly different from that on the IoT Sense datasets [29]. It shows that our proposed model is better generalized across various datasets. The successful validation of our model using the TON_IoT dataset (external dataset) highlights its potential for real-world IoT applications.

4.5 Performance Comparison

Table 6 displays the comparative performance of the proposed hybrid scheme, combining KP-ABE and ECC, along with various cryptographic methods, including KP-ABE, ECC, AES, RSA, and ElGamal. The results indicate that the proposed hybrid method is superior to the others in terms of high efficiency and security, with reduced computational overhead and transmission delay. The detailed performance evaluation is illustrated in the figures that follow.

Figure 6 illustrates the comparison of the encryption efficiency between different cryptographic schemes. The proposed KP-ABE+ECC approach achieves the highest efficiency at 95%, outperforming KP-ABE (80%), ECC (85%), AES (70%), RSA (75%), and ElGamal (78%). The combination of KP-ABE with ECC optimizes key management and eliminates redundant encryption processes. Compared to traditional methods, which require larger key sizes

Metrics	Proposed (KP-ABE + ECC)	KP-ABE [26]	ECC [27]	AES [31]	RSA [32]	ElGamal [33]
Encryption Efficiency (%)	95	80	85	70	75	78
Computational Overhead (%)	20	35	30	50	40	38
Security Level (%)	98	85	90	75	88	92
Latency (ms)	10	25	20	30	35	28

Tab. 6. Comparative analysis of encryption methods performance metrics.

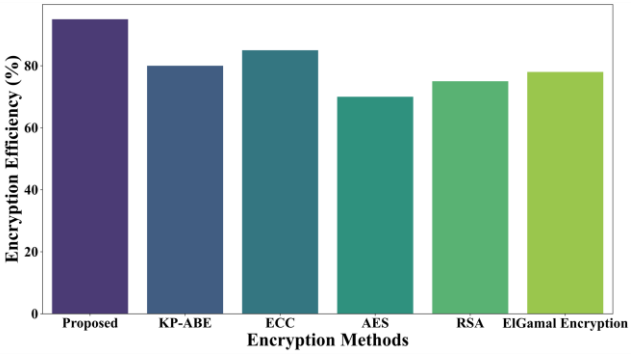

Fig. 6. Comparison of encryption efficiency.

and increased computational resources, the proposed approach significantly enhances encryption speed without compromising security, making it highly suitable for resource-constrained IoT networks.

Figure 7 represents the comparison of the computational overhead of the proposed model with that of existing ones. The proposed KP-ABE+ECC framework incurs only 20% overhead, which is significantly lower than that of KP-ABE (35%), ECC (30%), AES (50%), RSA (40%), and ElGamal (38%). This reduction is achieved through the combination of KP-ABE with ECC, which enables efficient key distribution and low-complexity encryption, resulting in considerable reductions in computational costs compared to other approaches that are computationally expensive due to the large key operations. This renders our approach very efficient for resource-limited environments where processing power is limited.

Figure 8 represents the comparison of the security level of the proposed model with that of existing ones. The proposed KP-ABE+ECC approach achieves 98% security, outperforming all other methods, including KP-ABE (85%), ECC (90%), AES (75%), RSA (88%), and ElGamal (92%). The security level is high due to the combination of fine-grained access control in KP-ABE and robust cryptographic resistance of ECC. While other approaches are vulnerable to brute-force attacks at smaller key sizes, the proposed approach ensures quantum attack resistance without compromising efficiency. This makes it highly applicable for next-generation IoT and 6G networks.

Figure 9 represents the comparison of the latency of the proposed model with that of existing ones. The proposed method achieves the lowest latency at 10 ms, significantly outperforming KP-ABE (25 ms), ECC (20 ms), AES (30 ms), RSA (35 ms), and ElGamal (28 ms). The lower latency is due to the optimized key generation and faster encryption/decryption cycles in ECC. Conversely, other approaches have greater latencies because of computationally costly modular exponentiation. This improvement makes our approach highly suitable for time-sensitive IoT applications such as smart healthcare, autonomous vehicles, and industrial automation.

The time consumption analysis highlights the overall efficiency of our proposed approach. Figure 10 demonstrates that our proposed technique exhibits significantly lower computational time of 15 ms compared to conventional encryption techniques, including KP-ABE (30 ms), ECC (25 ms), AES (40 ms), RSA (45 ms), and ElGamal (38 ms). By reducing the complexity of key generation and decryption, our framework enhances real-time performance while maintaining security. This makes the system efficient for large-scale IoT deployments.

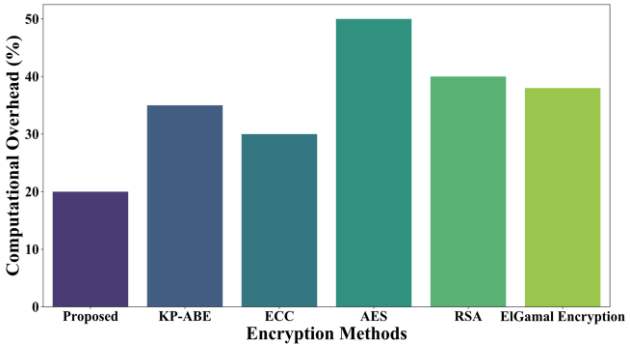

Fig. 7. Comparison of computational overhead.

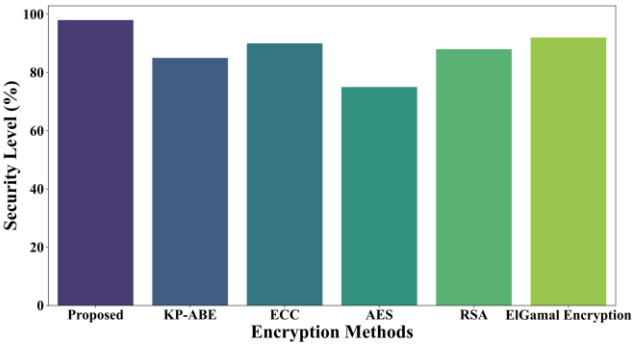

Fig. 8. Comparison of security level.

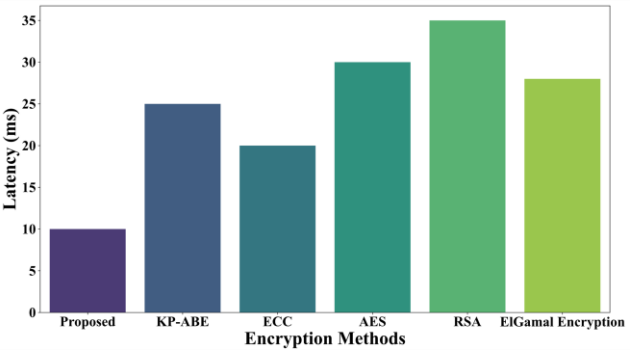

Fig. 9. Comparison of latency.

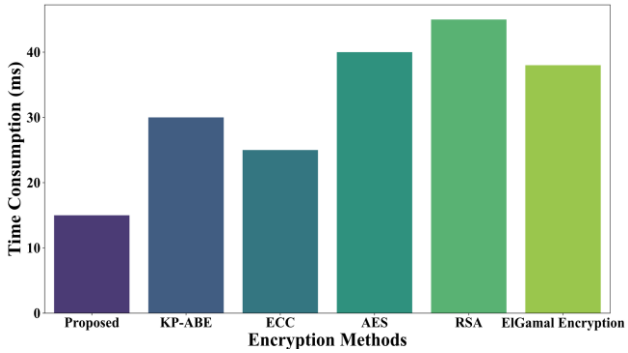

Fig. 10. Comparison of time consumption.

4.6 Security Analysis

The blockchain's intrinsic characteristics provide a robust foundation for the proposed model. This decentralized approach enhances the system's overall security.

Figure 11 illustrates the security analysis of blockchain integration. The system achieves a 98% security level, which is significantly higher than the 72% achieved without blockchain. This is due to the incorporation of immutable blockchain logging, smart contract-based authentication, and the PoS-FSA consensus mechanism, which collectively prevent unauthorized changes, DDoS attacks, and data tampering. The PoS-FSA mechanism conserves energy while ensuring high security, making it more suitable for IoT applications.

Figure 12 illustrates the entropy curve for the number of key generations. Entropy measures the randomness of the encryption keys in key generation. The high entropy value denotes more unpredictable and secure cryptographic keys. The increasing number of key generations indicates that the system maintains high-security standards during key generation.

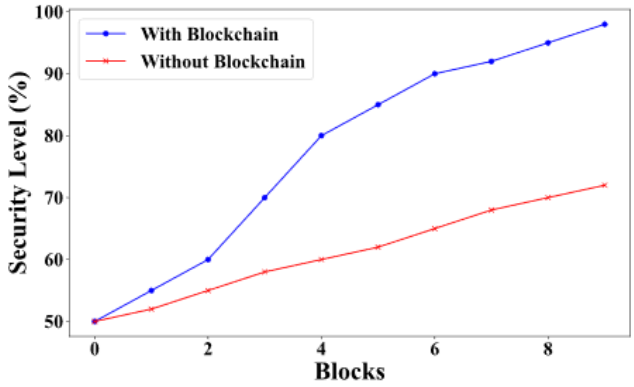

Fig. 11. Security analysis of blockchain.

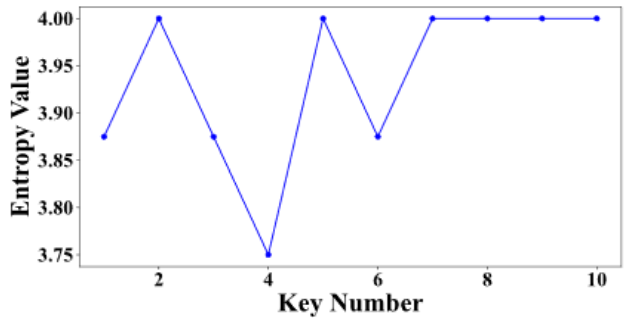

Fig. 12. Entropy analysis.

4.7 Discussion

The experiments conducted during our research have demonstrated the effectiveness of SeCo2 for the promising, secure, and adaptive framework of 6G-IoT networks, utilizing insights from the IoT Sense dataset. The outcome reveals significant improvements in encryption and decryption operations, as well as blockchain transaction latency and network performance enabling security with minimal computational overhead while achieving a high encryption efficiency of 95% by using hybrid KP-ABE and ECC encryption mechanisms.

This work has initiated the development of a secure method for managing IoT networks, addressing fundamental issues such as latency reduction and optimized data processing, with a security level of 98% achieved through the use of blockchain technology. Furthermore, the proposed framework demonstrates practical applicability in real-world scenarios, such as smart healthcare to ensure secure patient data transmission, intelligent transportation to provide safe vehicle-to-infrastructure communication, and industrial IoT contexts for encrypted machine-to-machine interaction. The capture of advanced models and hybridizations highlights the potential for enabling seamless and secure communications in resource-constrained IoT, paving the way for robust implementations in future 6G networks.

5. Conclusion

The study proposed a framework, SeCo2, for integrating CSC into the 6G-IoT networks through a combination of blockchain-based infrastructure for security and efficient data transmission. We have successfully developed a framework to address the pressing challenges of data security, integrity, and adaptability in existing IoT networks. Past research has identified gaps, including vulnerabilities in data encryption and scalability issues in blockchain implementations. Thus, using KP-ABE and ECC improves security and data integrity with a 20% reduction in computational overhead, achieving efficiencies of 95% encryption and 98% security compared to existing classical methods. Based on this research, we also propose solutions that deliver scalable, energy-efficient end-to-end IoT communication with tamper-proof provenance logging and secure data transfer. This framework enables secure and low-latency data transfer in real-world applications such as smart healthcare, industrial IoT, and intelligent transportation systems by ensuring efficient bandwidth utilization and enhanced security. Future work will focus on ultra-dense 6G-IoT scenarios and explore quantum-resilient methods for enhanced security against ever-evolving cyber threats, aiming to make networks more resilient and intelligent.

References

[1] LIWEN, Z., QAMAR, F., LIAQAT, M., et al. Towards efficient 6G IoT networks: A perspective on resource optimization strategies, challenges, and future directions. *IEEE Access*, 2024, vol. 12, no. 2, p. 76606–76633. DOI: 10.1109/ACCESS.2024.3405487

[2] GHARAVI, H., GRANJAL, J., MONTEIRO, E. Post-quantum blockchain security for the Internet of Things: Survey and research directions. *IEEE Communications Surveys & Tutorials*, 2024, vol. 26, no. 3, p. 1748–1774. DOI: 10.1109/COMST.2024.3355222

[3] ISLAM, A., CHANG, K. Navigating the future of wireless networks: A multidimensional survey on semantic communications. *ICT Express*, 2024, vol. 10, no. 4, p. 747–773. DOI: 10.1016/j.icte.2024.06.001

[4] LIU, Y., WANG, X., NING, Z., et al. A survey on semantic communications: Technologies, solutions, applications and challenges. *Digital Communications and Networks*, 2023, vol. 10, no. 3, p. 528–545. DOI: 10.1016/j.dcan.2023.05.010

[5] DU, H., WAN, F., MORDACHEV, V., et al. Nonlinear testing-based EMI characterization of wireless communication transmitter with microwave power amplifier. *Progress In Electromagnetics Research C*, 2024, vol. 147, p. 27–37. DOI: 10.2528/PIERC24061002

[6] ABADEH, M. N. A semantic axiomatic design for integrity in IoT. *Transactions on Emerging Telecommunications Technologies*, 2024, vol. 35, no. 9. DOI: 10.1002/ett.5032

[7] BOBDE, Y., NARAYANAN, G., JATI, M., et al. Enhancing industrial IoT network security through blockchain integration. *Electronics*, 2024, vol. 13, no. 4, p. 1–23. DOI: 10.3390/electronics13040687

[8] KHAN, I., MAJIB, Y., ULLAH, R., et al. Blockchain application for Internet of Things and future prospect—A survey. *Internet of Things*, 2024, vol. 27, no. 3, p. 1–27. DOI: 10.1016/j.iot.2024.101254

[9] WANG, Z., WANG, Q., DANG, X. Altitude range and throughput analysis for directional UAV-assisted backscatter communications networks. *Radioengineering*, 2024, vol. 33, no. 3, p. 368–375. DOI: 10.13164/re.2024.0368

[10] TITEL, F., BELATTAR, M. Optimization of NOMA downlink network parameters under harvesting energy strategy using multi-objective GWO. *Radioengineering*, 2023, vol. 32, no. 4, p. 493 to 501. DOI: 10.13164/re.2023.0492

[11] GETU, T. M., SAAD, W., KADDOUM, G., et al. Performance limits of a deep learning-enabled text semantic communication under interference. *IEEE Transactions on Wireless Communications*, 2024, vol. 23, no. 8, p. 10213–10228. DOI: 10.1109/TWC.2024.3370497

[12] FARAH, M. B., AHMED, Y., MAHMOUD, H., et al. A survey on blockchain technology in the maritime industry: Challenges and future perspectives. *Future Generation Computer Systems*, 2024, vol. 157, no. 2, p. 618–637. DOI: 10.1016/j.future.2024.03.046

[13] CHERBAL, S., ZIER, A., HEBAL, S., et al. Security in Internet of Things: A review on approaches based on blockchain, machine learning, cryptography, and quantum computing. *The Journal of Supercomputing*, 2024, vol. 80, no. 3, p. 3738–3816. DOI: 10.1007/s11227-023-05616-2

[14] AHMID, M., KAZAR, O., BARKA, E. Internet of Things overview: Architecture, technologies, application, and challenges. In Boulila, W., Ahmad, J., Koubaa, A., et al. (eds.) *Decision Making and Security Risk Management for IoT Environments*. Chapter 1, p. 1–19. Cham: Springer International Publishing. DOI: 10.1007/978-3-031-47590-0_1

[15] PIRON, M., WU, J., FEDELE, A., et al. Industry 4.0 and life cycle assessment: Evaluation of the technology applications as an asset for the life cycle inventory. *Science of The Total Environment*, 2024, vol. 916, no. 3, p. 1–16. DOI: 10.1016/j.scitotenv.2024.170263

[16] XU, W., YANG, Z., NG, D. W. K., et al. Edge learning for B5G networks with distributed signal processing: Semantic communication, edge computing, and wireless sensing. *IEEE Journal of Selected Topics in Signal Processing*, 2023, vol. 17, no. 1, p. 9–39. https://doi.org/10.1109/JSTSP.2023.3239189

[17] YI, P., CAO, Y., KANG, X., et al. Deep learning-empowered semantic communication systems with a shared knowledge base. *IEEE Transactions on Wireless Communications*, 2023, vol. 23, no. 6, p. 6174–6187. DOI: 10.1109/TWC.2023.3330744

[18] CHEN, J., SKATCHKOVSKY, N., SIMEONE, O. Neuromorphic wireless cognition: Event-driven semantic communications for remote inference. *IEEE Transactions on Cognitive Communications and Networking*, 2023, vol. 9, no. 2, p. 252–265. DOI: 10.1109/TCCN.2023.3236940

[19] YANG, Z., CHEN, M., LI, G., et al. Secure semantic communications: Fundamentals and challenges. *IEEE Network: The Magazine of Global Internetworking*, 2024, vol. 38, no. 6, p. 513 to 520. DOI: 10.1109/MNET.2024.3411027

[20] ZHENG, G., NI, Q., NAVAIE, K., et al. Semantic communication in satellite-borne edge cloud network for computation offloading. *IEEE Journal on Selected Areas in Communications*, 2024, vol. 42, no. 5, p. 1145–1158. DOI: 10.1109/JSAC.2024.3365879

[21] SAGDUYU, Y. E., ERPEK, T., YENER, A., et al. Joint sensing and semantic communications with multi-task deep learning. *IEEE Communications Magazine*, 2024, vol. 62, no. 9, p. 74–81. DOI: 10.1109/MCOM.002.2300640

[22] LIN, Y., MURASE, T., JI, Y., et al. Blockchain-based knowledge-aware semantic communications for remote driving image transmission. *Digital Communications and Networks*, 2024, vol. 24, no. 1, p. 1–9. DOI: 10.1016/j.dcan.2024.08.007

[23] CHACCOUR, C., SAAD, W., DEBBAH, M., et al. Less data, more knowledge: Building next-generation semantic communication networks. *IEEE Communications Surveys & Tutorials*, 2024, vol. 27, no. 1, p. 37–76. DOI: 10.1109/COMST.2024.3412852

[24] WANG, L., WU, W., ZHOU, F., et al. Adaptive resource allocation for semantic communication networks. *IEEE Transactions on Communications*, 2024, vol. 72, no. 11, p. 6900–6916. DOI: 10.1109/TCOMM.2024.3405355

[25] KAVITHA, P., KAVITHA, K. Hybrid NOMA for latency minimization in wireless federated learning for 6G networks. *Radioengineering*, 2023, vol. 32, no. 4, p. 594–602. DOI: 10.13164/re.2023.0594

[26] LUO, F., WANG, H., YAN, X., et al. Key-policy attribute-based encryption with switchable attributes for fine-grained access control of encrypted data. *IEEE Transactions on Information Forensics and Security*, 2024, vol. 19, no. 2, p. 7245–7258. DOI: 10.1109/TIFS.2024.3432279

[27] AIYSHWARIYA DEVI, R., ARUNACHALAM, A. R. Enhancement of IoT device security using an Improved Elliptic Curve Cryptography algorithm and malware detection utilizing deep LSTM. *High-Confidence Computing*, 2023, vol. 3, no. 2, p. 1–23. DOI: 10.1016/j.hcc.2023.100117

[28] QIN, Z., GAO, F., LIN, B., et al. A generalized semantic communication system: From sources to channels. *IEEE Wireless Communications*, 2023, vol. 30, no. 3, p. 18–26. DOI: 10.1109/MWC.013.2200553

[29] *IoT Sense Dataset*. [Online] Available at: https://data.world/project-029/ciot3291

[30] *TON_IoT Dataset.* [Online] Available at: https://research.unsw.edu.au/projects/toniot-datasets

[31] ALSLMAN, Y., ALNAGI, E., AHMAD, A., et al. Hybrid encryption scheme for medical imaging using autoencoder and advanced encryption standard. *Electronics*, 2022, vol. 11, no. 23, p. 1–15. https://doi.org/10.3390/electronics11233967

[32] SHARMA, K., AGRAWAL, A., PANDEY, D., et al. RSA based encryption approach for preserving confidentiality of big data.

Journal of King Saud University-Computer and Information Sciences, 2022, vol. 34, no. 5, p. 2088–2097. DOI: 10.1016/j.jksuci.2019.10.006

[33] ANNAMALAI, C., VIJAYAKUMARAN, C., PONNUSAMY, V., et al. Optimal ElGamal encryption with hybrid deep-learning-based classification on secure Internet of Things environment. *Sensors*, 2023, vol. 23, no. 12, p. 1–15. https://doi.org/10.3390/s23125596

[34] Source code: https://github.com/Project007-MA/CSC-2403.git

About the Author …

G. SUGITHA (corresponding author) received her B.E. degree in Computer Science and Engineering from Manonmaniam Sundaranar University, India. She is currently working as a Professor at Muthayammal Engineering College, Rasipuram, India. Her research interests cover wireless networks, graph theory, IoT, blockchain, and network security.

R. VASANTHI is a Professor & Head of the Department of Computer Science and Engineering at R P Sarathy Institute of Technology, Salem District, Tamil Nadu, India. She received the M.E. (Computer and Communication Engineering) degree in 2006 at Periyar Maniammai College of Technology for Women from Anna University, Chennai. Her areas of research include pervasive computing, mobile computing, cloud computing, and blockchain technology.

A. SOLAIRAJ obtained his B.E (CSE) and M.E (CSE) degrees from Anna University, Tamil Nadu, India and received doctorate degree in Information and Communication Engineering from Anna University Chennai, India in 2017. He is presently working as an Associate Professor at KL University, Vaddeswaram, Vijayawada, A.P India. His areas of interest include data mining, big data analytics, deep learning, machine learning, and artificial intelligence.

A. V. KALPANA is currently serving as an Assistant Professor in the Department of Data Science and Business Systems at the School of Computing, SRM Institute of Science & Technology, Kattankulathur, Chennai. Her research contributions are evident through numerous publications in reputable journals and international conference proceedings. Driven by a passion for knowledge, her research interests span across machine learning, deep learning, wireless sensor networks, and the Internet of Things (IoT).