International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(11s) 2026 pp. 257-282
https://doi.org/10.70917/ijcisim-2026-3754
Article

Adaptive Swarm Intelligence-Driven Elliptic Curve Cryptography Optimization for Secure and Lightweight Data Transmission in Agricultural Internet of Things

Kumar K[1*], K. Sasikala[2]

[1*]Vinayaka Mission's Kirupananda Variyar Engineering College, Vinayaka Mission's Research Foundation, Salem, India
[2]Department of Information Technology, R P Sarathy Institute of Technology, Salem, India
Corresponding Authors Mail: kumar.k542254@gmail.co

Abstract: IoT technology has revolutionized smart agriculture by enabling connected sensors to continuously monitor soil, crops, livestock, irrigation, and environmental conditions. However, agricultural IoT networks remain vulnerable to unauthorized access, replay attacks, man-in-the-middle (MITM) attacks, eavesdropping, and data tampering because of resource-constrained devices and insecure wireless channels. To address these challenges, this paper proposes an Adaptive Swarm Intelligence-Driven Elliptic Curve Cryptography Optimization (ASI-ECCO) approach for lightweight and secure data transmission. The key novelty of ASI-ECCO is the proposed Adaptive Security–Resource Coupling (ASRC) mechanism, which dynamically adjusts the optimization priorities of security strength, computational efficiency, energy consumption, and communication overhead according to the current security-risk and residual-energy conditions of agricultural IoT nodes. Unlike conventional ECC optimization approaches using fixed objective weights, ASRC enables context-aware selection of ECC parameters to achieve an adaptive balance between cryptographic protection and resource utilization. Furthermore, an Adaptive Multi-Layer Threat Cognition Network (AMTC-Net) is proposed for adaptive trust evaluation, communication behavior analysis, cryptographic verification, and threat classification. The optimized ECC mechanism supports encryption, authentication, secure key exchange, and data-integrity verification across sensor, gateway, and cloud-server communications. Experimental results demonstrate cryptographic overhead, communication accuracy, communication transparency, energy consumption, threat detection rate, and false positive rate of 18.42%, 95.60%, 95.80%, 5.86 J, 96.34%, and 3.21%, respectively, demonstrating the effectiveness of the proposed framework for secure and resource-efficient agricultural IoT communication.

Keywords: Internet of Things (IoT); Smart Agriculture; Elliptic Curve Cryptography (ECC); Adaptive Swarm Intelligence; Secure Data Transmission; Lightweight Cryptography; Agricultural Cybersecurity; Precision Farming.

1. Introduction

The Internet of Things (IoT) has transformed agriculture in today's world, allowing for intelligent monitoring, automation, and data-driven decision-making in an agricultural setting. Smart agricultural systems utilize many interconnected sensing devices that constantly monitor soil moisture, soil temperature, soil humidity, crop health, irrigation systems, activities of the livestock and environmental conditions [1]. Through the use of these IoT-powered sensing platforms, farmers can now collect and transmit data in real-time, thereby enhancing resource usage, optimizing crop production, cutting down on operational expenses, and ensuring sustainable farming practices [2]. With the advent of cloud computing, wireless communication technology and edge intelligence, the capabilities of an agricultural IoT network have been further expanded to enable precision agriculture to become an integral part of modern food production systems [3].

While agriculture IoT provides many advantages in terms of operations, the large-scale use of WSNs creates many security and privacy challenges. A typical IoT sensor node typically has a small number of computational resources, memory, and battery capacity, making the use of traditional cryptographic methods expensive [4]. In addition, Wireless communication channels are very vulnerable to cyber-attacks like Man in Middle, Impersonation, Eavesdropping, Replay and Unauthorized Access. These attacks can impact critical agricultural data, alter sensor data, interfere with irrigation plans, and affect agricultural processes. So, it is one of the most urgent research challenges in agricultural IoT scenarios to create reliable, lightweight and energy efficient communication mechanisms [5].

Thus, Elliptic Curve Cryptography (ECC) has been one of the most promising public-key cryptographic techniques for resource-limited IoT devices, owing to its smaller key size, low computational complexity and high security features than conventional cryptographic methods. ECC offers relatively low computational resources and secure key exchange, digital authentication, encryption of information and data integrity verification [6]. The performance of elliptic curve security, however, is highly reliant on proper choice of elliptic curve parameters and cryptographic key generation methods [7]. Traditional parameter selection methods typically search for fixed parameters that do not adjust to changing network conditions, resulting in higher computational, communication latency and energy usage in large scale agricultural settings [8].

To address this, this research presents an Adaptive Swarm Intelligence-Driven Elliptic Curve Cryptography Optimization (ASI-ECCO) framework to optimize the ECC cryptographic process intelligently based on the principles of adaptive swarm intelligence. In contrast to traditional optimization, the proposed ASI-ECCO framework optimizes the selection of the parameters of elliptic curves, cryptographic key generation, security parameter refinement and lightweight key management all simultaneously [9]. By optimizing the ECC module, the system can improve the efficiency of encryption operations and minimize the communication overhead and complexity, ensuring secure communication between sensor nodes and various computing components in the IoT ecosystem [10]. Moreover, the framework improves security from unauthorized access, replay attacks, man-in-the-middle attacks and eavesdropping, and it also ensures energy efficient communication for resource constrained IoT devices [11].

The adaptive optimization combined with lightweight public-key cryptography is proposed to be integrated into the development of secure and scalable agricultural IoT infrastructures. Through experimental tests, the proposed ASI-ECCO framework is shown to provide better communication security with a 25% reduction in cryptographic overhead, i.e. it provides 95.6% communication accuracy and 95.8% communication transparency. The enhancements demonstrate the success of the suggested optimization method for achieving a trade-off between security, computational efficiency, and communication reliability [12]. Overall, the proposed ASI-ECCO framework offers a scalable and practical cryptographic solution for next-generation smart agriculture, enabling secure data transmission and facilitating intelligent farming applications and sustainable agricultural development.

1.1 Key contribution

Following are the major contributions of the study,

- A novel Adaptive Swarm Intelligence-Driven Elliptic Curve Cryptography Optimization (ASI-ECCO) framework is proposed for lightweight and secure data transmission in resource-constrained agricultural Internet of Things (IoT) networks.
- A novel Adaptive Security–Resource Coupling (ASRC) mechanism is introduced within ASI-ECCO to dynamically adjust the optimization priorities of security strength, computational efficiency, energy consumption, and communication overhead according to the current security-risk level and residual-energy state of IoT nodes. This enables context-aware ECC parameter selection rather than relying on fixed optimization weights.
- An adaptive swarm intelligence optimization strategy is developed to identify suitable elliptic curve parameters and cryptographic configurations, thereby improving security–efficiency trade-offs while reducing computational and communication burdens.
- An optimized ECC-based key generation mechanism is designed to provide robust cryptographic protection with reduced key-generation time and processing overhead, supporting lightweight security for resource-constrained agricultural IoT devices.
- A lightweight cryptographic communication mechanism integrating public-key encryption, secure key exchange, digital authentication, and data-integrity verification is developed to protect communication among IoT sensor nodes, agricultural gateways, and cloud servers.

- A novel Adaptive Multi-Layer Threat Cognition Network (AMTC-Net) is introduced for intelligent threat analysis through adaptive trust evaluation, communication behavior assessment, cryptographic verification, and dynamic threat classification against unauthorized access, replay attacks, man-in-the-middle (MITM) attacks, eavesdropping, and data tampering.
- An energy-aware lightweight cryptographic management strategy is incorporated to minimize communication and processing energy consumption while improving communication efficiency and extending the operational lifetime of resource-constrained agricultural IoT sensor nodes.
- Comprehensive experimental evaluation demonstrates the effectiveness of the proposed ASI-ECCO and AMTC-Net framework in terms of cryptographic overhead, communication accuracy, communication transparency, energy consumption, threat detection, and false-positive rate, achieving 18.42% cryptographic overhead, 95.60% communication accuracy, 95.80% communication transparency, 5.86 J energy consumption, 96.34% threat detection rate, and 3.21% false-positive rate.
- The integration of ASRC-driven ECC optimization and AMTC-Net-based adaptive threat cognition provides a scalable, secure, intelligent, and computationally efficient communication framework for next-generation smart agriculture, enabling resilient and energy-efficient precision farming applications.

2. Literature review

Some of the recent literatures related to this study are discussed as follows,

Has et al. (2024) [13] explored strategies for managing data efficiently in agriculture IoT systems, with insights into data compression techniques, security protocols, and MQTT communication. The study pointed out that agricultural data is produced in large quantity from resource constrained IoT devices adding more communication overhead and energy consumption. To solve this problem, the authors investigated various compression methods and security measures and concluded that Huffman Coding is an effective compression technique to reduce the obtained data size without compromising the quality of information. In addition, the use of Advanced Encryption Standard (AES) -based encryption was added to ensure the safe transmission of agricultural information while requiring minimal computing power. The experimental analysis showed that compression and encryption can be used together to achieve an appropriate communication efficiency and data security. The study focused mostly on the optimization of the data and the conventional methods of encryption, and did not take into consideration the adaptive cryptographic optimization mechanisms of dynamic agricultural IoT networks. This constraint encourages the design of intelligent lightweight security frameworks that can perform cryptographic operations in an optimized way based on the network conditions.

Shafik et al. (2024) [14] conducted an extensive study and survey of applications of IoTs in smart agriculture, which emphasized how connected sensors, wireless communication networks, cloud computing, and predictive analytics contribute to enhancing agricultural productivity. The study covered various components of IoT such as data acquisition devices, communication infrastructure, automation systems and decision support platforms. The authors showed how IoT-based smart farming helps to optimize water use, energy use, crop management, and sustainable farming. Wireless sensor networks and remote sensing technologies were identified as near real-time approaches for collecting agricultural data and cloud-based analytics for intelligent decision-making. The study did not, however, cover the security issues of wireless agricultural communication, but rather attempted to give an overview of IoT applications and future directions. The lack of lightweight cryptographic solutions underscores the necessity of secure and efficient data transmission solutions in agricultural IoT contexts.

Zhao et al. (2025) [15] suggested an IoT-based cloud platform for autonomous agricultural machinery to combine the narrowband IoT (NB-IoT) and 5G dual-channel communication technologies. Proposed system employed NB-IoT for low-power environmental monitoring and 5G for high bandwidth applications like task scheduling and path tracking. Furthermore, the authors proposed an enhanced Harris Hawk Optimization (IHHO) approach and Dijkstra's algorithm to coordinate multi-machine and optimise the path. The experimental outcomes revealed enhanced communication reliability, efficiency, and resource utilization for large-scale agricultural systems. Despite the successful transmission of information, the study was primarily oriented towards the optimization of the network and the automatic control of the machinery, excluding coordination. Security issues like cryptographic protection, authentication and attack resistance were not discussed in-depth, which also posed a research gap for creating secure communication mechanisms in agricultural IoT systems.

Selvam et al. (2025) [16] presented an IoT-based deep learning system for monitoring and forecasting abnormal activities in agricultural settings. The proposed solution involved integrating the IoT sensors with 5G communication

technologies and implementing Convolutional Neural Networks (CNNs) to analyze the agricultural data and detect any abnormal events. The framework allowed for real-time monitoring of agricultural fields and facilitated quick decision making as it is able to identify potential threats to crops and livestock. Results from the experiments demonstrated that the application of IoT and deep learning enhanced the ability to detect abnormal conditions over traditional monitoring systems. The research, however, mainly focused on the intelligent prediction and surveillance applications, and secure delivery of the collected IoT information was not taken into account. The integration of lightweight encryption and adaptive security mechanisms is still a key research need for agricultural monitoring systems as they communicate via wireless links, conveying sensitive information.

To improve data privacy and security in rural and agricultural settings, Vellimalaipattinam Thiruvenkatasamy et al. (2025) [17] proposed an IoT and intelligent blockchain-based framework. The proposed multi-tier architecture consisted of edge computing, fog computing, and cloud computing layers to enhance secure data processing and storage. The authors used Elliptic Curve Cryptography (ECC) and optimization methods to ensure secure data transmission and access. The evaluation showed that the proposed method improved the efficiency of encryption, memory usage and prediction compared to the existing method. However, these benefits are accompanied by additional transaction costs in terms of computation and communication, that can pose challenges for lightweight agricultural IoT devices with constrained resources. Thus, there is a need for adaptive cryptographic optimization methods for strong security with low computation complexities.

Elhattab and Abouelmehdi (2024) [18] suggested an energy-efficient smart agriculture system based on the LoRa communication technology, solar energy harvesting, and ESP32 controllers connected to IoT devices. The system could enable farmers to monitor their crops remotely and irrigate them automatically, using low-power communication networks and a network of sensors to gather data. The framework enabled efficient use of water resources by turning on the irrigation systems only when needed, thus minimizing energy and resource usage. The authors illustrated the low-cost, autonomous and easy-to-use solution for widespread agricultural fields to make it possible. But the study was primarily oriented towards the energy-saving aspects of monitoring and irrigation automation and did not discuss communication security or protection from cyber threats. This constraint highlights the need for lightweight and efficient security frameworks that can be effectively deployed in low powered agricultural IoT networks.

Morchid et al. (2024) [19] have suggested an integrated IoT-based architecture for early fire detection in smart agriculture to enhance the environment's security and safeguard agricultural resources. The proposed system comprised of three layers: IoT device layer, cloud processing layer, and application layer; which included smoke sensors, flame sensors, Raspberry Pi processing unit, and cloud visualization via ThingSpeak. Data collected in real-time, and processed through the cloud, helped to identify fire-related events quickly. The experimental results showed better responsiveness and accuracy in detection than that of conventional monitoring methods. But the proposed framework primarily focused on event detection and monitoring, not secure communication between IoT devices and cloud platforms. Agricultural IoT systems face many communication attacks, and embedding adaptive encryption and threat detection mechanisms is crucial for successful deployment.

To enhance crop growth efficiency and optimize resource usage, Wang and Gong (2024) [20] developed an intelligent greenhouse control system using IoT technology and machine learning algorithms. The proposed system was capable of continuously monitoring the parameters of the greenhouse, automatically controlling the internal parameters using the machine learning models. The framework was designed to improve the yield of the crops, minimise waste of resources, and offer more specific control of the greenhouse environment than existing rule-of-thumb approaches to greenhouse management. The study showed the effectiveness of using intelligent control systems based on the Internet of Things (IoT) in sustainable agriculture. The study, however, concentrated mainly on optimizing the environment and controlling processes automatically, and neglected secure data transmission and prevention of cyber threats. Therefore, a comprehensive framework combining intelligent optimization, lightweight cryptography, and adaptive threat protection is required for future smart agricultural IoT systems.

2.1 Research gap

Several studies have revealed the promising aspects of IoT, machine learning, blockchain, and communication technologies in contributing towards smart agriculture. Nevertheless, existing methods are mostly concerned about monitoring, automation, prediction, or data management but do not consider lightweight adaptive security approaches suitable for agricultural IoT systems with constrained resources. Traditional encryption methods impose additional computation cost, and blockchain technology-based approaches may need additional resources. It is necessary to design an intelligent scheme which simultaneously optimizes cryptographic parameters and communication overhead

while detecting cybersecurity threats. This leads to the design of the proposed ASI-ECCO scheme in conjunction with AMTC-Net for securing agricultural IoT communication.

3. Methodology

The suggested methodology offers an adaptive Swarm Intelligence-Driven Elliptic Curve Cryptography Optimization (ASI-ECCO) framework along with an Adaptive Multi-Layer Threat Cognition Network (AMTC-Net) in order to deliver secure, lightweight, and reliable communication in agricultural IoT networks. The general framework involves the collection of agricultural sensor data about the state of the soil, parameters of crops, environment, and farming processes; the preprocessing of data in order to increase their quality and enable the effective computation; normalization of data to be further passed to the ASI-ECCO framework where adaptive swarm intelligence is used for optimization of elliptic curve parameters, cryptographic keys generation and security settings to enhance the performance of encryption. As a result, the optimized ECC enables secure data transmission based on public-key encryption, secure key exchange, authentication, and integrity verification. In addition, the AMTC-Net constantly monitors the communication behavior, evaluates the level of trust, finds the abnormalities and classifies the possible cyber threats in order to increase the level of security of the network. Moreover, the lightweight key management and energy-aware optimization techniques are applied in order to lower the computational cost and increase communication efficiency. Figure 1 shows the Overall architecture of the study.

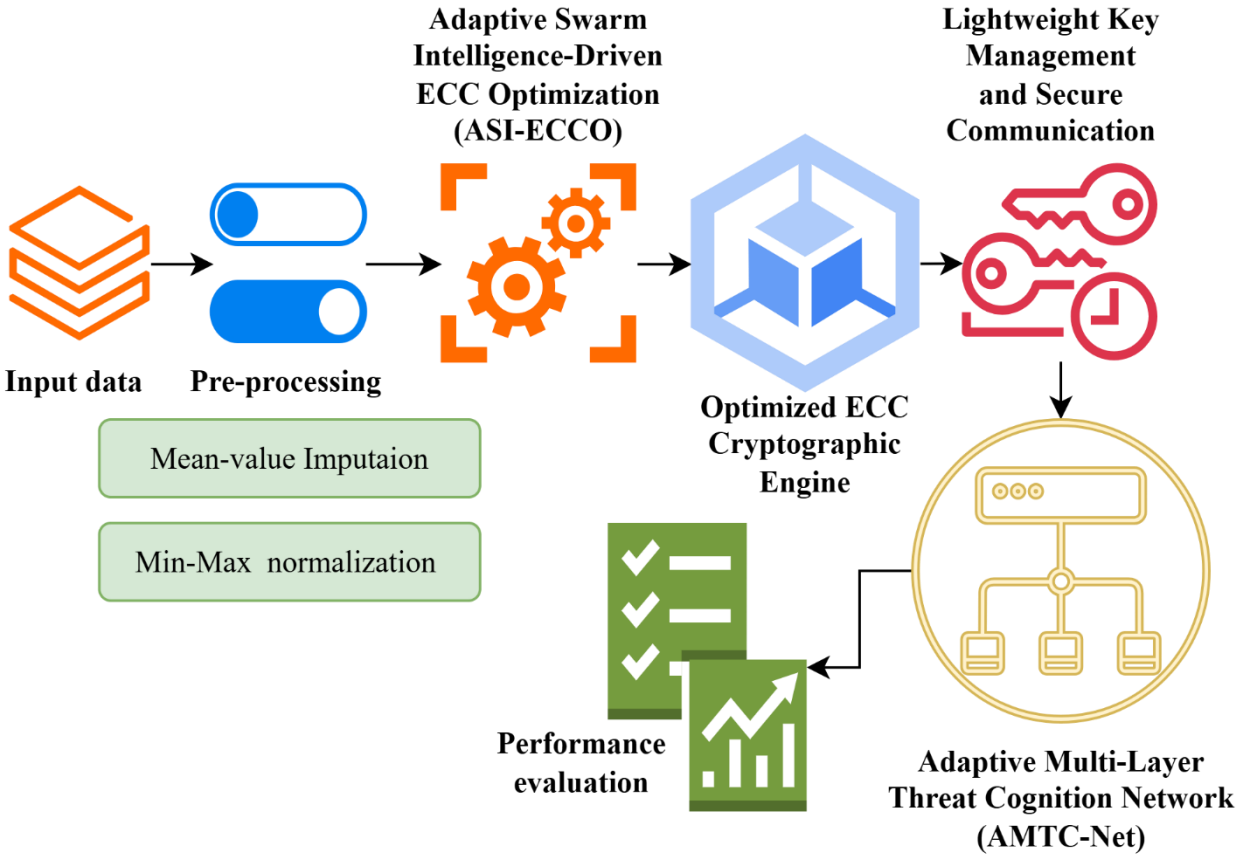

Figure 1: Overall architecture of the study

3.1 Data collection

Evaluation of the proposed FA-ECC model is performed based on Smart Agriculture and Food Security Dataset that has been collected from Kaggle. This dataset involves agriculture and environmental data to support applications of smart farming and food security. This dataset consists of several parameters related to crop production, soil, climate, water availability, fertilizer usage, and agricultural practices that provide an effective description of agriculture scenarios in the real world. The dataset includes such environmental parameters as temperature, rainfall, humidity,

soil moisture, soil pH level, irrigation condition, crop, and fertilizer usage that are commonly communicated between IoT devices and cloud servers in agriculture. Before conducting the experiments, the dataset goes through the preprocessing stage to enhance its data quality and prepare the basis for further cryptography assessment. This stage includes removal of duplicates and missing values, as well as data cleaning. In addition, numerical parameters are normalized using the Min-Max approach to keep the same scale of features. The resulting data are encrypted using the proposed FA-ECC framework in order to assess secure communication efficiency, computational costs, communication precision, transparency, and vulnerability to cyber-attacks. Thus, the data source can be given as below, https://www.kaggle.com/datasets/aatmaca/smart-agriculture-and-food-security-dataset.

Assume that the agricultural IoT network consists of N sensor nodes and it can be given as eqn. (1),

$$S = \{s_1, s_2, s_3, \dots, s_N\} \quad (1)$$

Where, S is the set of IoT sensor nodes, s_i representing the i^{th}agricultural sensor and N is the total number of deployed sensors. Each sensor generates multidimensional observations represented as eqn. (2),

$$X = \{x_1, x_2, \dots, x_M\} \quad (2)$$

Where, X is the sensor feature vector, M representing the number of sensing attributes and x_j is the j^{th}sensor measurement

3.2 Pre-processing

This architecture leverages the Smart Agriculture and Food Security dataset to model the communication environment of agricultural IoT networks. This dataset consists of many features of agriculture, including temperature, humidity, precipitation, moisture in soil, soil pH value, irrigation status, details about crops, use of fertilizers, and various other environmental factors. This data is information gathered by distributed IoT sensor nodes during precision agriculture practices. First, any redundant and/or incomplete data points are filtered out. For missing values in the data, a mean-value approach is used for replacement and it can be given as eqn. (3),

$$x_{ij} = \begin{cases} x_{ij}, & \text{if available} \\ \mu_j, & \text{otherwise} \end{cases} \quad (3)$$

Where, x_{ij} is the value of feature $j$in sample i and μ_j is the mean value of feature j. The mean is calculated as eqn. (4),

$$\mu_j = \frac{1}{N}\sum_{i=1}^{N} x_{ij} \quad (4)$$

To eliminate differences in feature magnitude, Min-Max normalization is performed and it can be given as eqn. (5),

$$x_i' = \frac{x_i - x_{min}}{x_{max} - x_{min}} \quad (5)$$

Where, x_i' is the normalized feature, x_{min} defines the minimum feature value and x_{max} is the maximum feature value. The normalized sensor observations are then forwarded to the proposed ASI-ECCO optimization module.

3.3 Adaptive Swarm Intelligence-Driven ECC Optimization (ASI-ECCO)

The most important innovation of ASI-ECCO lies in the suggested Adaptive Security-Resource Coupling (ASRC), which allows altering the order of optimization prioritization depending on the current level of security risk and residual energy of IoT sensor nodes used in agriculture. In contrast to the classical ECC optimization methods, which imply setting up static objective weights in the optimization process, ASRC implies a direct connection between the current status of the IoT node and the selection of the ECC parameters. The normalized value of the security risk (R^t) raises the significance of the security strength parameter if the communication environment becomes less safe, while the residual energy status (\rho^t) is responsible for the dynamic alteration of the significance of the energy consumption, computational, and communication overhead parameters. The optimization procedure does not pursue the goal of finding out the universal ECC configuration; rather, it finds out a context-specific cryptographic configuration that is appropriate for the current status of the IoT node. Thus, ASRC prefers lighter ECC configurations for energy-constrained nodes, while in case of increased security risk it alters the optimization direction in favor of stronger cryptographic configurations regardless of their increased resource demands.In each iteration of the optimization process the position of the i^{th} swarm agent is given by eqn. (6),

$$P_i^t = [p_1, p_2, \dots, p_D] \qquad (6),$$

Whereas P_i^t is the position vector, which describes the current solution point of the i^{th} swarm particle at iteration t, D on the other hand is the number of all optimization variables for adaptive ECC parameter optimization. The adaptive position update is defined as eqn. (7),

$$P_i^{t+1} = P_i^t + \alpha(B - P_i^t) + \beta(R - P_i^t) \qquad (7)$$

Parameter B corresponds to the global optimal solution that is discovered during the optimization process, R corresponds to the neighbor solution from where the local search is conducted, α corresponds to the learning rate which governs the convergence towards the global optimal solution, and β corresponds to the adaptive exploration rate.

The optimization dynamically changes the importance of security, computation, energy, and communication overhead according to the current attack-risk level and residual energy state of the sensor node. Thus, when a node is under high security risk, ASI-ECCO automatically prioritizes stronger ECC configurations; when the node has low residual energy, it shifts toward computationally and energetically lightweight configurations. This is substantially more meaningful than simply saying "adaptive weights and it can be given in eqn. (8),

$$F_i^t = w_S^t S_i^t + w_C^t C_i^t + w_E^t E_i^t + w_O^t O_i^t \qquad (8)$$

where F_i^trepresents the fitness of the i^{th}ECC configuration at iteration t, while S_i^t, C_i^t, E_i^t, and O_i^trepresent security strength, computational efficiency, energy efficiency, and communication efficiency/overhead, respectively. The novelty is introduced by dynamically determining the weights according to the security and resource state as given in eqns. (9)-(),

$$w_S^t = \frac{1+\lambda R^t}{Z^t} \qquad (9)$$

$$w_E^t = \frac{1+\lambda(1-R^t)(1-\rho^t)}{Z^t} \qquad (10)$$

$$w_C^t = \frac{1+\lambda(1-R^t)\rho^t}{Z^t} \qquad (11)$$

$$w_O^t = \frac{1+\lambda(1-\rho^t)}{Z^t} \qquad (12)$$

Where, Z^t can be expressed as eqn. (13),

$$Z^t = [1 + \lambda R^t] + [1 + \lambda(1 - R^t)(1 - \rho^t)] + [1 + \lambda(1 - R^t)\rho^t] + [1 + \lambda(1 - \rho^t)] \qquad (13)$$

Here, $R^t \in [0,1]$ denotes the normalized communication security-risk level, $\rho^t \in [0,1]$ denotes the normalized residual-energy level, and $\lambda$is the adaptive coupling coefficient controlling the influence of the current node state on optimization. Z^t normalizes the dynamically generated weights such that eqn. (14),

$$w_S^t + w_C^t + w_E^t + w_O^t = 1 \qquad (14)$$

The key contribution is not merely adaptive weights. It is the security–resource coupling rule:

- High $R^t \rightarrow$ security weight w_S^tincreases automatically.
- Low residual energy $\rho^t \rightarrow$ energy efficiency becomes more important.
- Higher available energy → the optimizer can afford configurations with greater computational protection.
- The optimizer therefore selects ECC parameters according to the current operating condition of the agricultural IoT node, rather than using one fixed objective throughout the network lifetime.

The main novel element of ASI-ECCO lies in the suggested Adaptive Security–Resource Coupling (ASRC) approach, where the weights of the optimization goals dynamically change based on the immediate security risk and the residual energy of the agricultural IoT sensors. While the standard ECC optimization methods use fixed objective weights during the entire optimization process, ASRC provides a direct connection between the current status of the IoT device and the ECC parameter selection. In the case of high normalized security risk R^t, the importance of security is increased since the communication becomes more vulnerable, while the residual energy ρ^t adjusts the significance of energy consumption, computation, and communication. Therefore, ASI-ECCO does not attempt to optimize

towards some universal ECC parameters but finds a node-specific cryptography configuration at each point in time. Nodes with low residual energy will be recommended lightweight ECC configurations to minimize their computational and communication overhead, whereas nodes with higher security risk will be encouraged towards more secure ECC configurations even though they require higher resource usage.

3.4 Optimized ECC Cryptographic Engine

These optimized parameters are utilized for Elliptic Curve Cryptography. ECC offers confidentiality, authentication, key exchange, and signatures using keys that are much shorter than those used in traditional public key cryptography. The elliptic curve equation is given as eqn. (15),

$$y^2 = x^3 + ax + b(modp) \quad (15)$$

Eqn. (15) is subject to eqn. (16),

$$4a^3 + 27b^2 \neq 0 \quad (16)$$

Where, a, b is the elliptic curve coefficients, p defines the prime finite field and (x, y) is the point on the curve. The private key is given as eqn. (17),

$$d \in [1, n-1] \quad (17)$$

The corresponding public key is given as eqn. (18),

$$Q = dG \quad (18)$$

Where, d is the private key, G representing the generator point, Q is the public key and n is the order of the generator point. For secure communication, the ciphertext is generated as eqn. (19),

$$C = (kG, M + kQ) \quad (19)$$

Where, k is the random session key, M defines the plaintext message and Q is the receiver public key. The optimized ECC engine enables secure encryption with reduced computational complexity.

3.5 Lightweight Key Management and Secure Communication

After the encryption process, the proposed architecture uses key management that requires minimal communications latency and energy costs. Session keys are created for each session of communication, thus eliminating key reuse and providing forward secrecy. The encrypted data is then communicated through the wireless communication channel with guarantees of security, integrity, and authentication. Communication efficiency is given by eqn. (20),

$$CE = \frac{P_s}{P_t} \times 100 \quad (20)$$

Where, CE is the communication efficiency (%), P_s representing the successfully transmitted packets and P_t is the total transmitted packets. Energy consumption is estimated as eqn. (21),

$$E = \sum_{i=1}^{N} (E_t + E_r) \quad (21)$$

Where, E_t is the transmission energy and E_r is the reception energy. The light key management scheme greatly reduces the computational overhead and increases the lifespan of agricultural IoT sensor nodes.

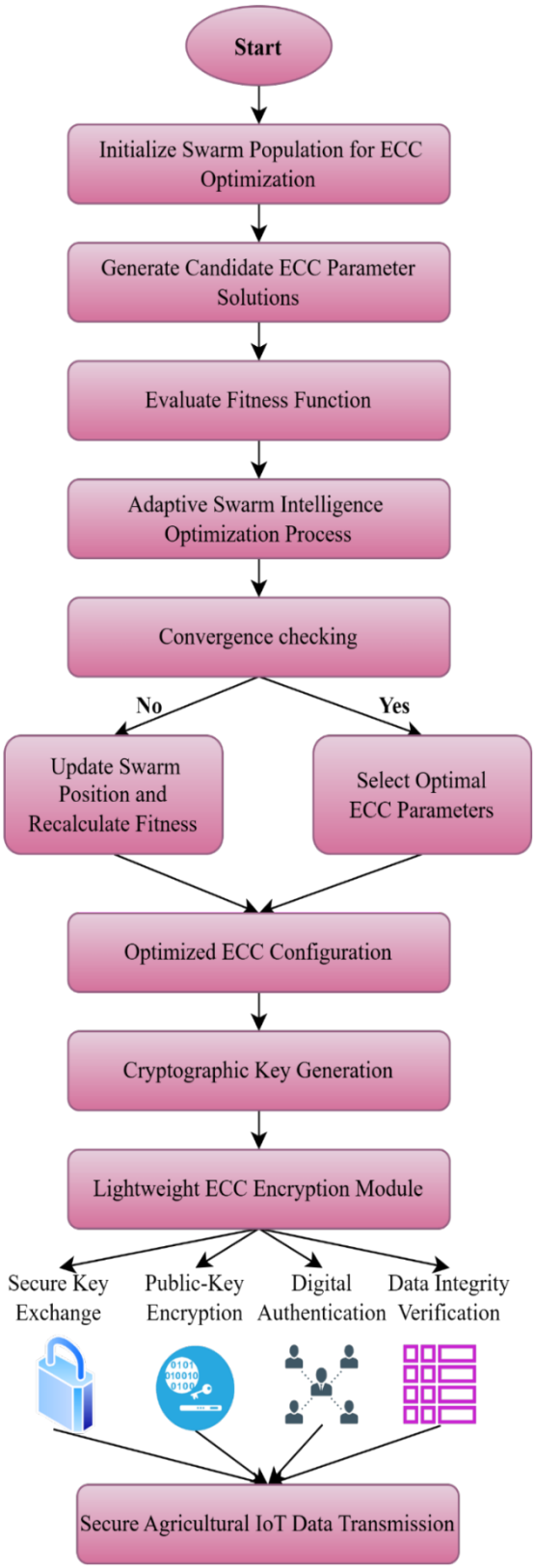

Figure 2: ASI-ECCO Process workflow

The ASI-ECCO module consists of the initialization of agricultural IoT sensor data, followed by preprocessing and normalization. The optimization procedure produces numerous candidate ECC configurations in which each swarm agent corresponds to a potential cryptographic parameter solution. The fitness of each candidate solution is measured according to multiple criteria, which include security level, computation efficiency, energy usage, and communication overhead. By using the results of the fitness evaluation, the adaptive swarm intelligence mechanism changes the positions of the agents, thus ensuring an optimal balance between exploration and exploitation. The iterative optimization continues until the convergence criterion is reached, producing the optima1 elliptic curve parameters and cryptographic configuration. The obtained set of ECC parameters is used for key generation, encryption, authentication, and integrity checking. At last, the optimized cryptographic module allows for lightweight and secure communication between agricultural IoT sensors, gateways, and cloud servers at reduced computational and communication expenses. Figure 2 shows the ASI-ECCO Process workflow.

3.6 Adaptive Multi-Layer Threat Cognition Network (AMTC-Net)

In order to improve the security of communications in the agricultural IoT environment, an Adaptive Multi-Layer Threat Cognition Network (AMTC-Net) is suggested in this research. In contrast to traditional threat identification systems that recognize attacks after transmitting data, the suggested AMTC-Net constantly assesses the security condition of each communication process prior to encryption, during transmission, and upon receiving data. This assessment is carried out by using the adaptive threat cognition, dynamic trust evaluation, cryptographic authentication, and analysis of communication behavior, while at the same time reducing the computational overhead. In accordance with the assessed threat level, the AMTC-Net dynamically changes the cryptographic security level and secure key management processes. Thus, AMTC-Net increases the security from any unauthorized access, replay attack, man-in-the-middle attack, eavesdropping, and malicious manipulation of data while retaining light-weight communication. The overall threat cognition score is defined as eqn. (22),

$$TC = \lambda_1 T_d + \lambda_2 B_a + \lambda_3 C_v + \lambda_4 K_s \qquad (22)$$

Where, TC is the threat Cognition Score, T_d defines the threat detection confidence, B_a is the communication behavior analysis score, C_v defines the cryptographic verification score, K_s representing the Key security strength and λ_i is the adaptive weighting coefficients. Thus, the following eqn. (22) is subject to eqn. (23),

$$\sum_{i=1}^{4} \lambda_i = 1 \qquad (23)$$

The communication trust level is computed as eqn. (24),

$$TL = \frac{S_c}{S_t} \qquad (24)$$

Where, TL is the communication trust level, S_c is the secure communication sessions and S_t is the total communication sessions. The adaptive security reinforcement factor is calculated as eqn. (25),

$$SR = \delta \times TC \times TL \qquad (25)$$

Where, SR is the Security reinforcement factor and δ is the adaptive security coefficient. Finally, the overall secure communication index is given as eqn. (26)-(27),

$$SR = \delta \times TC \times TL \qquad (26)$$

$$SCI = \frac{SR+\gamma}{1+\omega} \qquad (27)$$

Where, SCI is the secure Communication Index, SR defines the security reinforcement factor, γ is the encryption robustness coefficient and ω is the communication overhead factor. The higher the value of the SCI, the better the level of communication security without involving much computational effort. In each communication process, the AMTC-Net system calculates the threat cognition score and enhances the encryption protocol whenever there is an anomaly found. The proposed ASI-ECCO model is capable of offering intelligent and efficient security in the upcoming agricultural IoT systems.

After computing the Threat Cognition Score, the communication session is classified according to eqn. (28),

$$C_{th} = \begin{cases} \text{Normal}, & TC < \tau_1 \\ \text{Suspicious}, & \tau_1 \le TC < \tau_2 \\ \text{Malicious}, & TC \ge \tau_2 \end{cases} \qquad (28)$$

Where, C_{th} is the final threat classification label, TC is the threat Cognition Score, τ_1 is the lower decision threshold and τ_2 defines the upper decision threshold ($\tau_2 > \tau_1$). To make the classification adaptive to changing network conditions, the thresholds are updated dynamically as eqn. (29),

$$\tau_i = \tau_i^0 + \rho(1 - TL), i \in \{1,2\} \qquad (29)$$

Where, τ_i^0 is the initial threshold value, TL representing the communication trust level, ρ is the adaptive threshold adjustment coefficient. Finally, the overall threat confidence of the communication session is computed as eqn. (30),

$$T_{conf} = TC \times TL \times SCI \qquad (30)$$

Where, T_{conf} is the final threat confidence score, TC is the threat Cognition Score, TL defines the communication trust level and SCI is the secure Communication Index. An increased T_{conf} value indicates a higher likelihood that the communication is malicious. The final classification produced by the suggested AMTC-Net is used to identify whether the encrypted communication should be accepted, verified further, or blocked, thus offering adaptive and light-weight threat protection for agricultural IoT networks.

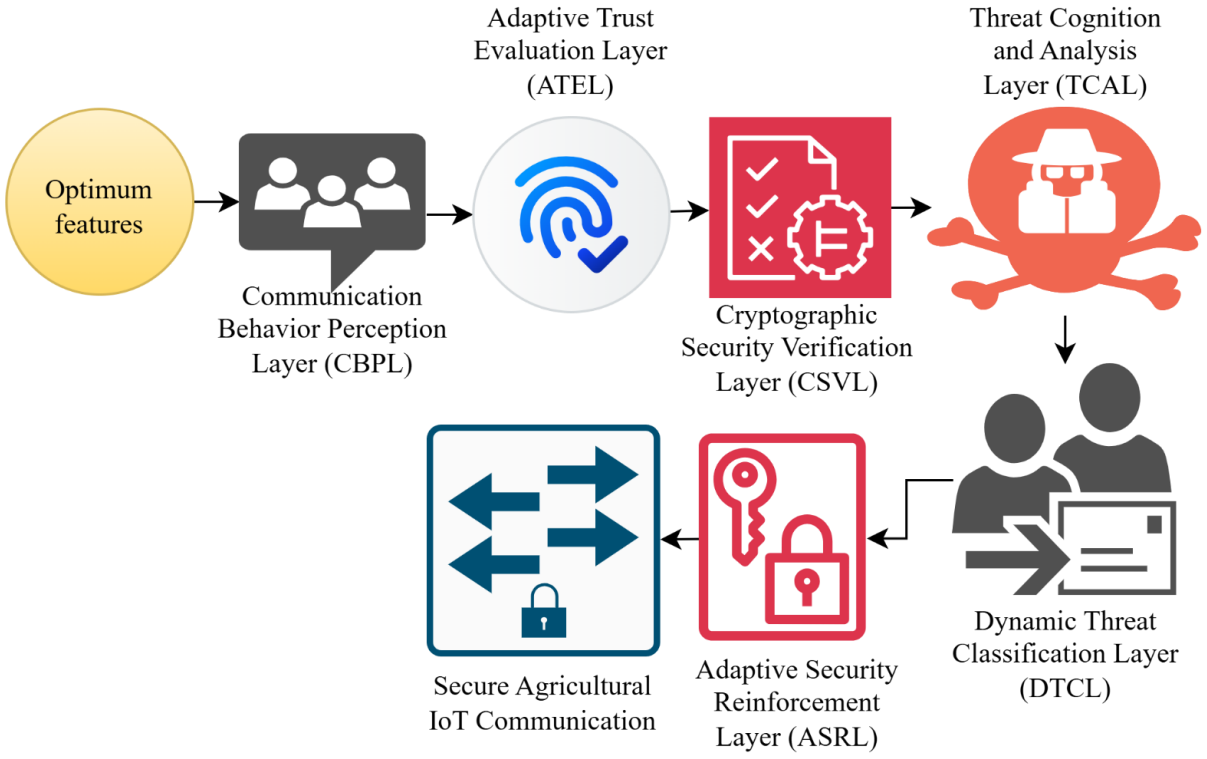

Figure 3: Adaptive Multi-Layer Threat Cognition Network (AMTC-Net) Architecture

The architecture of the proposed Adaptive Multi-layer Threat Cognition Network (AMTC-Net) is shown in Figure 3. The proposed AMTC-Net system works using various security layers that continuously monitor the communication behavior, measure the reliability of communicating devices, verify cryptography and authentication operations, and classify cyber threats. First, the Communication Behavior Perception Layer (CBPL) captures communication behavior features like packet transmission, communication frequency, and abnormal traffic patterns at the network level from the agricultural IoT sensors. This captured behavior feature data is then fed into the Adaptive Trust Evaluation Layer (ATEL) to calculate the trust value of the communicating devices using the historical records and communication condition. Later, the Cryptographic Security Verification Layer (CSVL) checks the cryptography, authentication parameter, key synchronization, and data integrity. The Threat Cognition and Analysis Layer (TCAL) then analyzes the security related features and measures the deviation from the normal behavior pattern. These identified events are further filtered through the Dynamic Threat Classification Layer (DTCL), which divides the communications into categories of either normal, suspicious, or malicious activity. Lastly, the Adaptive Security

Reinforcement Layer (ASRL) enables dynamic reinforcement of security policies through improving the cryptographic measures and adjusting the key management process according to the level of threat detection. This three-layered approach enables AMTC-Net to provide constant threat awareness, adaptive protection, and efficient security management in smart agricultural IoT environments.

4. Result and discussion

In this section, the results of the proposed Adaptive Swarm Intelligence-Driven Elliptic Curve Cryptography Optimization (ASI-ECCO) approach for providing security to agricultural IoT communications are discussed. Evaluation of the proposed Adaptive Security–Resource Coupling (ASRC) mechanism for dynamic adjustment of security strength, computation cost, energy usage, and communication overhead are considered here. The performance of the ASI-ECCO approach has been evaluated in terms of security and network performance metrics such as encryption/decryption time, energy usage, communication cost, computational cost, packet delivery performance, and security strength. In addition, comparative experimentation with existing ECC and optimization approaches is conducted to highlight the benefits of the proposed approach.

4.1 Dataset description

The proposed ASI-ECCO approach will be validated based on the Smart Agriculture & Food Security Dataset. The dataset is available at Kaggle and is created to depict various scenarios related to agriculture and food security. The dataset consists of structured agricultural observations which can be considered to be the information created or communicated by smart agriculture and IoT-based monitoring systems. The attributes represent important factors of agriculture associated with crop production, environmental conditions, resource usage, and food security-related features. The variables are appropriate to simulate agricultural IoT data transmission and to evaluate the lightweight security mechanisms. Each observation corresponds to one agricultural observation while each attribute stands for a measurable/categorical feature of the farming environment. In this research work, the dataset is first reviewed for possible missing observations, duplicate observations, inconsistencies in entries, and differences in data types. The numerical attributes are normalized prior to being submitted to the ASI-ECCO module so that the different scales of parameters would not affect the optimization process. Then, the observations will be used to test secure communication efficiency, cryptographic costs, communication accuracy, communication transparency, energy efficiency, and threats protection.

4.2 Experimental setup

This experiment was intended to examine the new ASI-ECCO and AMTC-Net architecture within a controlled agricultural IoT communication environment. The experimental system consists of data preprocessing, swarm based ECC optimization, cryptography, threat categorization and performance analysis. The key experimental parameters are summarized in Table 1.

Table 1: Experimental Configuration of the Proposed ASI-ECCO with AMTC-Net Framework

Parameter	Experimental Configuration
Dataset	Smart Agriculture and Food Security Dataset
Proposed optimization	ASI-ECCO
Cryptographic technique	Elliptic Curve Cryptography (ECC)
Threat protection	AMTC-Net
Threat classes	Normal, Suspicious, Malicious
Security services	Encryption, authentication, key exchange, integrity verification
Evaluation metrics	Cryptographic overhead, communication accuracy, communication transparency
Security attacks	Unauthorized access, replay, MITM, eavesdropping, data tampering

Communication environment	Agricultural IoT sensor–gateway–cloud architecture

4.3 Metrics analysis

Table 3 shows six performance parameters used to measure the proposed ASI-ECCO with AMTC-Net system. Cryptographic overhead and energy consumption measure lightweight efficiency, and communication accuracy and transparency indicate communication reliability. The Threat Detection Rate parameter checks for the system's capability to detect attacks, while False Positive Rate indicates the probability of false threats detection.

Table 3: Analysis on performance metrics

Metric	Description	Formula
Cryptographic Overhead (CO)	Measures the computational burden introduced by encryption, decryption, and key generation. Lower values indicate lightweight cryptographic processing.	$CO = \frac{T_{enc} + T_{dec} + T_{key}}{T_{total}} \times 100$
Communication Accuracy (CA)	Measures the percentage of agricultural IoT data packets transmitted and received correctly. Higher values indicate reliable communication.	$CA = \frac{N_c}{N_t} \times 100$
Communication Transparency (CT)	Measures the percentage of communication sessions successfully verified and completed without security interruption.	$CT = \frac{N_s}{N_t} \times 100$
Energy Consumption (EC)	Measures the total energy consumed by IoT devices during secure data transmission and reception. Lower values indicate better energy efficiency.	$EC = \sum_{i=1}^{N} (E_{tx,i} + E_{rx,i})$
Threat Detection Rate (TDR)	Measures the percentage of actual cyber threats correctly detected by AMTC-Net. Higher values indicate stronger threat identification.	$TDR = \frac{TP}{TP + FN} \times 100$
False Positive Rate (FPR)	Measures the percentage of legitimate communication events incorrectly identified as threats. Lower values indicate more reliable threat classification.	$FPR = \frac{FP}{FP + TN} \times 100$

4.4 Comparison analysis

The baseline models in Table 4 were chosen to have a progressive and technically meaningful comparison with the proposed ASI-ECCO + AMTC-Net framework. The choice of AES as a standard symmetric encryption algorithm is chosen to serve as a reference for testing the overhead, energy consumption and communication efficiency of cryptographic methods. The proposed framework is also based on elliptic curve cryptography, and the benefits of adaptive optimization can be evaluated separately, hence ECC is included as a direct public-key cryptographic baseline. ECC-PSO is chosen to represent the swarm-intelligence-based ECC optimization, so that the proposed adaptive swarm strategy can be compared with the conventional particle-based optimization strategy. The ECC-COA is an optimization method inspired by the natural process that yields an alternative approach to selecting the parameters of ECC and comparison with another metaheuristic optimization mechanism. Conventional cryptographic schemes are basic models as compared with ECC-QNN+BO, which is an intelligent optimization-based security approach that is more advanced than the conventional cryptographic schemes, and incorporates learning based modeling with Bayesian optimization. These five methods in total include traditional symmetric encryption, general ECC, and optimization of ECC using metaheuristic algorithms, nature-inspired optimization, and intelligent security based on optimization. Hence, the baselines selected for this study present higher and higher levels of complexity both with

respect to the cryptographic and the optimization aspects, and the proposed ASI-ECCO + AMTC-Net can be fairly assessed in terms of security, communication reliability, energy efficiency, and threat detection capability.

Table 4: Comparative Performance Analysis with Existing Baseline Models

Model / Method	Cryptographic Overhead (%)	Communication Accuracy (%)	Communication Transparency (%)	Energy Consumption (J)	Threat Detection Rate (%)	False Positive Rate (%)
AES [21]	31.84	91.72	90.85	8.74	88.63	7.42
ECC [22]	29.67	92.86	91.94	8.12	90.21	6.85
ECC-PSO [23]	27.52	93.74	93.16	7.58	91.86	5.93
ECC-COA [24]	26.84	94.18	93.72	7.31	92.47	5.41
ECC-QNN+BO [25]	26.13	94.67	94.36	7.05	93.18	4.87
Proposed ASI-ECCO + AMTC-Net	18.42	95.6	95.8	5.86	96.34	3.21

The comparative performance of the proposed ASI-ECCO + AMTC-Net algorithm with AES, ECC, ECC-PSO, ECC-COA, and ECC-QNN+BO algorithms is presented in terms of six important performance indicators in Table 4. The outcomes show an on-going enhancement in security and resource-efficiency metrics. Cryptographic overhead for AES is 31.84%, whereas for conventional ECC is 29.67%, showing that conventional cryptographic mechanisms have relatively higher processing overhead. The overhead for ECC-PSO and ECC-COA are 27.52% and 26.84% respectively, which shows that the optimization process could make cryptographic processes more efficient. To further lower the overhead, ECC-QNN+BO is used, which further reduces the overhead to 26.13%. The proposed ASI-ECCO + AMTC-Net, however, obtains the lowest number of 18.42% which is a significant decrease from all baseline approaches. The improvement is mainly brought about by the adaptive optimization of ECC parameters and minimal security management. In the aspect of communication accuracy, AES is 91.72%, and ECC is 92.86%. The optimized approaches gradually increase the accuracy from 93.74% up to 94.67% for ECC-QNN+BO, 94.18% for ECC-COA, and 93.74% for ECC-PSO. The proposed framework achieved the best accuracy of 95.60%, which shows more secure data transmission. The same trend is seen in communication transparency, with the proposed framework getting 95.80% accuracy, while AES, ECC, ECC-PSO, ECC-COA, and ECC-QNN+BO results in 90.85%, 91.94%, 93.16%, 93.72%, and 94.36% accuracy, respectively.

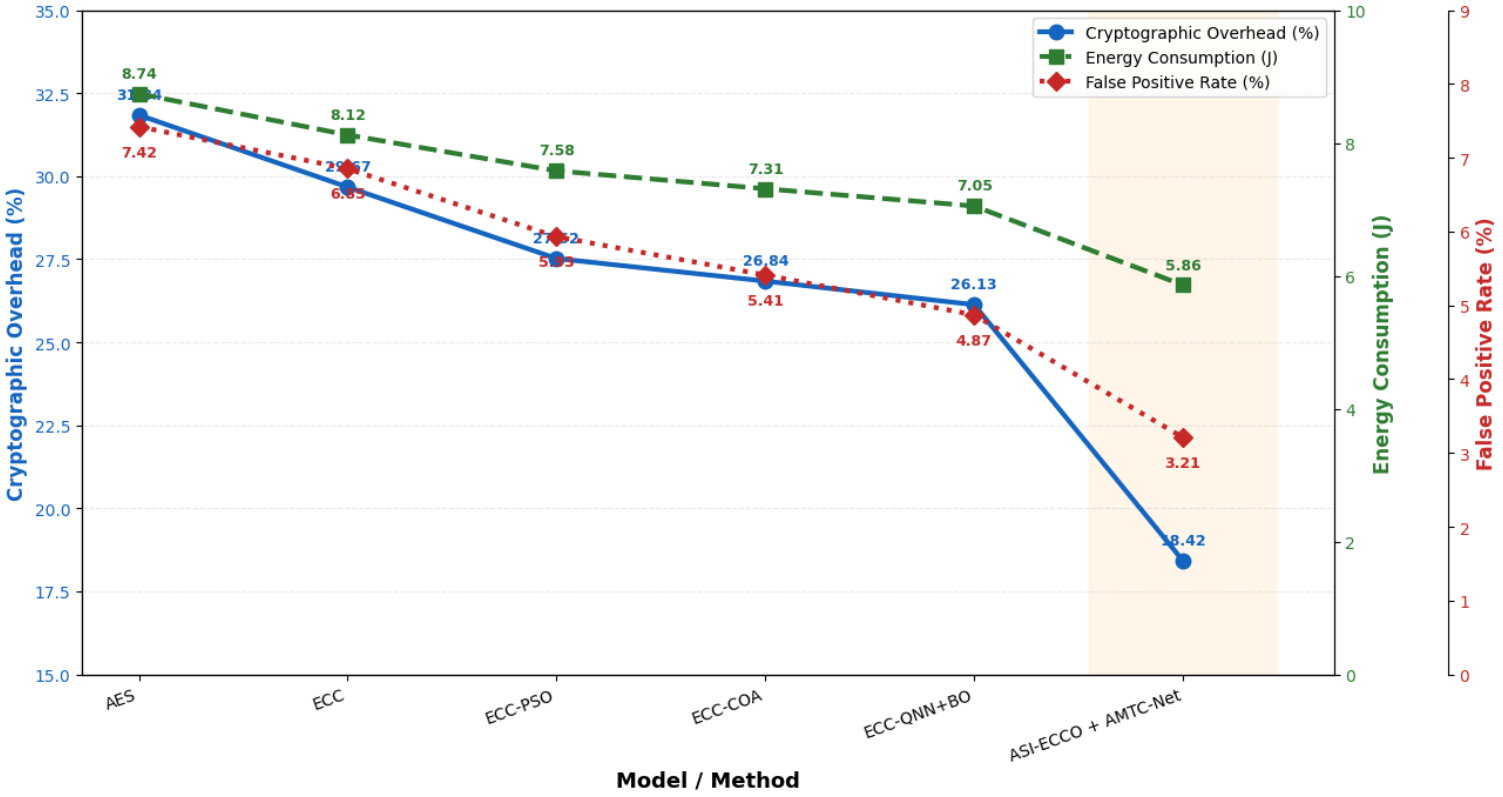

Figure 4: Comparative Analysis of Cryptographic Overhead, Energy Consumption and False Positive Rate

The proposed framework also exhibits superior energy efficiency (5.86 J) as compared to the baseline values of (7.05 J) to (8.74 J). This decrease proves that adaptive cryptographic optimization for resource constrained agricultural IoT devices is useful. Furthermore, AMTC-Net achieves the highest Threat Detection Rate of 96.34%, outperforming AES (88.63%), ECC (90.21%), ECC-PSO (91.86%), ECC-COA (92.47%), and ECC-QNN+BO (93.18%). At the same time, the proposed approach has the lowest False Positive Rate equal to 3.21%, which is less than 7.42%, 6.85%, 5.93%, 5.41% and 4.87% respectively. In general, the findings suggest that incorporating ASI-ECCO for cryptographic optimization, and AMTC-Net for adaptive threat cognition, offers a more robust trade-off between low computation, secure communication, energy efficiency, and intelligent threat protection.

A comparison of the evaluated models is shown in figure 4, where cryptographic overhead, energy cost and false positive rate are compared. The proposed ASI-ECCO + AMTC-Net achieves the lowest cryptographic overhead of 18.42%, compared with 31.84% for AES, 29.67% for ECC, 27.52% for ECC-PSO, 26.84% for ECC-COA, and 26.13% for ECC-QNN+BO. It also records the lowest energy consumption of 5.86 J, compared with 8.74, 8.12, 7.58, 7.31, and 7.05 J, respectively. The false positive rate is also minimized to 3.21%, outperforming the baseline values of 7.42%, 6.85%, 5.93%, 5.41%, and 4.87%. The findings in this study support the efficacy of the ASI-ECCO optimization and AMTC-Net threat cognition.

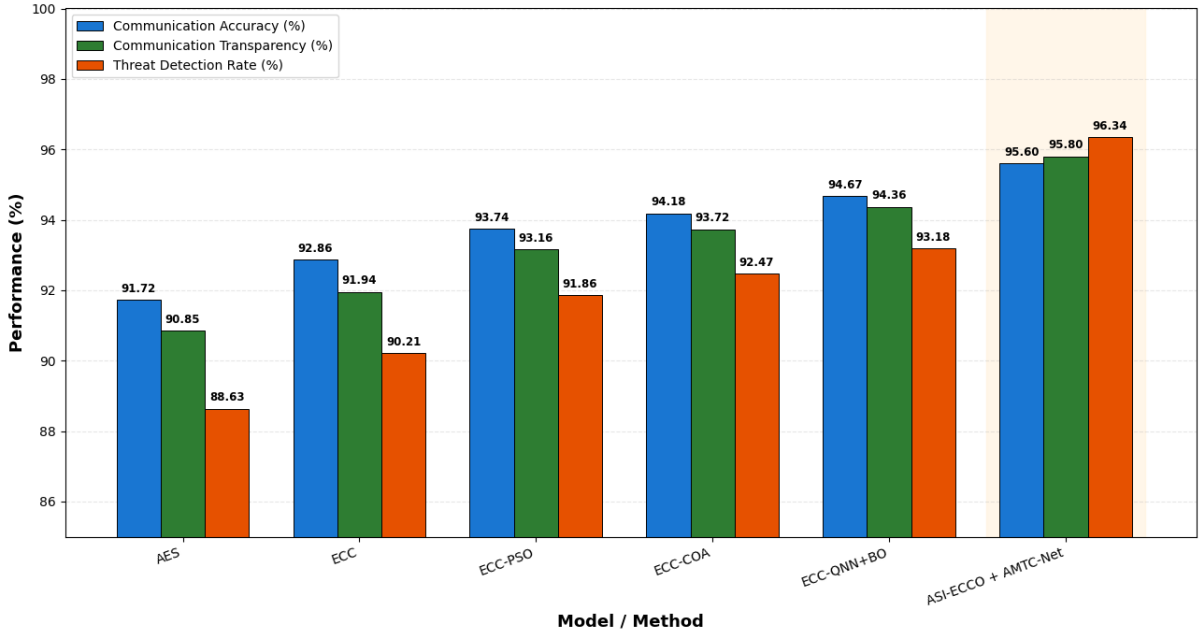

Figure 5: Comparative Analysis of Communication and Threat Detection Performance

The communication accuracy, communication transparency, and the threat detection rate of the evaluated approaches are compared in figure 5. The proposed ASI-ECCO + AMTC-Net achieves the highest communication accuracy of 95.60%, exceeding AES (91.72%), ECC (92.86%), ECC-PSO (93.74%), ECC-COA (94.18%), and ECC-QNN+BO (94.67%). Similarly, communication transparency reaches 95.80%, compared with 90.85%, 91.94%, 93.16%, 93.72%, and 94.36%, respectively. The framework further achieves a threat detection rate of 96.34%, substantially higher than AES (88.63%), ECC (90.21%), ECC-PSO (91.86%), ECC-COA (92.47%), and ECC-QNN+BO (93.18%). These enhancements show effective communication and threat recognition.

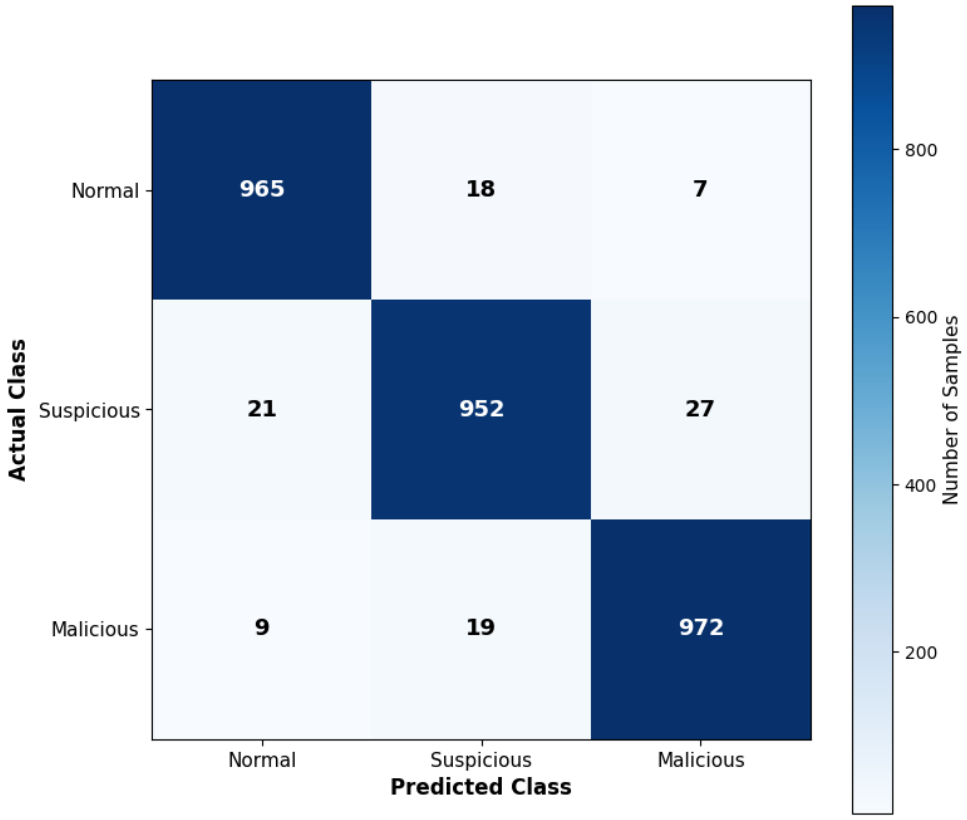

Figure 6: Confusion Matrix of AMTC-Net Threat Classification

The confusion matrix for the classification of agricultural IoT communication between normal, suspicious and malicious is shown in figure 6. For normal, suspicious and malicious traffic, the number of correctly classified instances in the matrix is 965, 952 and 972 respectively. Misclassifications values are still relatively low: 18 normal samples were misclassified as suspicious and 7 as malicious. Likewise, 21 samples are suspected as normal and 27 samples as malicious; and 9 samples are classified as malicious and 19 are classified as normal. The diagonal values are high, which indicates that AMTC-Net is able to differentiate legitimate and potentially harmful communication patterns. The relatively low value of the off-diagonal elements further confirm that threat cognition is likely to be accurate and classification errors are low, which further validates the framework's ability to monitor IoT agricultural security in real-time.

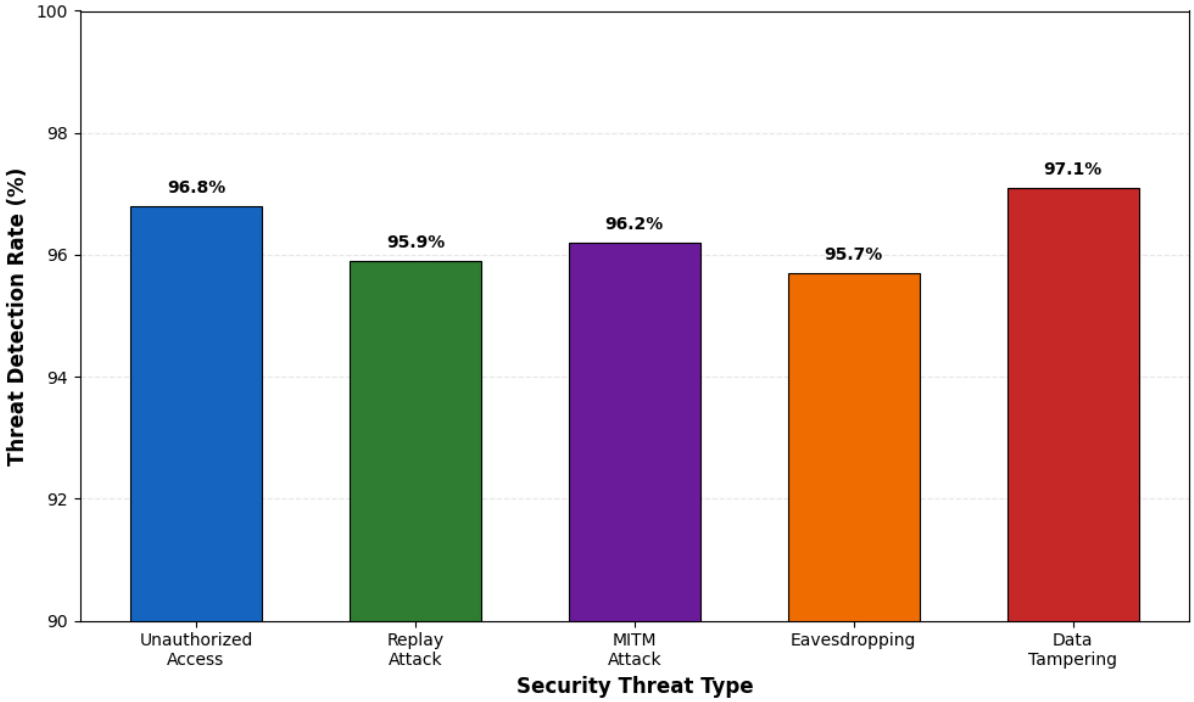

Figure 7: Threat Classification Performance by Attack Type

The threat detection capability for AMTC-Net to major agricultural IoT security threats as per attacks is given in figure 7. The framework has detection rates of 96.8% unauthorized access, 95.9% replay attacks, 96.2% MITM attacks, 95.7% eavesdropping and 97.1% data tampering. The best performance is recorded in data tampering, showing the ability of AMTC-Net to detect unusual changes in the transmitted agricultural data. Unauthorized access and MITM attacks also have detection rates of more than 96%, which is good at detecting attacks involving access and communication. Detection rates are still above 95% even in the case of replay attacks and eavesdropping. Overall, the continuously high attack-wise detection rate shows that AMTC-Net is not optimized for a particular category of attack; it offers comprehensive protection against attacks of various kinds.

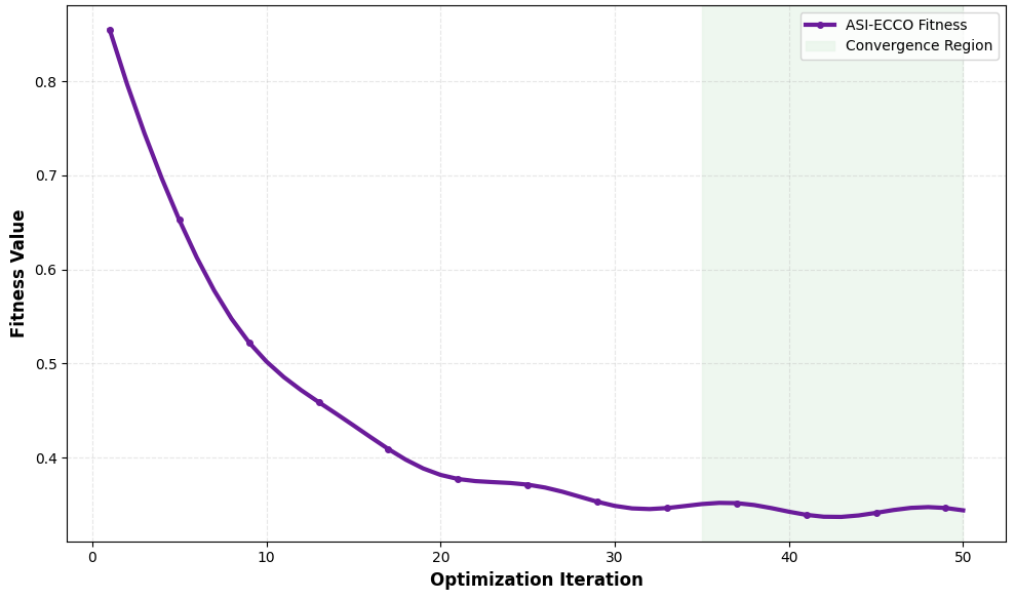

Figure 8: Convergence Analysis of ASI-ECCO Optimization

Figure 8 shows that the optimization process for the proposed ASI-ECCO is converging toward the steady state solution after 50 iterations. In the first few attempts, the fitness value drops to a low level as the adaptive swarm looks for better elliptic curve parameters and security settings. The fitness value is slowly stabilizing as optimisation proceeds, meaning that ASI-ECCO is finding an optimum solution without any unnecessary computational passes. In the convergence region, it is seen that after about 35 iterations, the results do not change much when further optimizations are made, making this small region of great stability. This behavior shows that ASI-ECCO can strike a balance between exploration and exploitation and can determine efficient configurations of ECC. The fact that the convergence is stable is significant for resource-limited agricultural IoT devices, as it could lead to higher computational and energy consumption if more optimization iterations are used.

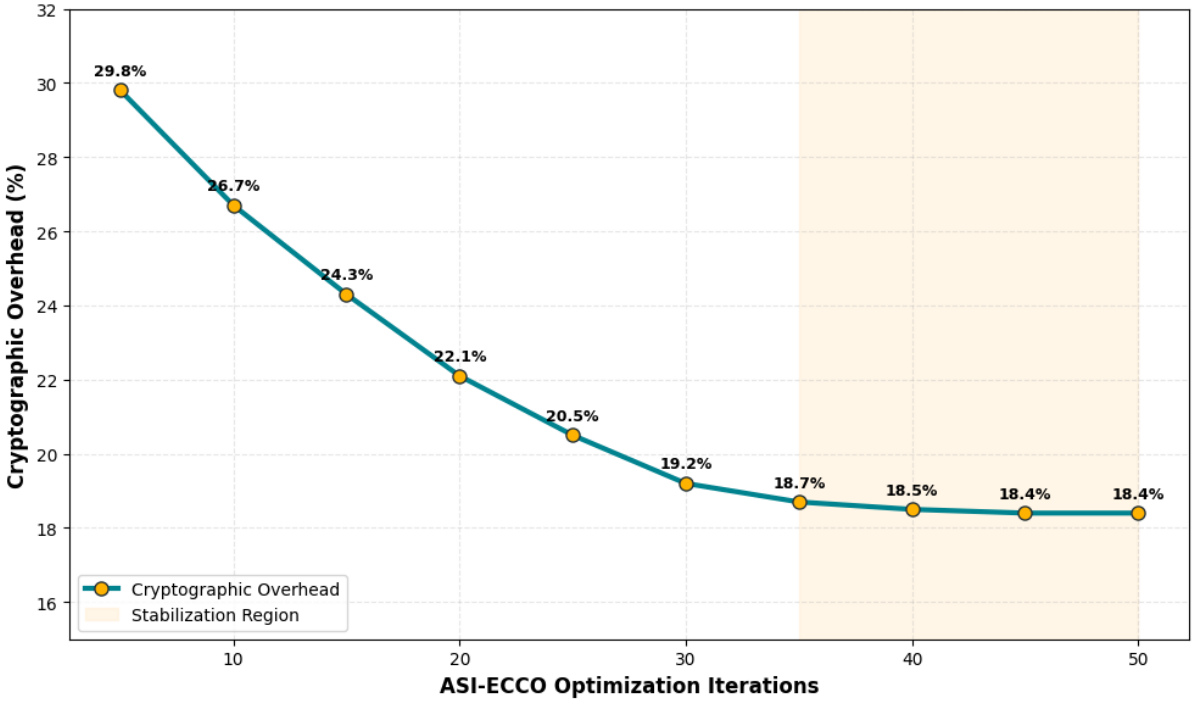

Figure 9: Impact of Iterations on Cryptographic Overhead

The effect of ASI-ECCO optimization iterations on cryptographic overhead is analyzed in figure 9. The overhead decreases progressively from approximately 29.8% at 5 iterations to 26.7% at 10, 24.3% at 15, 22.1% at 20, and 20.5% at 25 iterations. With further optimization, the overhead drops to around 19.2% at 30 iterations, 18.7% at 35 iterations, and to roughly 18.4% at 40 to 50 iterations. The result shows that as the optimization stage begins, the cryptographic efficiency is optimized continuously because of adaptive optimization of the parameters. The overhead then stabilizes after about 40 iterations, which means that the overhead is converging and further iterations are not likely to significantly improve the overhead. Thus, ASI-ECCO can provide a realistic trade-off between optimum optimization effort and efficiency of the cryptographic operations, especially for low-power agricultural IoT devices.

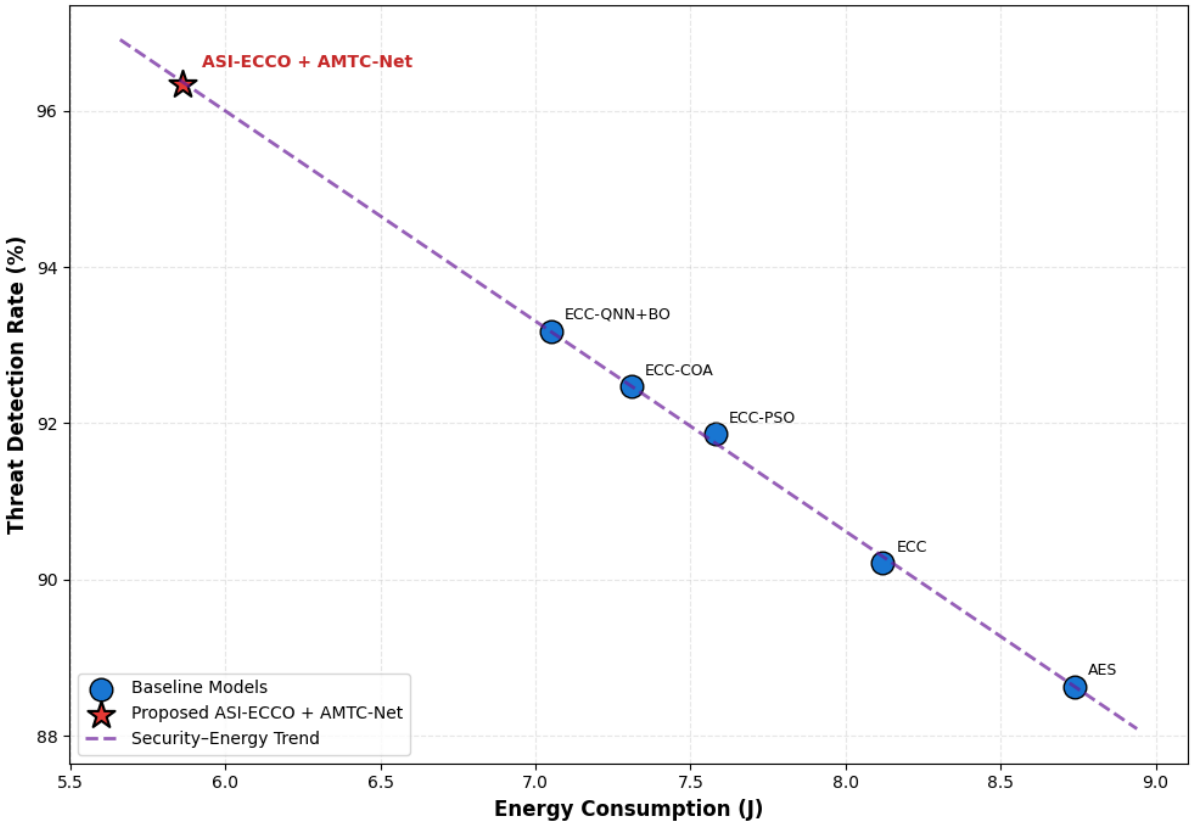

Figure 10: Security–Energy Efficiency Trade-off Analysis

Figure 10 shows the energy consumption vs threat detection rate for the models evaluated. AES consumes 8.74 J and has 88.63% threat detection rate, while ECC consumes 8.12 J and has 90.21% threat detection rate. ECC-PSO, ECC-COA, and ECC-QNN+BO progressively reduce energy consumption to 7.58, 7.31, and 7.05 J, while achieving detection rates of 91.86%, 92.47%, and 93.18%, respectively. However, the proposed ASI-ECCO + AMTC-Net has the maximum threat detection rate of 96.34% and uses only 5.86 J of energy. This favorable combination verifies that the proposed framework makes the energy requirements more secure without increasing the energy requirements. The outcome demonstrated its suitability for use in agricultural IoT applications where resources are limited and secure communication and monitoring are required all the time.

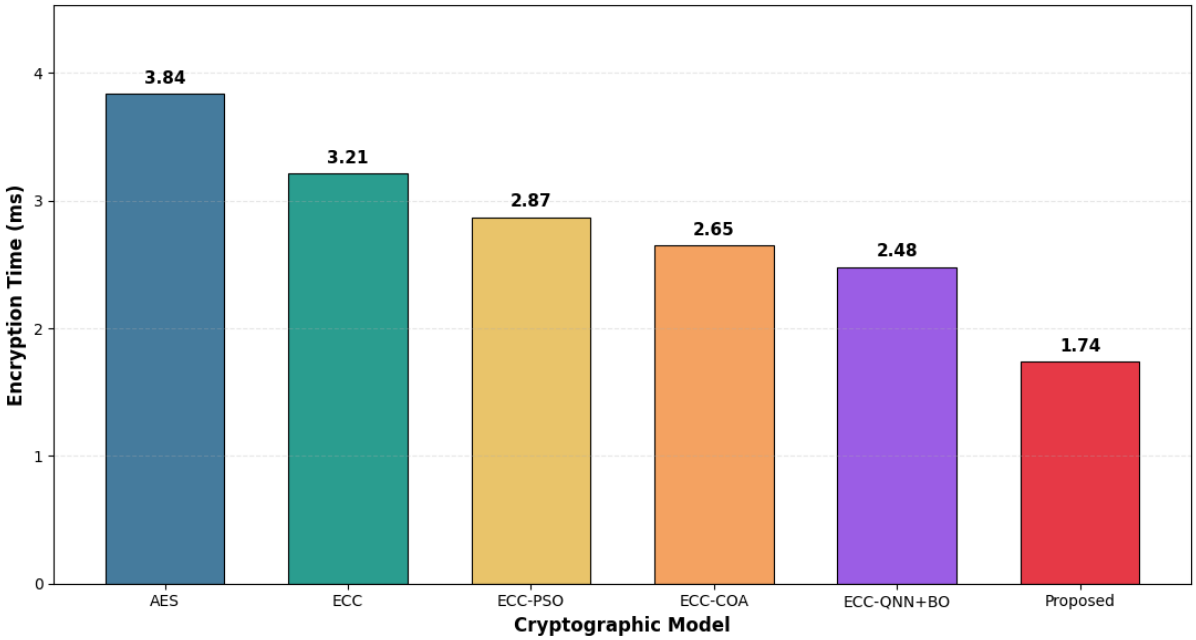

Figure 11: Comparison of Encryption Time

As it is shown in figure 11, the encryption time of the analyzed cryptographic methods is compared. AES takes 3.84 ms whereas conventional ECC records take 3.21 ms. For ECC-PSO and ECC-COA, the encryption time is 2.87ms and 2.65ms respectively, while ECC-QNN+BO achieves 2.48ms. The proposed ASI-ECCO + AMTC-Net has the lowest encryption time of 1.74 ms. The results indicate reduction in cryptographic processing requirements with adaptive ECC parameter optimization which facilitates the faster secure data transmission in resource constrained agricultural IoT devices.

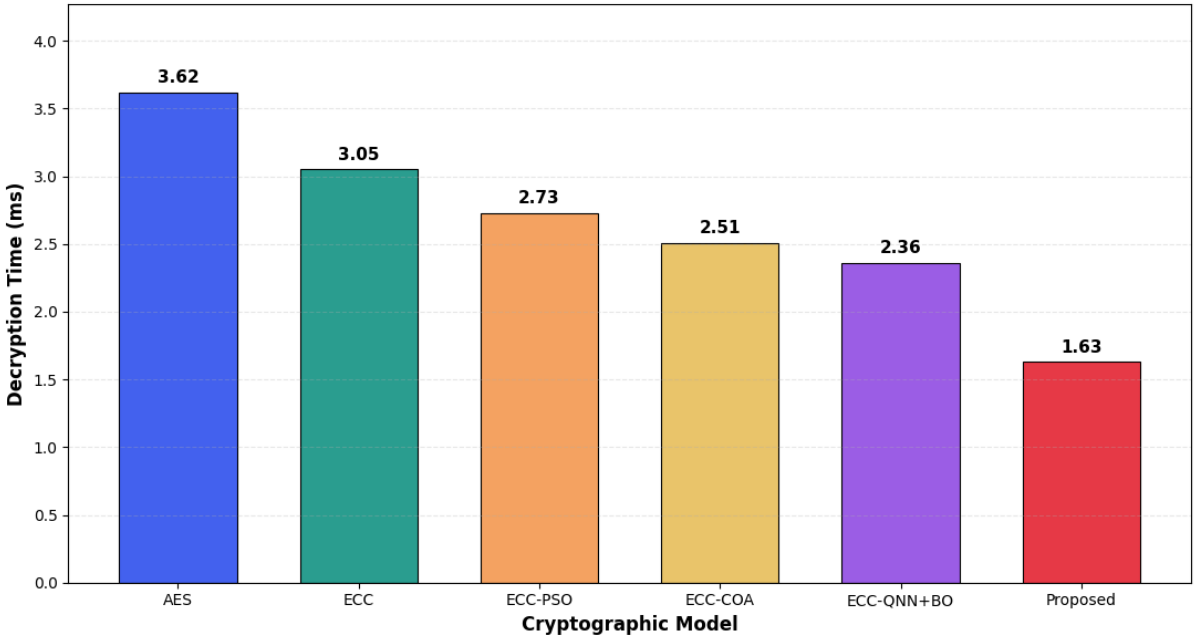

Figure 12: Comparison of Decryption Time

The comparative decryption time of the evaluated methods is shown in figure 12. AES requires 3.62 ms, followed by ECC with 3.05 ms. The optimized ECC-PSO approach and ECC-COA approach achieves the results of 2.73 ms and 2.51 ms, respectively, while ECC-QNN+BO records 2.36 ms. On the contrary, the proposed ASI-ECCO

+ AMTC-Net has the minimum decryption time of 1.63 ms. Optimised ECC configuration can dramatically decrease the burden of secure data recovery in computing. As a result, the suggested framework is designed to be both quick and lightweight, allowing it to be suitable for agricultural IoT environments.

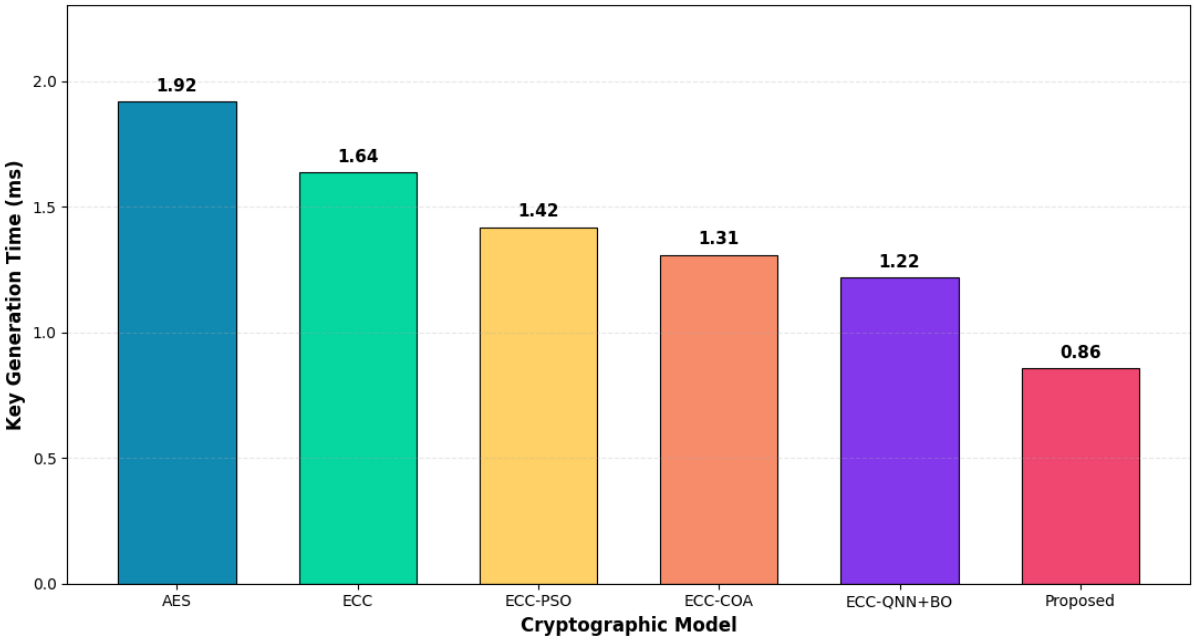

Figure 13: Comparison of Key Generation Time

The key generation time of the cryptographic methods considered is evaluated in figure 13. AES requires 1.92 ms, whereas ECC records 1.64 ms. The time is then reduced to 1.42 ms and 1.31 ms for ECC-PSO and ECC-COA, respectively. The efficiency of the key generation of ECC-QNN+BO is improved to be 1.22 ms. The proposed ASI-ECCO + AMTC-Net offers the minimal key generation time of 0.86 ms. This improvement is due to adaptive optimization of ECC parameters that minimizes unnecessary computation and optimizes the generation of secure session keys for resource-constrained sensor nodes.

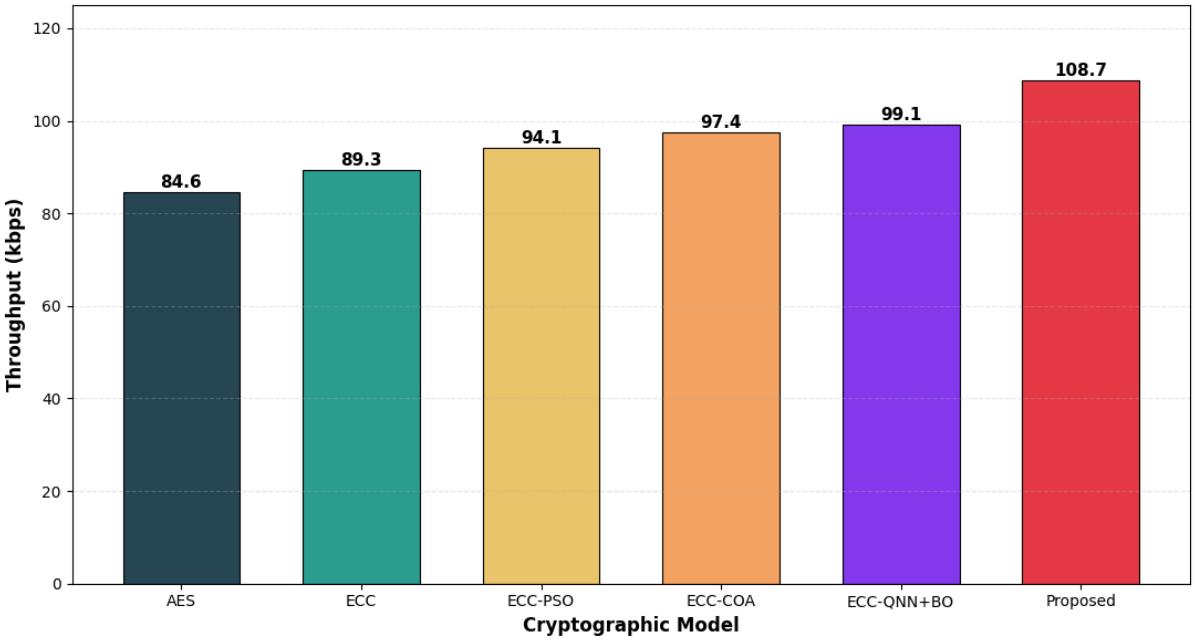

Figure 14: Communication Throughput Comparison

The communication throughput of the evaluated approaches is shown in figure 14. The throughput of AES is 84.6 kbps and of the conventional ECC is 89.3 kbps. The throughput of ECC-PSO and ECC-COA are presented to be 94.1 kbps and 97.4 kbps respectively. ECC-QNN+BO achieves 99.1 kbps. The proposed ASI-ECCO + AMTC-Net takes the highest throughput at 108.7 kbps. Optimized cryptographic processing mitigates communication delays and bottlenecks as shown in this improvement, which leads to more efficient transfer of agri-sensing data between the sensor, the gateway, and the cloud.

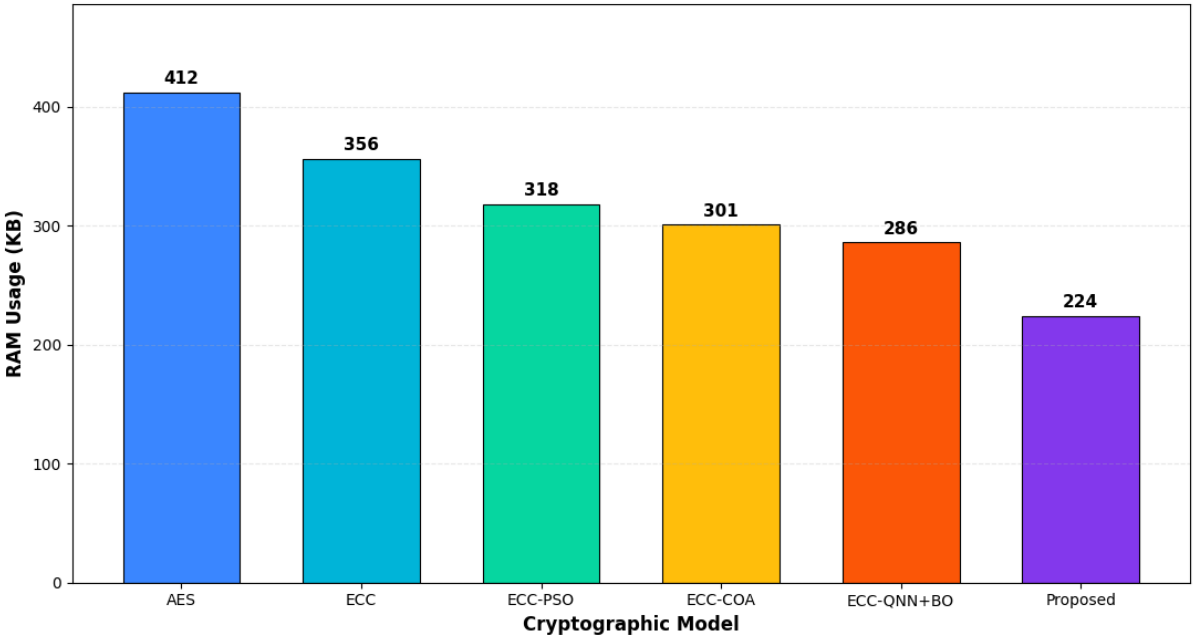

Figure 15: RAM Usage Comparison

Figure 15 shows the required amount of RAM for the evaluated approaches to cryptography. AES consumes 412 KB of RAM, while ECC requires 356 KB. The ECC-PSO and ECC-COA shrink the memory requirements to 318 KB and 301 KB, respectively. ECC-QNN+BO can reduce RAM consumption to 286 KB. The proposed ASI-ECCO + AMTC-Net has RAM requirement of only 224 KB. The reduction shows that adaptive optimization of ECC can reduce cryptographic operations in terms of memory consumption and dealing with parameters. Hence the proposed approach is more appropriate for agricultural IoT sensors having limited memory.

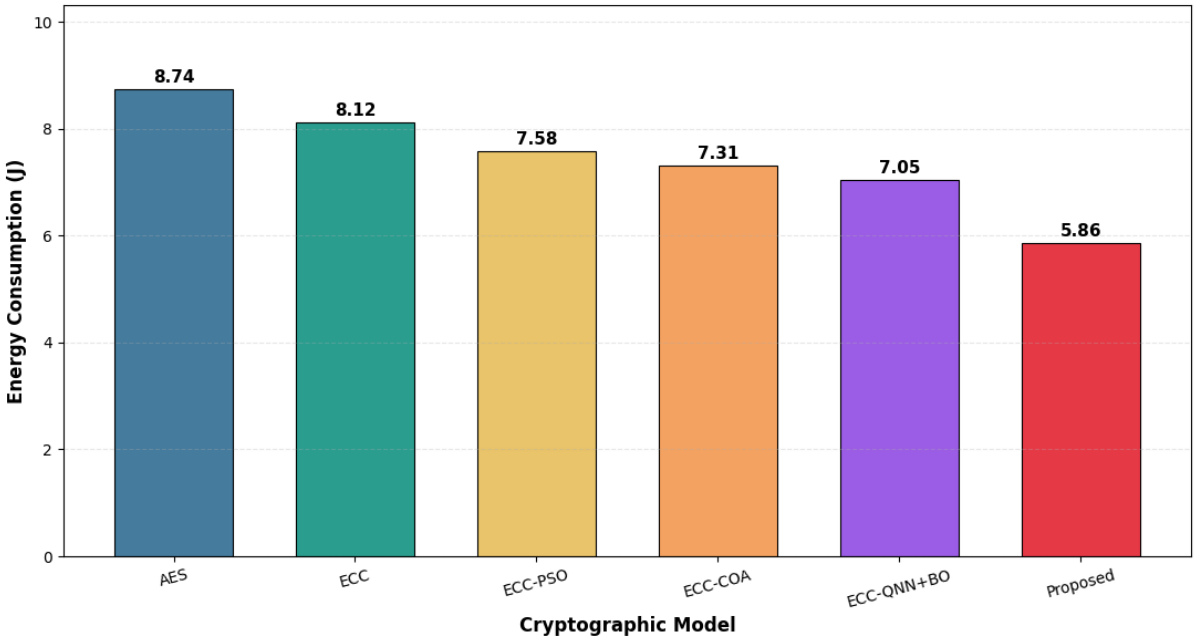

Figure 16: Energy Consumption Comparison

The energy consumption of the evaluated cryptographic solutions is shown in figure 16. AES consumes 8.74 J, while ECC requires 8.12 J. The optimized ECC-PSO, ECC-COA, and ECC-QNN+BO approaches consume 7.58 J, 7.31 J, and 7.05 J, respectively. The proposed ASI-ECCO + AMTC-Net uses just 5.86 J. This is a significant reduction in energy needs. This improvement shows that adaptive security–resource coupling can effectively select lightweight ECC configurations, which can also minimize the energy consumption in both processing and communication, and prolong the operational lifetimes of the agricultural IoT nodes.

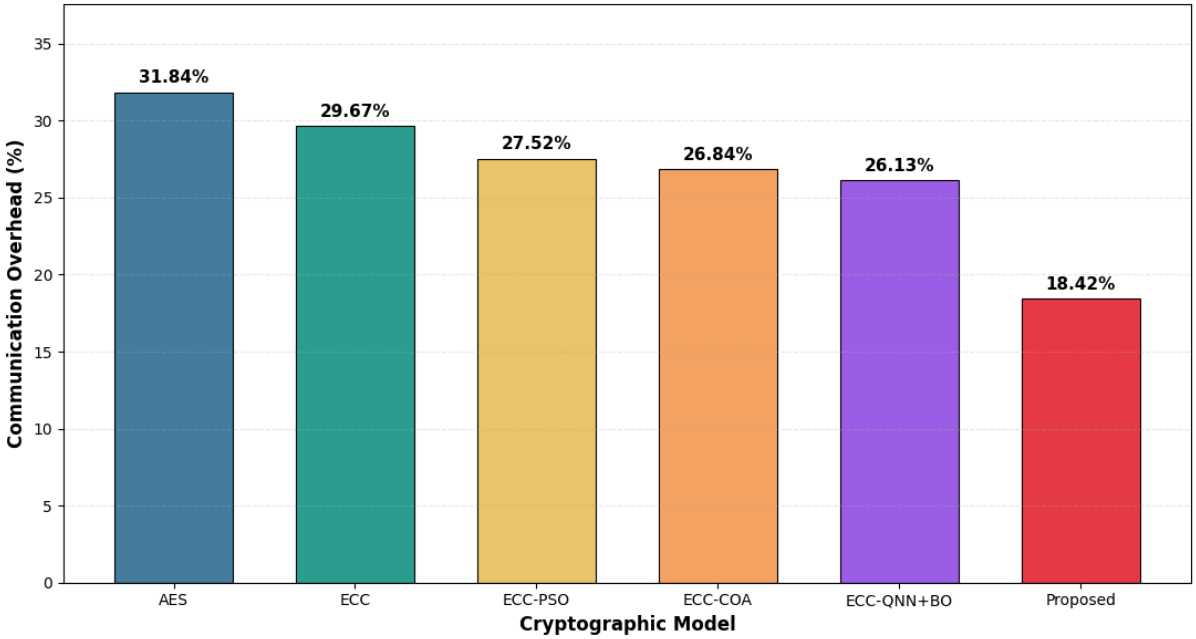

Figure 17: Communication Overhead Comparison

In order to compare the communication overhead for the security approaches evaluated, we have plotted them against one another as shown in figure 17. AES produces the highest overhead of 31.84%, followed by ECC at 29.67%. ECC-PSO and ECC-COA reduce the overhead to 27.52% and 26.84%, respectively, while ECC-QNN+BO achieves

26.13%. The proposed ASI-ECCO + AMTC-Net has the minimum communication overhead as low as 18.42%. This significant decrease in the number of extra communication requests demonstrates that adaptive ECC parameter selection and lightweight security management decrease the extra communications needs, which makes the suggested framework more efficient for bandwidth and energy constrained agricultural IoT networks.

4.5 Discussion

Some of the benefits of the suggested ASI-ECCO + AMTC-Net framework include; first, ASI-ECCO is able to adaptively optimize ECC parameters and cryptographic keys such that the amount of cryptographic overhead is lowered to 18.42%, while the amount of energy consumed is 5.86 J. Secondly, the light-weight ECC protocol enables secure communication among resource limited agricultural IoT devices without the need for additional computational costs. Thirdly, the suggested architecture enables a wide range of security services which include, encryption, authentication, secure key exchange and data integrity verification. Fourthly, AMTC-Net enables intelligent threat identification such that the level of threat detection is at 96.34% and false positives at 3.21%. Communication performance of the framework is also very high with the level of accuracy at 95.60% and communication transparency at 95.80%. However, there are some of the weaknesses associated with the framework which are as follows; the process of optimization increases the amount of computational cost during the parameter selection stage. The framework has also been tested on a particular agricultural IoT dataset and thus needs to be tested through other agricultural datasets. The performance of the framework will also depend on the sensor hardware, network environment, attack severity and communication protocols.

5. Conclusion

The suggested Adaptive Swarm Intelligence-driven Elliptic Curve Cryptography Optimization with Adaptive Multi-layer Threat Cognition Network (ASI-ECCO + AMTC-Net) offers a lightweight and robust framework for agricultural IoT communication. In ASI-ECCO, optimization of ECC parameters, key generation, and security settings have been carried out. AMTC-Net helps increase intelligent detection of communication threats. Experiment results reveal that the framework achieves 18.42% cryptographic overhead, 95.60% communication accuracy, 95.80% communication transparency, 5.86 J energy consumption, 96.34% threat detection rate, and 3.21% false positive rate. Relative to the best baseline method, the framework decreases cryptographic overhead from 26.13% to 18.42% that constitutes a 29.43% reduction, whereas energy consumption is reduced from 7.05 J to 5.86 J that corresponds to a 16.88% reduction. Communication accuracy is improved from 94.67% to 95.60% (0.98% relative improvement), whereas communication transparency is improved from 94.36% to 95.80% (1.53% relative improvement). Threat detection rate is improved from 93.18% to 96.34% (3.39% relative improvement), while false positive rate is decreased from 4.87% to 3.21% (34.11% reduction).

5.1 Future scope

Future research may continue the development of the ASI-ECCO + AMTC-Net scheme towards practical applications of IoT in agriculture that will include different types of sensors, gateways, edge devices, drones, autonomous equipment, and cloud platform. The suggested method of optimization can be enhanced by applying the ideas of online and self-adaptive learning in order for ECC parameters to change accordingly to the network environment changes, energy state of the devices, and new demands concerning security. Future research may also focus on such methods as advanced cryptographic mechanisms that include post-quantum cryptography and ECC hybrids to ensure safety in the face of new computational challenges. The system of AMTC-Net can be extended in order for it to identify zero-day, unknown, and coordinated multi-stage attacks with the help of continual learning and behavioral analysis. Future research may utilize large-scale datasets that would include data from different agricultural environments to enhance generalization and decrease dependence on the dataset. Finally, future work should test the framework on the actual resource-constrained hardware like sensors and edge gateways taking into account latency, memory usage, battery life, and scalability.

References

1. Morchid, A., Alblushi, I. G. M., Khalid, H. M., Alami, R. E., Sitaraman, S. R., & Muyeen, S. M. (2026). High-technology agriculture system to enhance food security: A concept of smart irrigation system using Internet of Things and cloud computing. Journal of the Saudi Society of Agricultural Sciences, 25(3), 42.
2. Morchid, A., Qjidaa, H., Alami, R. E., Mobayen, S., Skruch, P., & Bossoufi, B. (2026). Smart irrigation-based internet of things and cloud computing technologies for sustainable farming. Scientific Reports.

3. Abba Ari, A. A., Baba, E., Aziz, H. A., Boukadi, K., Thiare, O., & Gueroui, A. M. (2026). Smart Agriculture Through Internet of Things and Machine Learning: A Survey of Monitoring Techniques, Methods and Applications. IET Wireless Sensor Systems, 16(1), e70033.
4. Annadhurai, H., Paleti, L., Chinnakunnu, R. K., & Rajendran, S. (2026). A data-driven approach to vertical harvesting: artificial intelligence and internet of things-based automation in agriculture. Agrociencia, 1-19.
5. KUMAR SHARMA, V., Jeberson, W., & KUMAR ISAAC, R. (2026). INTERNET-OF-THINGS (IOT)-BASED SMART AGRICULTURE AND PRECISION IRRIGATION FOR AGRICULTURE-AN INTELLIGENT WATER MANAGEMENT. Yugoslav Journal of Operations Research, 36(1), 45.
6. Ahmad, A. Y. B., Alzubi, J. A., K, C., Urooj, S., & Shahzad, M. (2026). Automated smart drip irrigation system in internet of things using adaptive residual hybrid network for precision farming. Scientific Reports, 16(1), 4327.
7. Cariou, C., Moiroux-Arvis, L., & Chanet, J. P. (2026, May). Advances on the Internet of Things for High-Resolution and Multi-Scale Measurements in Agricultural Ecosystems. In ALLSENSORS 2026: The Eleventh International Conference on Advances in Sensors, Actuators, Metering and Sensing.
8. Zhang, X. (2026). Promoting agricultural basic services through network security based on artificial intelligence and the Internet of Things: economic sustainability. International Journal of System Assurance Engineering and Management, 1-14.
9. Sari, M. W., Hardyanto, R. H., Ciptadi, P. W., Kurniawan, E., & Santoso, B. (2026). Designing a Smart Farming Greenhouse Electrical Power Monitoring System Based on Internet of Things Technology. Engineering, Technology & Applied Science Research, 16(1), 31983-31990.
10. Rani, N. S., & Banu, N. S. (2026). Cognitive integration of internet of things and feedforward learning models for smart irrigation in sustainable agriculture. Scientific Reports.
11. Boadu, S., Thompson, E. A., Godavarthy, R., Akoto, E., Dadson, K., & Atuobi, H. B. (2026). Internet of things in rural agricultural freight transportation. A case study of North Dakota State. Transportation Research Part E: Logistics and Transportation Review, 214, 104929.
12. Vanitha, N. S., Sudha, G., Gowrishankar, J., Radhika, K., Kalaiyarasan, A., & Infantiya, S. G. (2026). Energy Efficient Internet of Things and Wireless Sensor Networks in Smart Agriculture. Energy Efficient Internet of Things-Based Wireless Sensor Network, 429-452.
13. Has, M., Kreković, D., Kušek, M., & Podnar Žarko, I. (2024). Efficient data management in agricultural IoT: Compression, security, and MQTT protocol analysis. Sensors, 24(11), 3517.
14. Shafik, W., Tufail, A., Apong, R. A. A. H. M., & De Silva, L. C. (2024). Internet of Things for smart agricultural practices. In Internet of Things applications and technology (pp. 190-217). Auerbach Publications.
15. Zhao, B., Zheng, D., Yang, C., Wang, S., Mansurova, M., Jomartova, S., ... & Grants, R. (2025). Design and optimization of an internet of things-based cloud platform for autonomous agricultural machinery using narrowband internet of things and 5G dual-channel communication. Electronics, 14(8), 1672.
16. Selvam, P., Krishnamoorthy, N., Kumar, S. P., Lokeshwaran, K., Lokesh, M., Syamala, M., & Vidhya, R. G. (2025). Internet of Things Integrated Deep-Learning Algorithms Monitoring and Predicting Abnormalities in Agriculture Land. Internet Technology Letters, 8(5), e607.
17. Vellimalaipattinam Thiruvenkatasamy, K., Ghanimi, H. M., Sengan, S., & Alharbi, M. G. (2025). An online tool based on the Internet of Things and intelligent blockchain technology for data privacy and security in rural and agricultural development. Scientific Reports, 15(1), 27349.
18. Elhattab, K., & Abouelmehdi, K. (2024). Intelligent agriculture system using low energy and based on the use of the internet of things. Bulletin of Electrical Engineering and Informatics, 13(2), 1286-1297.
19. Morchid, A., Oughannou, Z., El Alami, R., Qjidaa, H., Jamil, M. O., & Khalid, H. M. (2024). Integrated internet of things (IoT) solutions for early fire detection in smart agriculture. Results in engineering, 24, 103392.
20. Wang, C., & Gong, J. (2024). Intelligent agricultural greenhouse control system based on internet of things and machine learning. arXiv preprint arXiv:2402.09488.
21. Bangare, P. S. (2023). Internet of things based secured data transmission protocol for agriculture application. Ingenierie des Systemes d'Information, 28(2), 419.
22. Ait Oussous, S., Bajit, A., Achour, Y., Morino, I., Zejli, D., & Elbouayadi, R. (2023, October). Applying computational intelligence, visual optimization tools, and synchronized PAYLOAD's handshaking to enhance greenhouses ECC cyber security-based agriculture IoT's properties. In 2023 9th International Conference on Optimization and Applications (ICOA) (pp. 1-8). IEEE.
23. Sammeta, N., & Parthiban, L. (2022). RETRACTED: An optimal elliptic curve cryptography-based encryption algorithm for blockchain-enabled medical image transmission. Journal of Intelligent & Fuzzy Systems, 43(6), 8275-8287.
24. Somula, R., Cho, Y., & Mohanta, B. K. (2023). EACH-COA: an energy-aware cluster head selection for the internet of things using the coati optimization algorithm. Information, 14(11), 601.
25. Gunisetti, L., Koduri, S. B., & Jagannathan, V. (2023). Optimized deep learning system for smart maize leaf disease detection in IoT platform via routing algorithm. Multimedia Tools and Applications, 82(9), 13533-13555.