

Lightweight Cryptography Algorithm for Secure Data Transmission in IoT Applications

Kumar K^{1,*} and Dr. K Sasikala²

¹Research Scholar, Department of Computer Science & Engineering, Vinayaka Mission's Kirupananda Variyar Engineering College, Periya Seeragapadi Salem - 636 308, Tamil Nadu, India

²Professor & Head /IT, R P Sarathy Institute of Technology, Poosaripatti, Salem, India

*E-mail: kumar.k542254@gmail.com

Received for publication
December 03, 2025.

Abstract

The rapid expansion of Internet of Things (IoT) networks introduces critical security challenges, particularly during data transmission. This manuscript presents a novel lightweight cryptography framework that integrates the Firefly Optimization with Elliptic Curve Cryptography (FA-ECC) to optimize key management and enhance data security. Additionally, a dense recurrent neural network (DRNN) module predicts and blocks malicious data entries, ensuring only legitimate data reaches the cloud. The proposed framework simultaneously improves security, efficiency and quality of service in IoT networks. Experimental evaluations demonstrate that the FA-ECC and DRNN integration effectively reduces energy consumption, transmission delay and vulnerability to attacks, establishing a secure and optimized data exchange mechanism for IoT environments.

Keywords

lightweight cryptography algorithm, Firefly optimization, elliptic curve cryptography, dense recurrent neural network

1. Introduction

In recent years, developing nations' economies have become highly dependent on agriculture, and it has become a greater source of income and contributions to the country's gross domestic product [1]. However, most of the agricultural practices followed in the country are based on the farmers' experience and *ad hoc* insights [2]. Properly controlling agricultural land increases productivity, resulting in more profits for farmers [3]. To achieve this, there is a need for continuous monitoring of the farm, which is quite impossible and demands more labor in traditional farming practices [4]. The Internet of Things (IoT) technology is applied in the agricultural field to resolve these issues. The utilization of IoT in agriculture aids continuous and regular monitoring of farms, which improves productivity [5]. Current advancements such as Agriculture 4.0, which is also known as smart agriculture, use rapidly growing technologies including artificial intelligence (AI), big data analysis, blockchain, robotics and wireless sensor networks (WSNs)

[6]. These technologies are integrated into the agricultural field, which enables farmers to identify problems on the farm at an early stage and helps to reduce productivity loss [7]. In smart agriculture, numerous sensors are utilized to collect farm information, including data such as air humidity, irrigation level, radiation, weather data and soil moisture [8]. Also, to monitor the farm surroundings, the smart agricultural system uses drones and IoT devices. This enables improved productivity and aids protection from disasters [9].

Although the smart agricultural system boosts yield production, it has several challenges. The primary concern of smart agriculture is the security and privacy issues, which need to be discussed to improve agricultural practices [10]. Rapidly growing technologies, such as IoT and big data, make smart agricultural systems prone to security breaches [11]. Moreover, the smart devices used in smart agriculture exchange numerous messages between the source and destination [39]. The insecure communication channels between IoT devices, drones and other sensor devices expose smart farming to diverse

attacks such as Denial of Service (DoS) and Wi-Fi de-authentication [12]. These attacks can cause severe consequences on the sensed data, such as water quality, chemical content of the soil, temperature, soil moisture, light and rainfall rate, collected from the agricultural fields, resulting in ineffective and suboptimal decision-making [13]. The ineffective decision-making results in incorrect choice of pesticides, inappropriate irrigation levels, etc., leading to economic and productivity losses [14]. Also, the utilization of open WSNs during data exchange potentially reduces the integrity, confidentiality and authenticity of the transferred data [40]. Therefore, ensuring secure communication in intelligent agriculture is important for improving agricultural practices. Hence, many studies have been conducted to design a robust algorithm to facilitate secure data transmission in the IoT-based agricultural system [15]. However, conventional methods cannot handle threats such as interception, message alteration and interference [16, 17]. To overcome these challenges, the studies focused on developing cryptographic algorithms for securely transmitting data in smart agriculture [41–43]. The cryptographic algorithms encrypt or encode the original sensed data into another form, which other persons cannot decode, except authenticated users [18, 19]. However, the studies found that issues such as effective energy resource utilization and highly secure data transmission in smart agriculture are yet to be solved [20].

Some existing works, such as lightweight encryption based on the tiny encryption algorithm (TEA) [21], privacy-preserving and efficient key agreement algorithm utilizing elliptic curve cryptography (ECC) [22] and ECC-based algorithm [23], are developed for resolving the security challenges. Although they offer comparatively better data security than conventional models, they face issues such as high delay, high energy usage and large packet loss [44]. Moreover, they cannot respond to evolving cyber threats in the network, making them ineffective for real-time applications. To address the above issues, we proposed a lightweight cryptographic algorithm combining meta-heuristic optimization and cryptographic techniques.

Key contributions of the presented research are described as follows:

- This article presents a novel lightweight cryptography approach for securing the IoT-based agriculture system. Initially, the agriculture dataset containing crop-related information was collected and imported into the system.

- A dense recurrent neural network (DRNN)-based attack prediction module was used to predict malicious data entry in the system, and the predicted malicious data were eliminated to ensure the security of the system.
- Then, an optimized lightweight cryptographic algorithm was created by combining Firefly optimization with elliptic curve cryptography to protect the data from cyber threats during transmission.
- Finally, the results of the proposed technique were examined and validated with existing techniques in terms of processing time, encryption and decryption time, confidentiality rate, error rate, etc.

The organization of the presented research article is sequenced as follows: Section II describes the recent literature related to the presented work, Section III illustrates the system model and problem statement, Section IV explains the proposed methodology and its working, Section V examines the results of the proposed work and Section VI states the conclusion of the article.

II. Related Works

A few recent studies relevant to the proposed work are described below:

Recent advances in IoT-enabled smart agriculture have intensified the need for lightweight, secure and energy-efficient data protection mechanisms due to the constrained nature of sensor nodes and the openness of wireless communication channels. Awotunde et al. [21] addressed computational efficiency by employing the TEA, prioritizing software-based lightweight encryption over hardware implementations. While their approach successfully reduced encryption latency and memory overhead, it overlooked critical IoT constraints such as sensor battery depletion, long-term scalability and cost-sensitive deployment, which are fundamental in large-scale agricultural environments.

To enhance privacy in smart agriculture, Itoo et al. [23] proposed an ECC- and hash-based key agreement protocol to secure communication among IoT devices. Although the protocol provides strong cryptographic guarantees and superior resistance to common attacks, its multistep key exchange process increases computational complexity, making it less practical for real-time agricultural monitoring systems composed of low-power devices.

Similarly, Abduljabbar et al. [23] developed an ECC-based secure data exchange mechanism that significantly reduced computational

and communication costs. Despite measurable improvements in efficiency and security attributes, the protocol suffers from limited adaptability when the network scales dynamically, a common characteristic of agricultural IoT deployments with frequently added or removed sensor nodes.

Energy efficiency has also been explored by Song et al. [24], who introduced a lightweight block cipher using a permutation–substitution architecture optimized for low-energy consumption. The integration of a genetic algorithm-based S-box effectively reduced latency and power usage. However, this approach primarily secures sensor-level transmission and fails to address end-to-end data confidentiality and integrity once data are transferred to cloud servers, leaving agricultural data vulnerable at higher layers.

In contrast to encryption-centric approaches, Pan et al. [25] focused on physical-layer security by proposing a lightweight channel authentication framework using frequency-domain attribute engineering. The model demonstrated high precision and recall in identifying legitimate transmitters. Nevertheless, it only detects unauthorized access attempts and does not provide preventive mechanisms such as access control or cryptographic isolation, limiting its effectiveness against coordinated attacks.

Blockchain-based security solutions were explored by Zhao et al. [26], who integrated Rivest Cipher 5 (RC5) encryption with blockchain-enabled data storage for IoT agriculture systems. Their approach improved data retrieval efficiency and ensured integrity through Merkle tree validation. However, the study neglected blockchain-specific cyber threats such as smart contract vulnerabilities, consensus manipulation and storage overhead, which may offset the benefits in resource-constrained agricultural IoT environments.

Beyond cryptographic techniques, Berguiga et al. [27] proposed a hybrid intrusion detection framework combining multilayer perceptron and Gaussian mixture models. The framework demonstrated strong detection performance against Distributed Denial of Service (DDoS) attacks using the CIC-DDoS2019 dataset. Despite its effectiveness, the model lacks generalization capability for emerging and multi-vector cyber threats, which are increasingly prevalent in modern smart agriculture infrastructures. The summary of the literature survey is detailed in Table 1.

III. Problem Statement

Smart agriculture is a rapidly developing field that integrates advanced technologies such as IoT, big

data and AI to revolutionize agricultural practices. Incorporating these technologies enables farmers to monitor the farm regularly and continuously, resulting in increased productivity and reduced economic loss. However, in smart agriculture, IoT devices exchange numerous data and messages over wireless channels, leading to security and privacy issues [28]. The main challenge is the vulnerability of the data to cyber threats during transmission. Since IoT devices are interconnected over wireless networks, the smart agriculture system becomes more susceptible to security threats such as unauthorized data access and data interception. Therefore, developing a robust security framework to address the privacy and security challenges in smart agriculture is significant. Hence, several studies have developed intrusion detection systems (IDS) for smart agriculture. The IDS frameworks use deep learning or machine learning algorithms to identify the pattern difference between normal and malicious data within a smart agriculture system. Although they offer improved accuracy in attack prediction, they face challenges such as overfitting, large data demands, limited generalization and high computational power. Moreover, they cannot offer confidentiality and integrity to the data during transmission. Hence, the studies focused on designing secure data exchange protocols for IoT-assisted agricultural systems. These protocols use cryptographic algorithms for protecting the data from cyber threats. However, they are limited in terms of adaptability and scalability. Moreover, they cannot respond to the evolving cyber threats in the smart agricultural system. To overcome these issues, this study proposed a hybrid lightweight cryptographic algorithm combining meta-heuristic optimization and a cryptographic algorithm. In addition, we utilized deep learning algorithms to protect the agricultural system. The attack prediction module created using deep learning prevents malicious data entry by accurately predicting and eliminating it from the system. Incorporating deep learning, optimization and cryptographic algorithms offers a balanced performance between security and scalability. By developing this algorithm, this study aims to improve the security of the smart agriculture system.

IV. Proposed Lightweight Cryptographic Algorithm for Smart Agriculture

The proposal suggests a novel lightweight cryptographic algorithm to enhance data security during

Table 1: Literature review summary

Authors	Methodology	Findings	Merits	Demerits
Awotunde et al. [21]	TEA	Minimized encryption time while maintaining efficiency vs. security trade-off	Provides secure and efficient data security	Low battery life and limited memory capacity in IoT devices
Ito et al. [23]	Privacy-preserving and efficient key agreement algorithm	Ensures secure data transmission among IoT devices in smart agriculture monitoring systems	Offers greater data protection	Implementation is complex and may require high computational resources
Abduljabbar et al. [23]	ECC-based data exchange algorithm	Enables secure data transmission between IoT devices	Reduces computation and implementation costs while improving security	Limited adaptability and scalability in large-scale deployments
Song et al. [24]	Low-energy lightweight block cipher framework	Minimizes data loss during sensor data transmission	Reduces latency and energy consumption	Cannot guarantee optimal security for data stored in the cloud
Pan et al. [25]	Lightweight channel authentication framework	Accurately differentiates between authentic and unauthorized users	Achieved 96.6% precision, 95.6% recall and 96.1% F-measure	Cannot prevent all types of security threats
Zhao et al. [26]	Reliable and fast data storage strategy using blockchain	Stores agricultural farm data rapidly	Reads farm data 10× faster than conventional methods	Does not consider cyber threats associated with IoT-based data storage
Berguiga et al. [27]	Multilayer perceptron and Gaussian mixture model-based intrusion detection framework	Predicts normal and abnormal traffic in smart agriculture accurately	Improved accuracy, recall, precision and F-measure for attack prediction	Limited to specific attacks (e.g., DDoS); cannot generalize to evolving cyber threats

ECC, elliptic curve cryptography; IoT, Internet of Things; TEA, tiny encryption algorithm.

data transmission in smart agriculture systems. The proposed strategy combines the efficiency of the meta-heuristic optimization algorithm with the cryptographic algorithm for secure data transmission within smart agriculture systems. Initially, the IoT-based agricultural data are collected from the standard site. Then, an attack prediction module is created using the DRNN [31] to predict the malicious data. After attack prediction, the identified malicious data are removed from the system to ensure security and privacy in the network. Further, the collected data are transmitted to the cloud for further analysis. However, the transmission of data over wireless

channels imposes security threats, adversely influencing data integrity and confidentiality. To resolve this challenge, we propose optimized lightweight cryptographic algorithms using the combination of FA-ECC. The strategy aims to ensure the confidentiality and integrity of sensitive information during transmission to the cloud. To meet this objective, we encrypt the agricultural data before transmission to the cloud using the proposed FA-ECC algorithm so that unauthorized users cannot access it. In the proposed method, the Firefly algorithm (FA) refines the initial parameters of the ECC, enabling effective data encryption.

The novelty of the proposed lightweight cryptographic framework is established through a systematic comparison with existing security solutions developed for IoT-based smart agriculture systems. While several prior studies focus on individual aspects of security such as encryption, authentication or intrusion detection, the proposed work introduces a holistic, optimized and adaptive security architecture tailored for resource-constrained agricultural IoT environments. Existing lightweight encryption approaches such as TEA-based schemes [21] primarily emphasize reducing computational overhead but fail to address energy efficiency, adaptive key management and evolving cyber threats. In contrast, the proposed framework integrates Firefly optimization with elliptic curve cryptography (FA-ECC) to dynamically optimize cryptographic parameters, thereby achieving lower energy consumption and reduced execution time without compromising security strength. ECC-based authentication and key agreement protocols proposed in [22, 23] provide strong cryptographic security but suffer from high computational complexity and limited scalability in large-scale and dynamic IoT deployments. The proposed model overcomes these limitations by employing meta-heuristic optimization for key refinement, enabling efficient key generation and management even when the network scales or changes dynamically. Unlike low-energy block cipher frameworks [24], which mainly secure sensor-level data transmission, the proposed framework ensures end-to-end data confidentiality and integrity, extending protection from sensor nodes to cloud storage. This comprehensive coverage addresses a critical limitation observed in existing agricultural IoT security solutions. Furthermore, physical-layer authentication techniques such as frequency-domain channel authentication [25] can only detect unauthorized transmitters but cannot prevent or mitigate cyberattacks. The proposed work enhances threat mitigation by integrating a DRNN-based intrusion prediction module, capable of identifying and eliminating malicious data entries before encryption and transmission. Blockchain-based storage solutions [26] improve data integrity but often ignore computational overhead and blockchain-specific cyber threats. In contrast, the proposed framework prioritizes lightweight cryptographic operations and optimized data transmission, making it more suitable for real-time agricultural monitoring systems. IDS using deep learning models [27] are typically trained for specific attack types such as DDoS and lack adaptability to emerging threats. The proposed DRNN-based attack prediction module is designed to learn sequential

attack patterns, improving generalization across multiple attack vectors commonly observed in IoT networks.

a. Data collection

The proposed security model commences with the collection of agricultural data from the smart farm. This study utilizes publicly available databases, namely the ToN-IoT dataset [29]. The ToN-IoT dataset contains a variety of data collected from IoT and IoT sensor telemetry records. This dataset comprises a variety of attack instances interconnected with the IoT network. The attack instances include backdoor, Man-in-the-Middle attack (MITM), DDoS, DoS, injection, password, scanning, Cross-Site Scripting (XSS) and ransomware. Also, this dataset contains normal instances. There are a total of 10 different classes in this dataset comprising 45 features, which are utilized to identify the pattern of attacks in smart agriculture. In addition, the ToN-IoT database contains 378,782 data points. The normal class contains information regarding the farm, such as soil moisture, humidity, temperature, pH and rainfall rate. This dataset is split into sets containing 303,025 and 75,757 data points for training and testing purposes. The description of the dataset is provided in Table 2. Furthermore, the data have been collected using the following link: <https://research.unsw.edu.au/projects/toniot-datasets>.

b. Attack prediction

Hackers utilize a technique known as a cryptographic attack to target cryptographic solutions, such as encryption keys and ciphertext. These attacks aim to either decrypt the encrypted data or extract the plaintext from the ciphertext. By identifying gaps and holes in cryptography methods, cryptographic protocols, encryption algorithms or key management strategies, hackers may try to get around a cryptographic system's security. Text or video sequences can have sequential data, and RNNs are used to anticipate what will come next. A layer's neuron in an Recurrent Neural Network (RNN) additionally gets a time-delayed input from the prediction of its own prior instance. The RNN cell, which serves as a second input for each prediction, stores this instance prediction. A convolutional neural network is a type of network with a limited impulse response, while a recurrent neural network is a class of networks with an infinite impulse response. Networks in both groups behave dynamically over time. The proposed framework is demonstrated in Figure 1.

Table 2: Dataset description

Dataset	Class partition	Data points	Rate of class frequency (%)
ToN-IoT training set	Backdoor	14,135	4.35
	MITM	727	0.21
	DDoS	13,971	4.32
	DoS	13,913	4.33
	Injection	14,071	4.34
	Password	14,017	4.37
	Scanning	14,100	4.29
	XSS	14,012	4.36
	Ransomware	13,992	4.32
	Normal	209,792	65.06
ToN-IoT testing set	Backdoor	5,865	4.29
	MITM	316	0.25
	DDoS	6,029	4.33
	DoS	6,087	4.36
	Injection	5,929	4.31
	Password	5,983	4.26
	Scanning	5,900	4.44
	XSS	5,988	4.28
	Ransomware	6,008	4.36
	Normal	90,208	65.06

DoS, Denial of Service.

Deep networks can be trained more effectively than models without skip connections, thanks to skip connections that omit certain layers. Skip connections are often used in research toward feedback links. Apply the skip connections toward recurrent connections in this research. The skip connections across time equal the shortcut paths from the various hidden states before to the hidden state at time t . The feedback linkages between various layers at various time steps are part of the shortcut pathways. Like the global gate in the gated feedback RNN, the attention gate governs each link. The definition of the dense RNN is represented in Eq. (1).

$$h_t^j = \mathcal{O}\left(w^j h_t^{j-1} + \sum(k=1)(i=1)g^{(k,i) \rightarrow j} U^{(k,i) \rightarrow j} h_{t-k}^i\right) \quad (1)$$

where h denotes the hidden state, w indicates the weight and g is represented in Eq. (2)

$$g^{(k,i) \rightarrow j} = \sigma\left(w_{gh}^j h_{t-1}^{i-1} + u_g^{(k,i) \rightarrow j} h_{t-k}^i\right) \quad (2)$$

This is a function of the hidden state that came before it at layer i and time $t - k$, whereas Eq. (6) is a function of the hidden states that came before, combined. The following describes the rationale behind changing the gate function to an attention gate. A dense Long Short-Term Memory (LSTM) can be simply expanded from a dense RNN. Here is how the dense LSTM is represented in Eqs (3)–(6).

$$i_t^j = \sigma\left(w^{(i,j)} h_t^{i-1} + \sum(k=1)(i=1)g^{(k,i) \rightarrow j} U^{(k,i) \rightarrow j} h_{t-k}^i\right) \quad (3)$$

$$f_t^j = \sigma\left(w^{(f,j)} h_t^{j-1} + \sum(k=1)(i=1)g^{(k,i) \rightarrow j} U^{(k,i) \rightarrow j} h_{t-k}^i\right) \quad (4)$$

$$o_t^j = \sigma\left(w^{(o,j)} h_t^{j-1} + \sum(k=1)(i=1)g^{(k,i) \rightarrow j} U^{(k,i) \rightarrow j} h_{t-k}^i\right) \quad (5)$$

$$c_t^j = \mathcal{O}\left(w_c^j h_t^{j-1} + \sigma(k=1, i=1)g_c^{(k,i) \rightarrow j} U_c^{(k,i) \rightarrow j} h_{t-1}^i\right) \quad (6)$$

The attention gate g is applied to all gates and the state of the memory cell, in contrast to gated feed-back LSTM [30]. Given previous sequential data, recurrent connections allow for the prediction of subsequent data. Based on the previous word and the last context acquired before the previous word, the RNNs in language modeling are able to forecast the word that will come next. It assumes that the previous word alone influences word prediction.

c. Data encryption

By converting data into ciphertext, which can only be decoded with a special decryption key generated either before or at the time of the encryption, data encryption serves to protect the secrecy of data. Data encryption transforms information into a code that is only accessible to those with a secret key or password. Data that have undergone encryption is known as ciphertext, whereas data that have not are known as plaintext. In today's business sector, encryption is one of the most popular and effective data protection solutions. The significance of encryption as a mechanism for preserving data integrity cannot be emphasized. The sender must choose which cipher will best conceal the message's meaning at the outset of the encryption process,

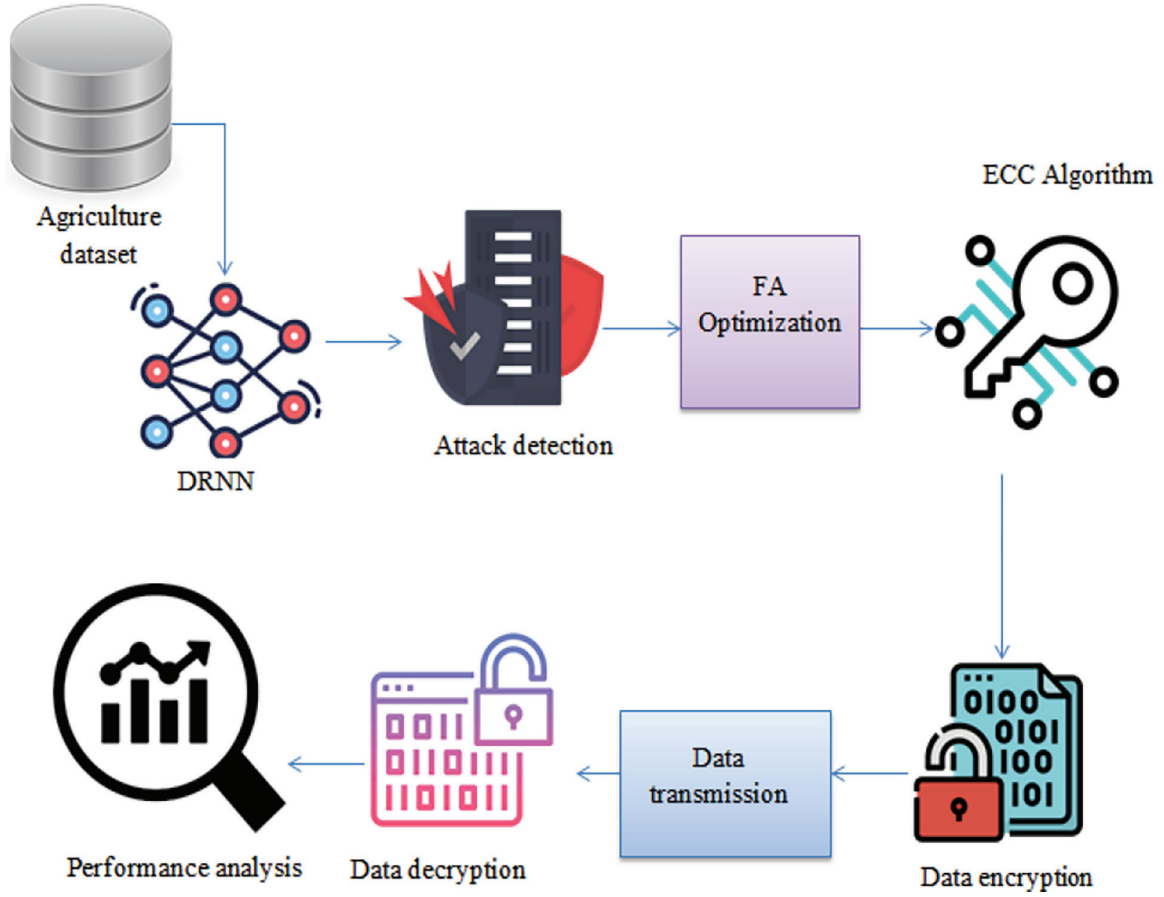


Figure 1: Proposed methodology. DRNN, dense recurrent neural network; ECC, elliptic curve cryptography; FA, Firefly algorithm.

as well as which variable to employ as a key to ensure that the encoded message is unique. Symmetric and asymmetric ciphers are the two most popular types of ciphers. Data encryption converts information into a different format, or code, so that only those with a password or secret key can access it. Plaintext refers to unencrypted data, while ciphertext is the term used to describe encrypted data. Right now, one of the most widely utilized and successful data security techniques employed by businesses is encryption. There are two primary forms of data encryption: symmetric encryption and asymmetric encryption, which is commonly referred to as public-key encryption.

d. Firefly optimized elliptic curve cryptography

One type of bionic swarm intelligence optimization technique is the FA. There are two things about fireflies: brightness and appeal. Fireflies that glow brightly can draw in other fireflies that glow less

brightly. Moving from the weak firefly to the strong firefly completes the position iteration procedure. The aforementioned idea states that a methodical, iterative approach can be used to find the best solution. Each firefly in the population is represented as a vector point in the search space, or as a solution to the problem, in the population-based algorithm known as the FA. The relative brightness and relative attraction of fireflies can be expressed as Eq. (7),

$$C = (c(x_1) \dots c(im)), \text{ where } x = 1, 2, \dots, \xi \quad (7)$$

where ξ represents the total number of individuals in the firefly population and m denotes the problem's dimension. The 128-bit cipher key (Kc), which is the initial stage of key encryption, is divided into 64-bit right and 64-bit left segments. That is described in Eqs (8) and (9),

$$\theta = \theta_0 e^{-Is_{xy}} \quad (8)$$

$$\mu(\delta) = \mu_0 e^{-l\delta_{xy}^2} \quad (9)$$

where μ_0 is the greatest degree of attraction or the degree of attraction at $\delta = 0$, and θ_0 is the firefly's fluorescence brightness at $\delta = 0$. The distance between positions x and y is represented by $\delta(xy)$, and L is the light absorption parameter, which can be set as a constant and indicates the property that the fluorescence is weakened by distance and propagation medium. The Euclidean distance between two fireflies is stated in Eq. (10)

$$\delta_{xy} = \|c_x - c_y\| = \sqrt{\sum_{k=1}^m c_{xk} - c_{yk})^2}. \quad (10)$$

The two present phases that comprise ECC's responsibilities are the prime stage and the binary stage. The sensible field is chosen for cryptographic operations with a finite number of points, and the prime phase tasks select a prime number; however, very few important fundamental focuses are built on elliptic curves. For "ECC," which uses prime numbers, the creation of private and public keys is crucial. The recipient decrypts the private key after the sender encrypts the data using the recipient's public key. A method of public-key cryptography (PKC) known as ECC is based on the algebraic structure of elliptic curves over finite fields. Compared to non-Elliptic Curve (EC) encryption, ECC enables equal security with smaller keys. Elliptic curves can be used for a variety of purposes, including digital signatures, pseudo-random generators and key agreement. By combining the key agreement with a symmetric encryption algorithm, they can be used indirectly for encryption. Additionally, they are a component of a number of integer factorization methods, including Lenstra elliptic-curve factorization, which finds value in encryption.

An elliptic curve is a plane curve made up of the points that meet the following equation over a finite field (as opposed to the real numbers), as described in Eq. (11),

$$y^2 = x^3 + ax + b. \quad (11)$$

In addition to the finite points on the curve, elliptic curve cryptography includes a unique point at infinity, denoted by the symbol ∞ . In order to avoid making the curve equation significantly more difficult, the coordinates in this case must be selected from a fixed finite field with a characteristic that is not equal

to 2 or 3. This collection of points is an abelian group, with the point at infinity serving as an identity element, along with the group operation of elliptic curves. The group's structure is derived from the underlying algebraic variety's divisor group in Eq. (12),

$$\text{Div}^0(E) \rightarrow \text{Pic}^0(E) \cong E. \quad (12)$$

The capacity to compute a point multiplication and the inability to compute the multiplicand given the original point and product point are prerequisites for the security of ECC. The problem's difficulty is determined by the size of the elliptic curve, which is expressed as the total number of discrete integer pairs that meet the curve equation. ECC's main advantage over other methods such as convention cryptographies is that it promises reduced key sizes, which means less storage and transmission power needs. For instance, the security of a 3072-bit convention cryptographies public key should be equivalent to that of a 256-bit elliptic curve public key. The second phase divides the 64 bits to the right and 64 bits to the left into 4-bit pieces. After the division, for every four bits, a shift row is created, and the f-function receives the output of the shifting.

ECC offers compact solutions for security, which lead to faster cryptographic operations even with smaller key sizes. Key creation is done using the ECC encryption and Diffie–Hellman exchange, which performs the key exchange. The data is encrypted and decrypted. As of right now, there are numerous varieties of PKC, including conventional cryptography. ECC is one of them; it's a straightforward method of encrypting and decrypting data for a limited group of authorized users. ECC encrypts and decrypts data using two keys—the public and private keys—so that encrypted data cannot be readily hacked or read +during transmission. This study's core algorithm is displayed below. After generating 128 bits for the ECC, the bit values are transformed into hexadecimal values. As shown, the f-function was divided into four parts, each of four bits (16 bits). As explained in Eq. (13), substitution can be generated for the encryption key (Kc) via the f-function.

$$Kb_i \text{ f} = \| 5 \text{ (j = 1) } K_{c^{4(j-1)+i}} \quad (13)$$

When $l = 5$, then Eq. (13) has been changed in the form of Eq. (14),

$$Ka_i \text{ f} = \text{f}(b_i \text{ f}). \quad (14)$$

Each f-function in the output is produced from a single, 16-bit matrix, 4×4 . Additionally, two keys

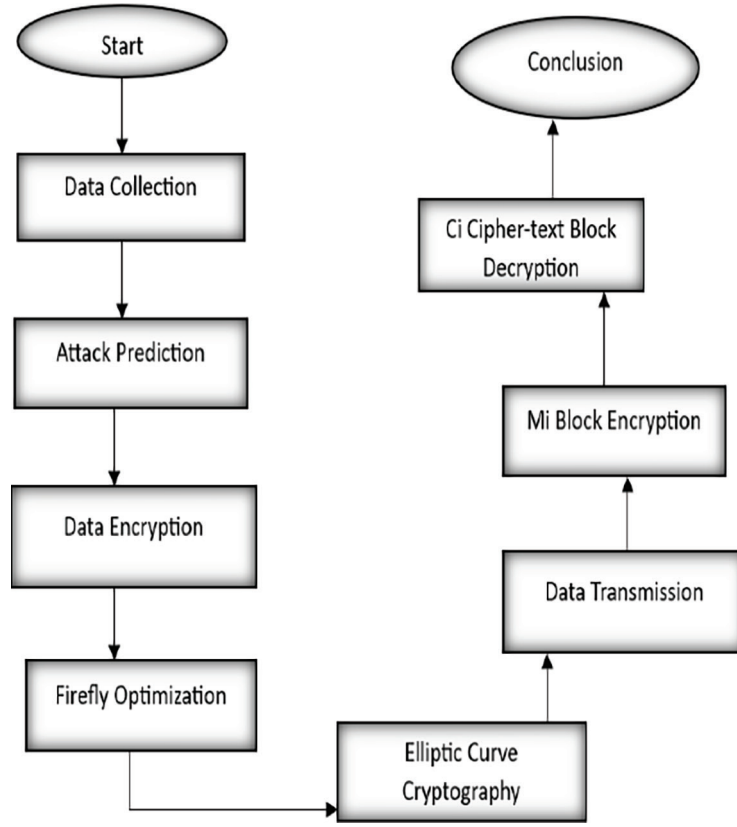


Figure 2: Flowchart of the proposed framework.

would be produced throughout this process based on the user-inputted seed. The user transmits the first key, which is used during the decryption process. The values R_0 (64 bits) and L_0 (64 bits) together form the 128-bit encryption key (K_c). Subsequently, if $RM = 0$ and $Cr - R[M] = 0$, the corresponding cryptographic operation is performed as defined in the proposed algorithm. Figure 2 illustrates the flowchart of the proposed work.

Sending digital or analog data to one or more computing, network, communication or electronic devices via a communication medium is known as data transmission [32]. Device transfer and communication in point-to-point, point-to-multipoint and multipoint-to-multipoint environments are made possible by it. Both digital and analog data can be transmitted; however, digital data are often sent and received. It functions when a computer or other equipment wants to deliver a file or data item to one or more receiver devices, such as another computer or server. Discrete signals or digital bit streams are the form in which the digital data emanates from the source device. To get to the destination or receiver device, these data streams or signals are sent over

a communication medium, such as actual copper wires, wireless carriers or optical fiber. Furthermore, baseband or passband can be used for each outgoing signal. The encrypted key will be taken from the key that the user sent throughout the decryption procedure. The steps involved is described. The 128-bit encryption key is divided into two 64-bit segments, R_0 and L_0 , which are merged to generate K_1 , the 128-bit decryption key.

The Mi block encryption technique and the Ci ciphertext block decryption process employ the same computing process. The 128-bit Ci block is divided into four sub-blocks before being processed using mixed Exclusive OR (XOR) and suboperations with the same working keys. Furthermore, there would be no need to write out the exact steps for the method because they are the opposite of the encryption operation.

Algorithm 1: Secure, Lightweight, and Energy-Efficient IoT Framework for Smart Agriculture

Input

Sensor nodes $S = \{s_1, s_2, \dots, s_n\}$

Gateway node G

Cloud server C

Cryptographic parameters (ECC keys, hash functions)

Lightweight encryption parameters

Output

Secure, authenticated, and energy-efficient transmission of agricultural sensor data

Detection of malicious activities

Algorithm Steps

Step 1: Sensor Initialization

Deploy IoT sensors in the agricultural field.

Initialize each sensor with a unique identity ID_i and minimal cryptographic parameters.

Step 2: Lightweight Key Generation

Generate elliptic curve-based public and private keys for each sensor node.

Store only essential keys to reduce memory and energy consumption.

Step 3: Secure Data Acquisition

Sensors collect real-time agricultural parameters such as soil moisture, temperature, humidity, and crop health.

Each sensed data packet is appended with timestamp and sensor ID.

Step 4: Lightweight Encryption

Encrypt the sensed data using a lightweight encryption algorithm (e.g., TEA-based or optimized ECC-hybrid encryption).

Apply hash function to ensure data integrity.

Step 5: Authentication and Key Agreement

Perform mutual authentication between sensor nodes and gateway using ECC-based key agreement. Validate message authenticity using hash verification.

Step 6: Secure Data Transmission

Transmit encrypted data from sensors to the gateway over a public channel.

Forward verified data from gateway to cloud server.

Step 7: Intrusion Detection and Monitoring

Monitor network traffic at the gateway using a lightweight intrusion detection module. Classify traffic as normal or malicious using machine learning or rule-based analysis.

Step 8: Secure Cloud Storage

Store validated data in cloud storage using blockchain-enabled or integrity-verified data blocks.

Verify data integrity before retrieval using Merkle tree or hash comparison.

Step 9: Energy and Resource Optimization

Dynamically adjust encryption and communication parameters based on node battery level. Minimize retransmissions and computation to extend sensor lifetime.

Step 10: Alert and Response Mechanism

If an intrusion or anomaly is detected, trigger alerts to the control system.

Isolate malicious nodes and update security parameters.

End Algorithm

V. Results and Discussion

In this paper, a novel optimized lightweight cryptography framework for securing IoT-based agriculture data was created. First, the IoT agriculture database was collected and imported into the system. The framework's goal is to safely transfer the gathered data to the cloud server. The proposed methodology combines firefly encryption with ECC to encrypt the input data and prevent other parties from accessing the information. The approach was created and executed using Python version 3.7 on a 64-bit operating system. The results of the study are examined in terms of confidentiality rate, accuracy, precision, recall, f-measure, etc.

a. Performance analysis

In this section, the training and testing performances of the proposed framework are assessed in terms of accuracy and loss. This dataset is split into two containing 303,025 and 75,757 data points for training and testing purposes. The training accuracy defines how quickly the proposed algorithm learns the difference between the normal and malicious data. It measures the model's learning efficiency. The proposed DRNN algorithm achieved 0.98 accuracy over increasing epochs from 0 to 500. On the other hand, the testing accuracy measures how precisely the developed algorithm implements its understanding in unknown data samples. It measures the generalization ability of the model. The designed methodology achieved 0.96 testing accuracy over increasing epochs.

Consequently, the loss performance of the proposed methodology was assessed over increasing epochs. The training loss measures the deviation between the actual and predicted values of the system. It measures how well the developed algorithm fits the training set. The designed algorithm achieved a minimum training loss of 0.05 over increasing epochs. Consequently, the testing loss determines how precisely the developed model predicts malicious entry in unknown data samples. This measures how effectively the developed model prevents the overfitting issue. Figures 3A and 3B present the accuracy and loss performances of the developed framework in both training and testing phases. The high accuracy and minimum loss validate that the designed framework accurately predicts the normal and malicious data in smart agriculture.

b. Comparative analysis

In order to demonstrate the created model's performance, it is contrasted with certain traditional security models, such as IoT-blockchain light-weight cryptographic (IBLWC) [33], ECC [34], symmetric key cryptography (SKC) [35], enhanced energy-efficient lightweight cryptography method (E3LCM) [36], blockchain enabled secure optimal lightweight cryptography-based image encryption (BC-LWCIE) [37] and asymmetric key cryptography (AKC) [38].

a.i. Accuracy

Accuracy quantifies the overall correctness of the developed framework in identifying the normal and malicious data cases in smart agriculture. It defines

the ratio of correctly detected faults (both true positives and negatives) to the total instances, and it is expressed in Eq. (15).

$$A_{cq} = \frac{T_{pq} + T_{nq}}{T_{pq} + T_{nq} + F_{pq} + F_{nq}} \quad (15)$$

where A_{cq} defines the accuracy, T_{pq} indicates true positive, T_{nq} refers to true negative, F_{pq} indicates the false positive and F_{nq} represents false negative.

The accuracy rate earned by the proposed technique is compared with conventional security techniques such as IBLWC, ECC, SKC, E3LCM, BC-LWCIE and AKC. The IBLWC model gained 97.3%, the ECC model gained 97.9, the SKC model gained 96%, the E3LCM model gained 97.8%, the BC-LWCIE model gained 97.3% and the AKC model gained 97% for the 100 kb data size. The designed proposed model achieved accuracy of 99%, 98.67%, 98.4%, 98.1%, 97.9% and 97.75% for 100 kb, 150 kb, 200 kb, 250 kb, 300 kb and 350 kb data rates. The developed model achieved a higher confidentiality rate of 99%, which is high compared to the existing techniques. This demonstrates that the proposed security model enhances the data confidentiality rate more than the existing techniques. The comparison of accuracy is shown in Figure 4.

The numerical comparison of the accuracy values for the proposed and existing methods is presented in Table 3.

a.ii. Precision

Precision indicates the model's capacity to correctly identify true positive instances among the total

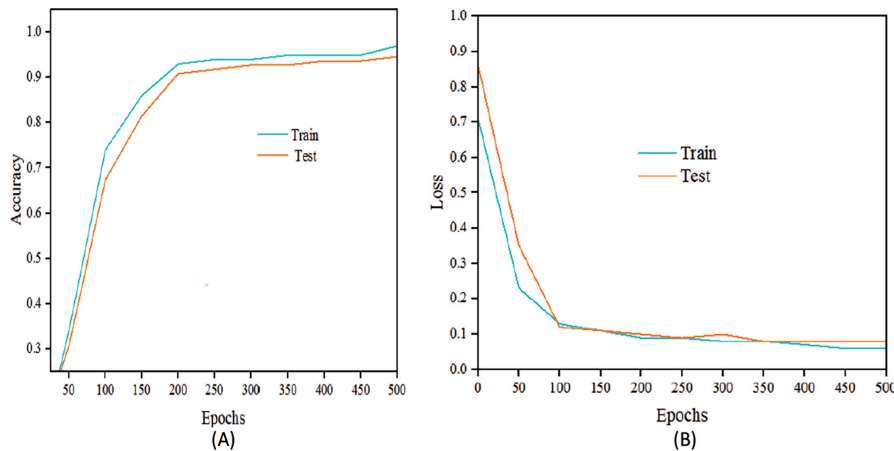


Figure 3: Performance analysis: (A) Accuracy, (B) loss.

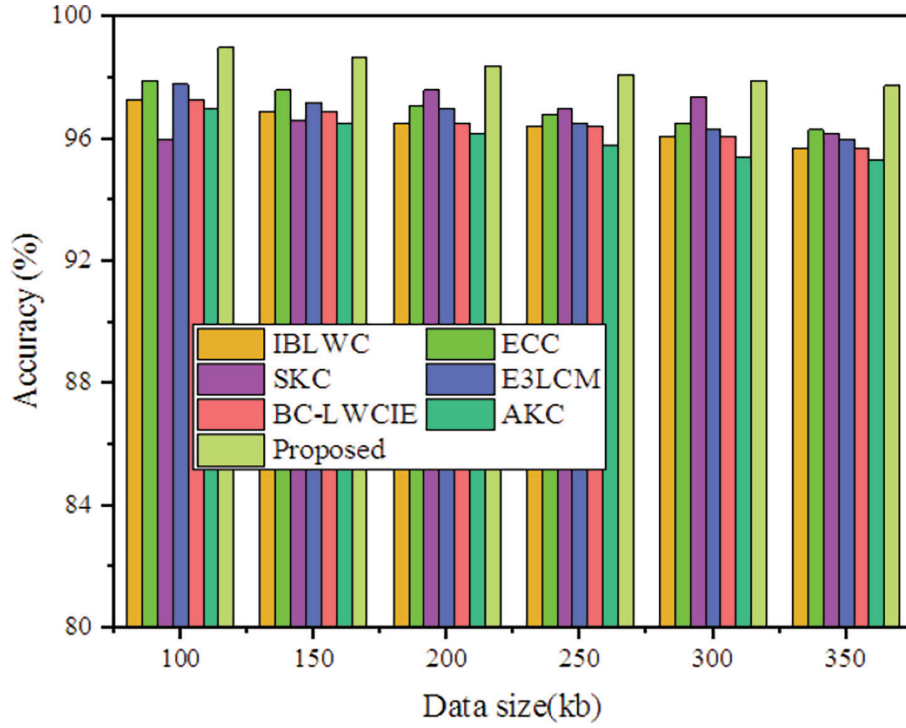


Figure 4: Comparison of accuracy. AKC, asymmetric key cryptography; BC-LWCIE, blockchain-enabled secure optimal lightweight cryptography-based image encryption; E3LCM, enhanced energy-efficient lightweight cryptography method; ECC, elliptic curve cryptography; IBLWC, IoT-blockchain light-weight cryptographic; SKC, symmetric key cryptography.

Table 3: Comparison of accuracy

Data size (kb)	IBLWC	ECC	SKC	E3LCM	BC-LWCIE	AKC	Proposed
100	97.3	97.9	96	97.8	97.3	97	99
150	96.9	97.6	96.6	97.2	96.9	96.5	98.67
200	96.5	97.1	97.6	97	96.5	96.2	98.4
250	96.4	96.8	97	96.5	96.4	95.8	98.1
300	96.1	96.5	97.4	96.3	96.1	95.4	97.9
350	95.7	96.3	96.2	96	95.7	95.3	97.75

AKC, asymmetric key cryptography; BC-LWCIE, blockchain-enabled secure optimal lightweight cryptography-based image encryption; E3LCM, enhanced energy-efficient lightweight cryptography method; ECC, elliptic curve cryptography; IBLWC, IoT-blockchain light-weight cryptographic; SKC, symmetric key cryptography.

positive instances. It measures the ratio of correctly detected attack instances to the total number of cases classified as attack by the developed framework, and it is represented in Eq. (16).

$$P_{cr} = \frac{T_{pq}}{T_{pq} + F_{pq}} \quad (16)$$

where P_{cr} defines the precision. The comparison of precision is presented in Table 4.

The precision rate earned by the proposed technique is compared with conventional security techniques such as IBLWC, ECC, SKC, E3LCM, BC-LWCIE and AKC. The IBLWC model gained 98.1%, the ECC model gained 97%, the SKC model gained 98.5%, the E3LCM model gained 97%, the

Table 4: Comparison of precision

Data size (kb)	IBLWC	ECC	SKC	E3LCM	BC-LWCIE	AKC	Proposed
100	98.1	97	98.5	97	97.7	97.8	99.3
150	97.6	96.5	98.1	96.5	97.5	97.2	98.9
200	97.4	96.2	97.7	96.2	97.2	97	98.6
250	97.1	95.8	97.3	95.8	96.9	96.5	98.5
300	96.7	95.4	97.0	95.4	96.5	96.3	98.3
350	96.5	95.3	96.8	95.3	96.1	96	98.0

AKC, asymmetric key cryptography; BC-LWCIE, blockchain-enabled secure optimal lightweight cryptography-based image encryption; E3LCM, enhanced energy-efficient lightweight cryptography method; ECC, elliptic curve cryptography; IBLWC, IoT-blockchain light-weight cryptographic; SKC, symmetric key cryptography.

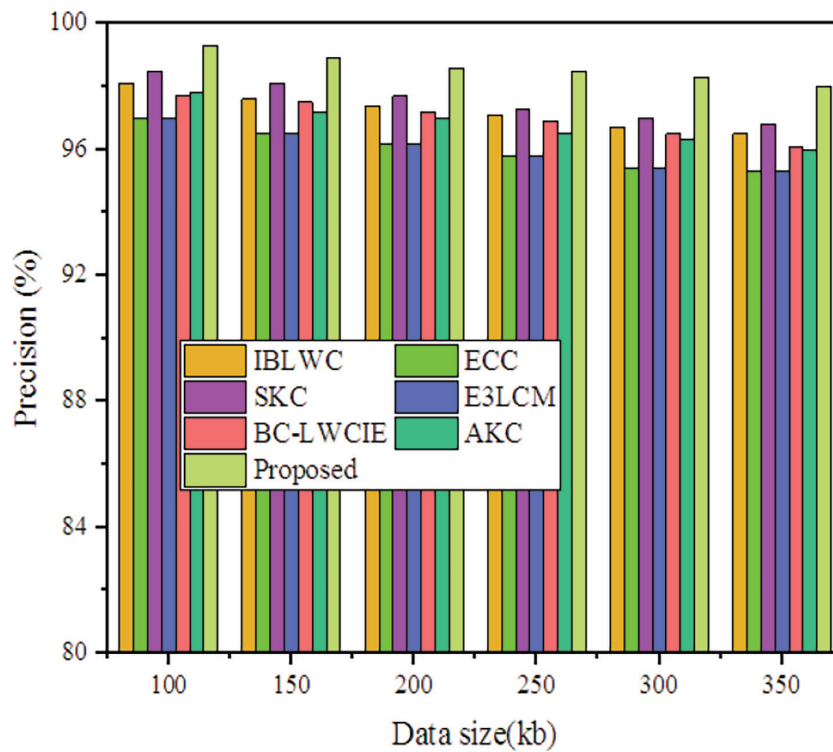


Figure 5: Comparison of precision. AKC, asymmetric key cryptography; BC-LWCIE, blockchain-enabled secure optimal lightweight cryptography-based image encryption; E3LCM, enhanced energy-efficient lightweight cryptography method; ECC, elliptic curve cryptography; IBLWC, IoT-blockchain light-weight cryptographic; SKC, symmetric key cryptography.

BC-LWCIE model gained 97.7% and the AKC model gained 97.7% for the 100 kb data size. The designed proposed model achieved accuracy of 99.3%, 98.9%, 98.6%, 98.5%, 98.3% and 98% for 100 kb, 150 kb, 200 kb, 250 kb, 300 kb and 350 kb data rates. The developed model achieved a greater precision rate of 99.3%, which is high compared to the existing techniques. This demonstrates that the proposed security

model enhances the data precision rate more than the existing techniques. The comparison of precision is shown in Figure 5.

a.iii. Recall

Recall indicates the ratio of correctly predicted abnormal traffic instances among the real abnormal traffic

instances. It quantifies the system's ability to identify all attack cases. Also, it measures the model's effectiveness in capturing all relevant instances for precise detection of attacks, and it is mathematically expressed in Eq. (17).

$$R_{cl} = \frac{T_{pq}}{T_{pq} + F_{nq}} \quad (17)$$

where R_{cl} denotes the recall. The comparison of recall is presented in Table 5.

The recall rate earned by the proposed technique is compared with conventional security techniques such as IBLWC, ECC, SKC, E3LCM, BC-LWCIE and AKC. The IBLWC model gained 98.1%, the ECC model gained 97.2%, the SKC model gained 98%, the E3LCM model gained 96%, the BC-LWCIE model gained 97.3% and the AKC model gained 97.2% for

Table 5: Comparison of recall

Data size (kb)	IBLWC	ECC	SKC	E3LCM	BC-LWCIE	AKC	Proposed
100	98.1	97.2	98	96	97.3	97.2	99.7
150	97.6	96.5	98.1	96.5	97.5	97.2	99
200	97.4	96.2	97.7	96.2	97.2	97	98.9
250	97	95.8	97	95.8	96.9	96.5	98.2
300	96.4	95	97	94.4	96.5	96	98.3
350	96.5	95	96.8	95.4	96.2	96	98

AKC, asymmetric key cryptography; BC-LWCIE, blockchain-enabled secure optimal lightweight cryptography-based image encryption; E3LCM, enhanced energy-efficient lightweight cryptography method; ECC, elliptic curve cryptography; IBLWC, IoT-blockchain light-weight cryptographic; SKC, symmetric key cryptography.

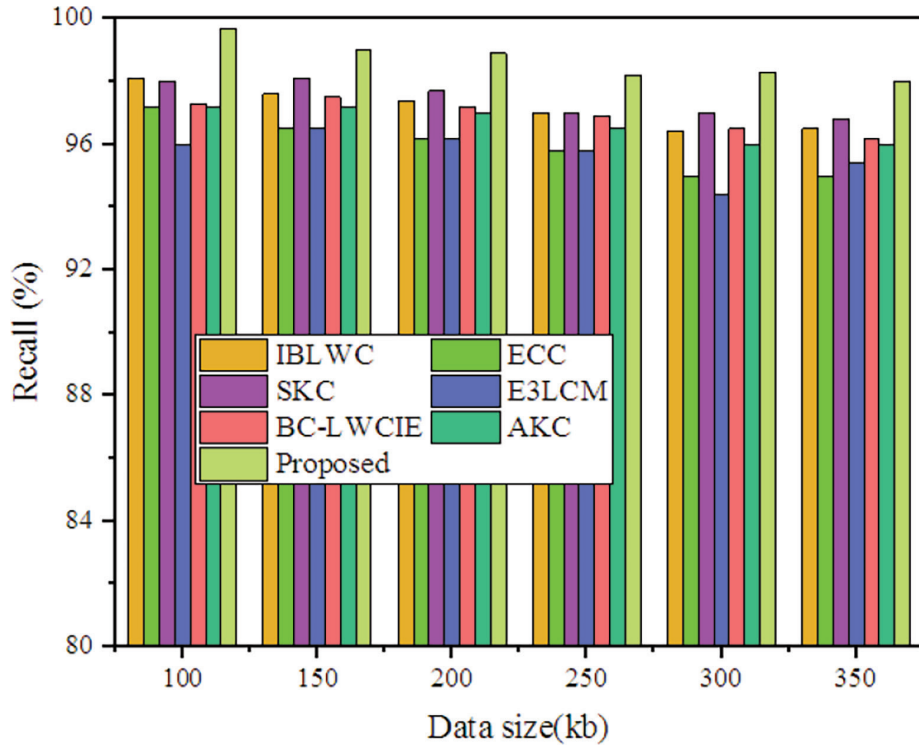


Figure 6: Comparison of recall. AKC, asymmetric key cryptography; BC-LWCIE, blockchain-enabled secure optimal lightweight cryptography-based image encryption; E3LCM, enhanced energy-efficient lightweight cryptography method; ECC, elliptic curve cryptography; IBLWC, IoT-blockchain light-weight cryptographic; SKC, symmetric key cryptography.

the 100 kb data size. The designed proposed model achieved accuracy of 99.7%, 99%, 98.9%, 98.2%, 98.3% and 98% for 100 kb, 150 kb, 200 kb, 250 kb, 300 kb and 350 kb data rates. The developed model achieved a greater recall rate of 99.7%, which is high compared to the existing techniques. This demonstrates that the proposed security model enhances the data confidentiality rate more than the existing techniques. The comparison of recall is shown in Figure 6.

a.iv. F-measure

F-measure represents the harmonic mean of both precision and recall parameters. It offers balanced performance of the system in detecting the attacks in smart agriculture by considering both positive and negative instances, and it is calculated using Eq. (18).

$$F_m = 2 \left(\frac{R_{cl} \times P_{cr}}{R_{cl} + P_{cr}} \right) \quad (18)$$

Table 6: Comparison of F-measure

Data size (kb)	IBLWC	ECC	SKC	E3LCM	BC-LWCIE	AKC	Proposed
100	97.3	97.1	96	98.1	97.7	97.4	98.5
150	97.0	96.7	98.1	97.6	97.5	97.2	98.3
200	96.8	96.5	95	95.4	97.5	96	98.0
250	97.3	97.1	95	97.8	97.9	97.3	99
300	96.5	95	95.4	97.2	97.6	96.9	98.67
350	95	95	95	97	97.1	96.5	98.4

AKC, asymmetric key cryptography; BC-LWCIE, blockchain-enabled secure optimal lightweight cryptography-based image encryption; E3LCM, enhanced energy-efficient lightweight cryptography method; ECC, elliptic curve cryptography; IBLWC, IoT-blockchain light-weight cryptographic; SKC, symmetric key cryptography.

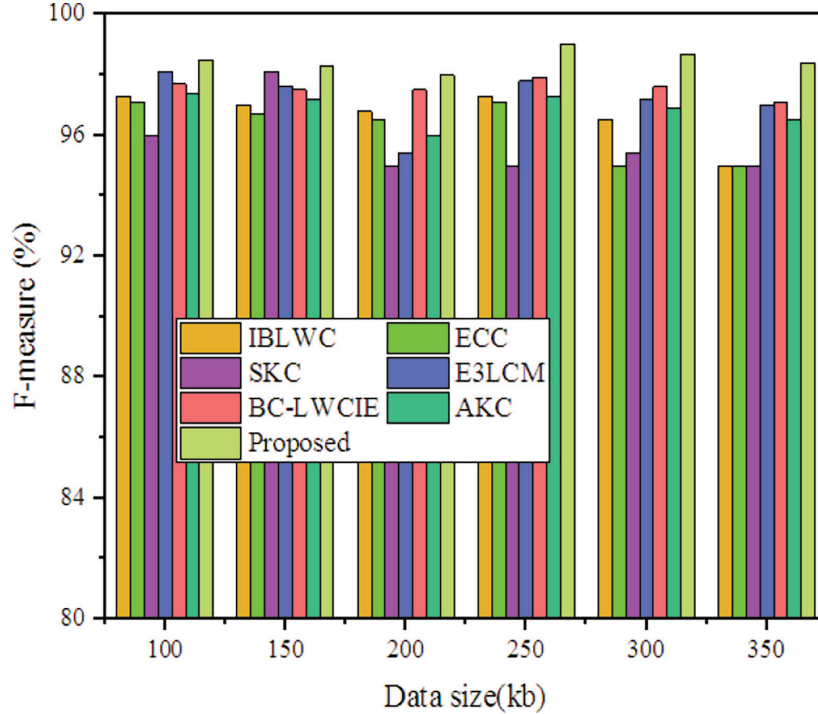


Figure 7: Comparison of F-measure. AKC, asymmetric key cryptography; BC-LWCIE, blockchain-enabled secure optimal lightweight cryptography-based image encryption; E3LCM, enhanced energy-efficient lightweight cryptography method; ECC, elliptic curve cryptography; IBLWC, IoT-blockchain light-weight cryptographic; SKC, symmetric key cryptography.

where F_m represents the F-measure. The comparison of F-measure is presented in Table 6.

The F-measure rate earned by the proposed technique is compared with conventional security techniques such as IBLWC, ECC, AI, E3LCM, BC-LWCIE and AKC. The IBLWC model gained 98.5%, the ECC model gained 98.3%, the SKC model gained 98.0%, the E3LCM model gained 99%, the BC-LWCIE model

gained 98.67% and the AKC model gained 98.4% for the 100 kb data size. The designed proposed model achieved accuracy of 98.5%, 98.3%, 98.0%, 99%, 98.67% and 98.4% for 100 kb, 150 kb, 200 kb, 250 kb, 300 kb and 350 kb data rates. The developed model achieved a greater F-measure rate of 98.5%, which is high compared to the existing techniques. The comparison of F-measure is shown in Figure 7.

Table 7: Comparison of energy consumption

Data size (kb)	IBLWC	ECC	SKC	E3LCM	BC-LWCIE	AKC	Proposed
100	6.5	8.4	11.6	7	11.2	6	3.2
150	6	4.9	7.4	5.7	3.7	4.1	3
200	8.6	5	7.2	6.2	6.1	5	4.2
250	6	6.5	7	5.8	7.9	7	5.1
300	4.8	6	4.9	8	5	5.0	4
350	7	7.8	5.9	7.4	5.8	7	4.4

AKC, asymmetric key cryptography; BC-LWCIE, blockchain-enabled secure optimal lightweight cryptography-based image encryption; E3LCM, enhanced energy-efficient lightweight cryptography method; ECC, elliptic curve cryptography; IBLWC, IoT-blockchain light-weight cryptographic; SKC, symmetric key cryptography.

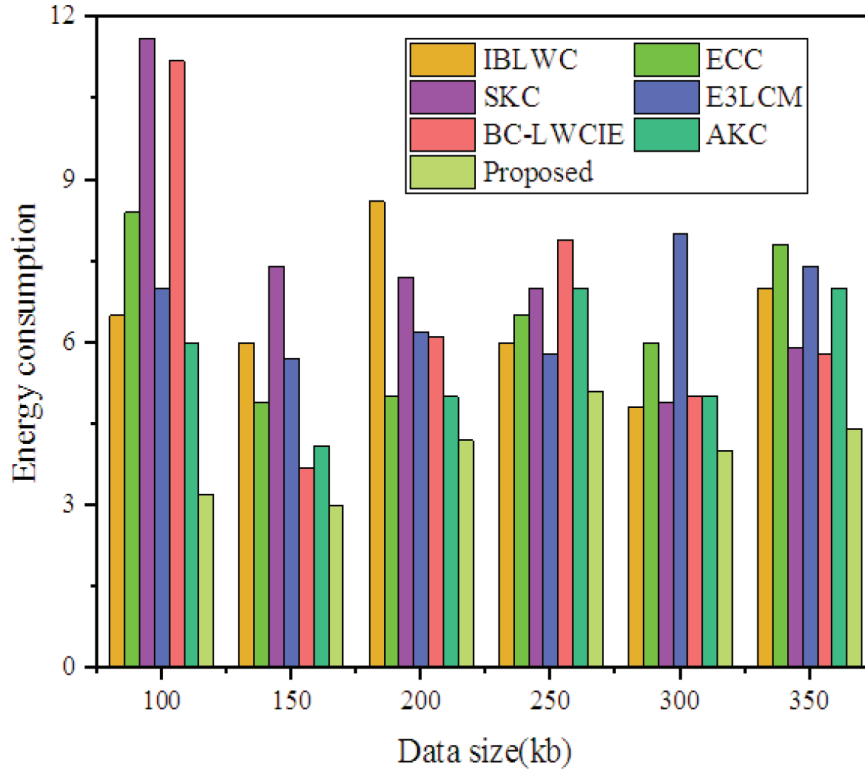


Figure 8: Comparison of energy consumption. AKC, asymmetric key cryptography; BC-LWCIE, blockchain-enabled secure optimal lightweight cryptography-based image encryption; E3LCM, enhanced energy-efficient lightweight cryptography method; ECC, elliptic curve cryptography; IBLWC, IoT-blockchain light-weight cryptographic; SKC, symmetric key cryptography.

a.v. Energy consumption

The gained energy consumption of the developed lightweight cryptography model results is validated with other prevailing techniques such as IBLWC, ECC,

SKC, E3LCM, BC-LWCIE and AKC. The comparison of energy consumption is presented in Table 7.

The existing model required a large energy consumption to execute the process compared to the proposed technique. The IBLWC model

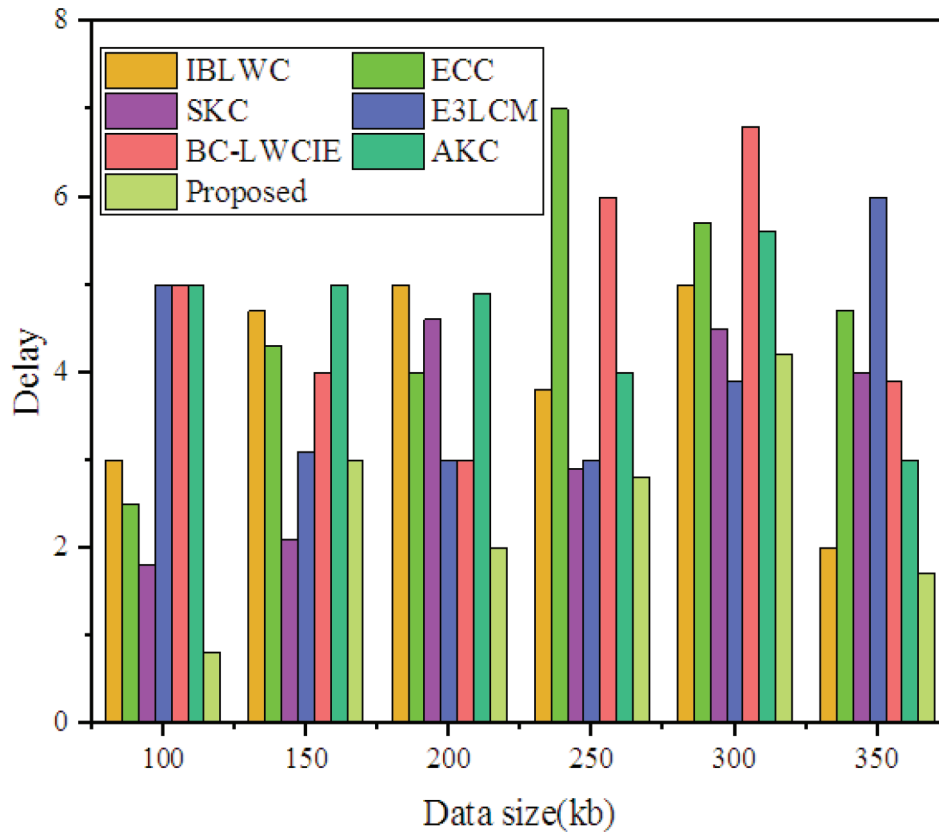


Figure 9: Comparison of delay. AKC, asymmetric key cryptography; BC-LWCIE, blockchain-enabled secure optimal lightweight cryptography-based image encryption; E3LCM, enhanced energy-efficient lightweight cryptography method; ECC, elliptic curve cryptography; IBLWC, IoT-blockchain light-weight cryptographic; SKC, symmetric key cryptography.

Table 8: Comparison of delay

Data size (kb)	IBLWC	ECC	SKC	E3LCM	BC-LWCIE	AKC	Proposed
100	3	2.5	1.8	5	5	5	0.8
150	4.7	4.3	2.10	3.10	4	5	3
200	5	4	4.6	3	3.0	4.9	2.0
250	3.8	7	2.9	3	6	4.0	2.8
300	5	5.7	4.5	3.9	6.8	5.6	4.2
350	2	4.7	4	6	3.9	3	1.7

AKC, asymmetric key cryptography; BC-LWCIE, blockchain-enabled secure optimal lightweight cryptography-based image encryption; E3LCM, enhanced energy-efficient lightweight cryptography method; ECC, elliptic curve cryptography; IBLWC, IoT-blockchain light-weight cryptographic; SKC, symmetric key cryptography.

gained 6.5 mJ, the ECC technique gained 8.4 mJ, the SKC model reached 11.6 mJ, the E3LCM technique reached 7 mJ to secure the data, the BC-LWCIE technique reached 11.2 mJ and the AKC technique reached 6 mJ to secure the data.

Finally, the developed method required an energy consumption of 3.2 mJ for securing the data. The developed model needs less energy consumption. The comparison of energy consumption is shown in Figure 8.

Table 9: Comparison of time consumption

Data size (kb)	IBLWC	ECC	SKC	E3LCM	BC-LWCIE	AKC	Proposed
100	5	2.7	3	4.5	5	4	2
150	8.6	5	7.2	6.2	6.1	5	4.2
200	6	6.5	7	5.8	7.9	7	5.1
250	8.6	5	7.2	6.2	6.1	5	4.2
300	6	6.5	7	5.8	7.9	7	5.1
350	6.5	8.4	11.6	7	11.2	6	3.2

AKC, asymmetric key cryptography; BC-LWCIE, blockchain-enabled secure optimal lightweight cryptography-based image encryption; E3LCM, enhanced energy-efficient lightweight cryptography method; ECC, elliptic curve cryptography; IBLWC, IoT-blockchain light-weight cryptographic; SKC, symmetric key cryptography.

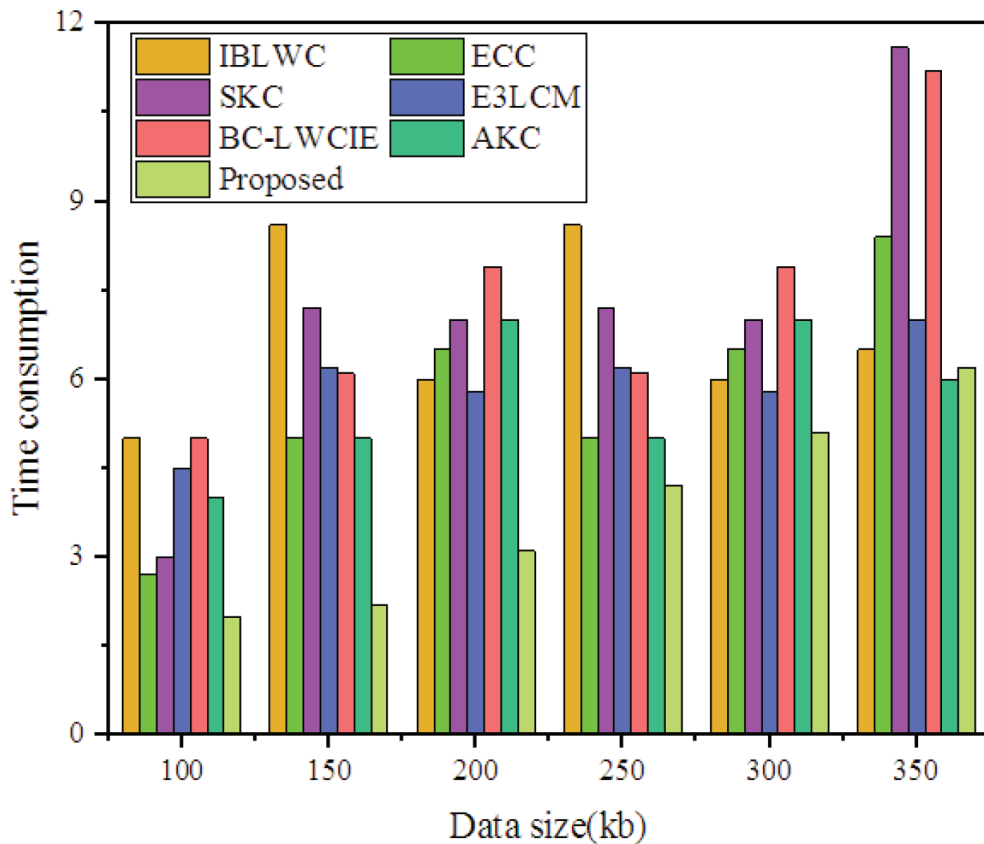


Figure 10: Comparison of time consumption. AKC, asymmetric key cryptography; BC-LWCIE, blockchain-enabled secure optimal lightweight cryptography-based image encryption; E3LCM, enhanced energy-efficient lightweight cryptography method; ECC, elliptic curve cryptography; IBLWC, IoT-blockchain light-weight cryptographic; SKC, symmetric key cryptography.

a.vi. Delay

The gained delay of the developed Lightweight cryptography model results is validated with other prevailing techniques such as IBLWC, ECC, SKC, E3LCM, BC-LWCIE and AKC. The comparison of delay is presented in Table 8.

The existing model required a large delay rate to execute the process compared to the proposed technique. The IBLWC model gained 3 s, the ECC technique gained 2.5 s, the SKC model reached 1.8 s, the E3LCM technique reached 5 s, the BC-LWCIE technique reached 5 s and the AKC technique reached 5 s to secure the data. Finally, the developed method

Table 10: Comparison of data confidentiality rate

Data size (kb)	IBLWC	ECC	SKC	E3LCM	BC-LWCIE	AKC	Proposed
100	0.94	0.97	0.95	0.97	0.96	0.97	0.98
150	0.93	0.95	0.96	0.93	0.94	0.96	0.97
200	0.90	0.94	0.93	0.92	0.94	0.94	0.95
250	0.92	0.93	0.92	0.93	0.92	0.93	0.94
300	0.96	0.93	0.95	0.95	0.96	0.95	0.97
350	0.92	0.91	0.93	0.94	0.90	0.94	0.96

AKC, asymmetric key cryptography; BC-LWCIE, blockchain-enabled secure optimal lightweight cryptography-based image encryption; E3LCM, enhanced energy-efficient lightweight cryptography method; ECC, elliptic curve cryptography; IBLWC, IoT-blockchain light-weight cryptographic; SKC, symmetric key cryptography.

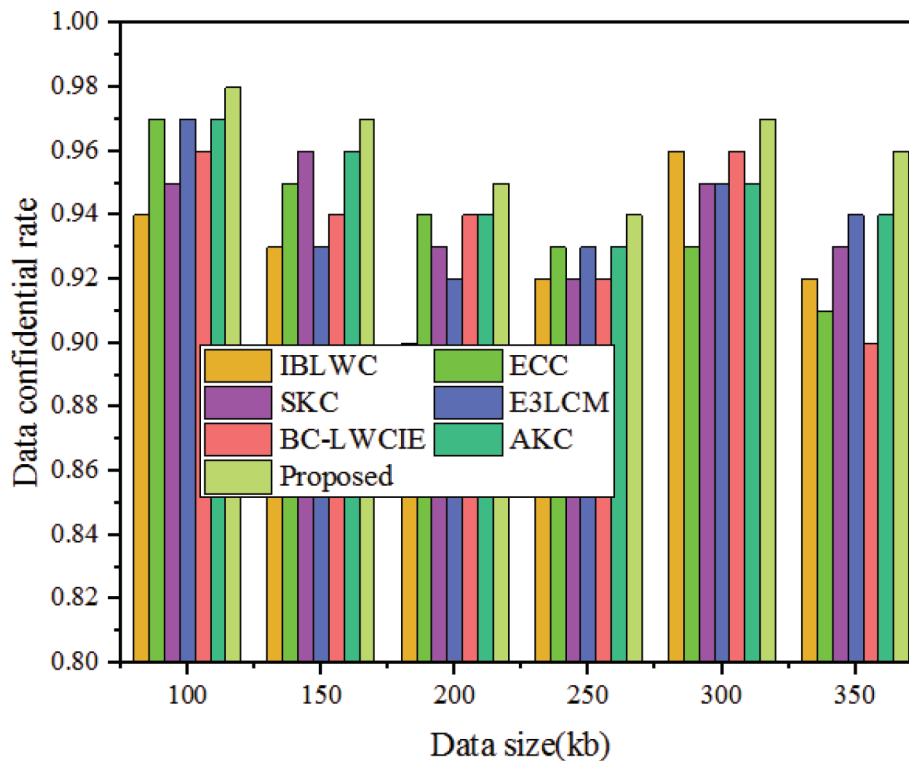


Figure 11: Comparison of data confidentiality rate. AKC, asymmetric key cryptography; BC-LWCIE, blockchain-enabled secure optimal lightweight cryptography-based image encryption; E3LCM, enhanced energy-efficient lightweight cryptography method; ECC, elliptic curve cryptography; IBLWC, IoT-blockchain light-weight cryptographic; SKC, symmetric key cryptography.

required a delay rate of 0.8 s for securing the data. The developed model needs a lower delay rate. The comparison of delay is shown in Figure 9.

a.vii. Time consumption

The gained time consumption of the developed lightweight cryptography model results is validated with other prevailing techniques such as IBLWC, ECC, SKC, E3LCM, BC-LWCIE and AKC. The comparison of time consumption is presented in Table 9.

The existing model required a large amount of time to execute the process when compared to the proposed technique. The IBLWC model gained 5 s, the ECC technique gained 2.7 s, the SKC model reached 3 s and the E3LCM technique reached 4.5 s. The BC-LWCIE model gained 5 s. The AKC model gained 4 s to secure the edge AI system. Finally, the developed method required a time consumption of 2 s for securing the data. It needs less time and saves energy consumption. The comparison of time consumption is shown in Figure 10.

a.viii. Data confidentiality rate

The data confidentiality rate is defined as the rate at which the proposed model protects the agriculture dataset from unauthorized usage. The confidentiality rate achieved by the proposed model is evaluated with the existing techniques. The comparison of data confidentiality rate is presented in Table 10.

The confidentiality rate earned by the proposed technique is compared with conventional security techniques such as IBLWC, ECC, SKC, E3LCM, BC-LWCIE and AKC. The confidentiality rate attained by these techniques is 0.88, 0.89, 0.91, 0.73, 0.75 and 0.84, respectively. The developed model achieved a higher confidentiality rate of 0.98, which is high compared to the existing techniques. This demonstrates that the proposed security model enhances the data confidentiality rate more than the existing techniques. The comparison of the data confidentiality rate is shown in Figure 11.

VI. Conclusion

This article presents a lightweight cryptography security model for securing agricultural data using Firefly optimization and elliptic curve cryptography techniques. The combination of optimization and cryptographic algorithm ensures robust security, data integrity and confidentiality. Metaheuristic algorithms

are optimization algorithms that try to improve the quality of solution members iteratively with some randomness properties. Most of these algorithms are inspired by biological aspects. Further, the Firefly algorithm is a bioinspired metaheuristic algorithm for optimization problems. A method to PKC known as ECC is based on the algebraic structure of elliptic curves over finite fields. The small deviation between the performances in before- and after-attack cases validates the efficiency of the model. Finally, a comparative assessment was performed with existing techniques such as IBLWC, ECC, SKC, E3LCM, BC-LWCIE and AKC. The comparative analysis demonstrates that in the proposed model, the performance metrics such as energy consumption, time consumption and data confidentiality rate are reduced, respectively. Thus, the proposed technique provides the highest level of security to the IoT-based agriculture systems and enhances the system's performance.

a. Future scope

Future studies may integrate advanced machine learning and deep learning models capable of detecting evolving and multi-vector cyberattacks beyond traditional threats such as DDoS. Training IDS using real-time agricultural datasets can enhance generalization and robustness. Additionally, secure cloud and edge-based data analytics should be investigated to protect sensitive agricultural data during storage, processing and sharing. Combining edge computing with privacy-preserving techniques such as federated learning can reduce latency and data exposure risks. Finally, real-world implementation and field-level validation of proposed security models in diverse agricultural environments is crucial to evaluate practicality, cost-effectiveness and long-term reliability, thereby facilitating large-scale adoption of secure smart agriculture systems.

Compliance with Ethical Standards

Conflict of Interest

The authors declare that they have no conflict of interest.

Human and Animal Rights

This article does not contain any studies with human or animal subjects performed by any of the authors.

Ethical Approval

This article does not contain any studies involving human participants or animals performed by any of the authors.

Informed Consent

Not applicable.

Funding

Not applicable.

Conflicts of Interest Statement

Not applicable.

Consent to Participate

Not applicable.

Consent for Publication

Not applicable.

Availability of Data and Material

Data sharing is not applicable to this article as no new data were created or analyzed in this study.

Code Availability

Not applicable

Competing Interests

Not applicable

References

- [1] Ru, Y., Blankespoor, B., Wood-Sichra, U., Thomas, T. S., You, L., & Kalvelagen, E. (2023). Estimating local agricultural gross domestic product (AgGDP) across the world. *Earth System Science Data*, 15(3), 1357-1387.
- [2] Prakash, Chander, et al. "Advancements in smart farming: A comprehensive review of IoT, wireless communication, sensors, and hardware for agricultural automation." *Sensors and Actuators A: Physical* (2023): 114605.
- [3] Zhang, Qingqing, Yanbo Qu, and Lingyun Zhan. "Great transition and new pattern: Agriculture and rural area green development and its coordinated relationship with economic growth in China." *Journal of Environmental Management* 344 (2023): 118563.
- [4] Pathmudi, Vivek Ramakant, et al. "A systematic review of IoT technologies and their constituents for smart and sustainable agriculture applications." *Scientific African* (2023): e01577.
- [5] Morchid, A., El Alami, R., Raetzah, A. A., & Sabbar, Y. (2023). Applications of internet of things (IoT) and sensor technology to increase food security and agricultural Sustainability: Benefits and challenges. *Ain Shams Engineering Journal*, 102509.
- [6] Sathiya, S., Cecil Antony, and Praveen Kumar Ghodke. "Smart Agriculture: Emerging and Future Farming Technologies." *Recent Trends and Best Practices in Industry 4.0* (2023): 135-181.
- [7] Liu, Ye, et al. "From Industry 4.0 to Agriculture 4.0: Current status, enabling technologies, and research challenges." *IEEE Transactions on Industrial Informatics* 17.6 (2020): 4322-4334.
- [8] Rajak, P., Ganguly, A., Adhikary, S., & Bhattacharya, S. (2023). Internet of Things and smart sensors in agriculture: Scopes and challenges. *Journal of Agriculture and Food Research*, 14, 100776.
- [9] Nayak, Padmalaya, Kayiram Kavitha, and Ch Mallikarjuna Rao. "IoT-enabled agricultural system applications, challenges and security issues." *IoT and analytics for agriculture* (2020): 139-163.
- [10] Gupta, M., Abdelsalam, M., Khorsandroo, S., & Mittal, S. (2020). Security and privacy in smart farming: Challenges and opportunities. *IEEE access*, 8, 34564-34584.
- [11] Rudrakar, Santoshi, and Parag Rughani. "IoT based agriculture (Ag-IoT): A detailed study on architecture, security and forensics." *Information Processing in Agriculture* (2023).
- [12] Mekdad, Y., Aris, A., Babun, L., El Fergougui, A., Conti, M., Lazzeretti, R., & Uluagac, A. S. (2023). A survey on security and privacy issues of UAVs. *Computer Networks*, 224, 109626.
- [13] Jena, Lopamudra, et al. "Unlocking Potential of Dryland Horticulture in Climate-Resilient Farming." *Enhancing Resilience of Dryland Agriculture Under Changing Climate: Interdisciplinary and Convergence Approaches*. Singapore: Springer Nature Singapore, 2023. 343-382.
- [14] Devi, T., et al. "A-Based Weather Forecasting System for Smart Agriculture System Using a Recurrent Neural Networks (RNN) Algorithm." *Sustainable Management of Electronic Waste* (2024): 97-112.

- [15] Rudrakar, Santoshi, and Parag Rughani. "IoT based agriculture (Ag-IoT): A detailed study on architecture, security and forensics." *Information Processing in Agriculture* (2023).
- [16] Chen, H., Liu, J., Wang, J., & Xun, Y. (2023). Towards secure intra-vehicle communications in 5G advanced and beyond: Vulnerabilities, attacks and countermeasures. *Vehicular Communications*, 39, 100548.
- [17] Makhdoom, I., Abolhasan, M., Franklin, D., Lipman, J., Zimmermann, C., Piccardi, M., & Shariati, N. (2023). Detecting compromised IoT devices: Existing techniques, challenges, and a way forward. *Computers & Security*, 132, 103384.
- [18] Thabit, F., Can, O., Aljahdali, A. O., Al-Gaphari, G. H., & Alkhzaimi, H. A. (2023). A Comprehensive Literature Survey of Cryptography Algorithms for Improving the IoT Security. *Internet of Things*, 100759.
- [19] Abikoye, Oluwakemi Christiana, et al. "Securing critical user information over the internet of medical things platforms using a hybrid cryptography scheme." *Future Internet* 15.3 (2023): 99.
- [20] Zhao, Junfang, Dongsheng Liu, and Ruixi Huang. "A Review of Climate-Smart Agriculture: Recent Advancements, Challenges, and Future Directions." *Sustainability* 15.4 (2023): 3404.
- [21] Awotunde, J. B., Brahma, B., Adeniyi, A. E., Lauretta Nkoneyasua, E., Imoize, A. L. & Mejdoub, Y. (2024). An enhanced hybrid cryptography model for online banking authentication and security. In *International Conference on Connected Objects and Artificial Intelligence* (pp. 287-293). Cham: Springer Nature Switzerland.
- [22] Itoo, S., Khan, A. A., Ahmad, M., & Idrisi, M. J. (2023). A Secure and Privacy-Preserving Lightweight Authentication and Key Exchange Algorithm for Smart Agriculture Monitoring System. *IEEE Access*.
- [23] Itoo, S., Baksh, R., Som, L. K., Ahmad, M. & Masoodi, F. S. (2025). Enhancing medical data protection with a resilient ECC and blockchain authentication framework. *Information Security Journal: A Global Perspective*, 34(6), pp. 616-632.
- [24] Song, Qingling, Lang Li, and Xiantong Huang. "LELBC: A low energy lightweight block cipher for smart agriculture." *Internet of Things* 25 (2024): 101022.
- [25] Pan, F., Jiang, Y., Wen, H., Liao, R. & Xu, A. (2017). September. Physical layer security assisted 5G network security. In *2017 IEEE 86th Vehicular Technology Conference (VTC-Fall)* (pp. 1-5). IEEE.
- [26] Zhao, Yingding, et al. "Agricultural IoT Data Storage Optimization and Information Security Method Based on Blockchain." *Agriculture* 13.2 (2023): 274.
- [27] Berguiga, A., Harchay, A., Massaoudi, A., Aayed, M. B., & Belmabrouk, H. (2023). GMLP-IDS: A Novel Deep Learning-Based Intrusion Detection System for Smart Agriculture. *Computers, Materials & Continua*, 77(1).
- [28] Chibuike, L. U., Kelechi, D. A., Onukwugha, C. G., & Daniel, A. N. (2023). IoT Applications in Agriculture: Impacts and Challenges (A Review). *University of Ibadan Journal of Science and Logics in ICT Research*, 9(1).
- [29] Kethineni, Keerthi, and Pradeepini Gera. "IoT-Based Privacy-Preserving Anomaly Detection Model for Smart Agriculture." *Systems* 11.6 (2023): 304.
- [30] Gulbarga, Mohammad Imtiyaz, et al. "Deep Learning (DL) Dense Classifier with Long Short-Term Memory Encoder Detection and Classification against Network Attacks." *2023 17th International Conference on Electronics Computer and Computation (ICECCO)*. IEEE, 2023.
- [31] Malik, Naveed Ahmed, Naveed Ishtiaq Chaudhary, and Muhammad Asif Zahoor Raja. "Firefly Optimization Heuristics for Sustainable Estimation in Power System Harmonics." *Sustainability* 15.6 (2023): 4816.
- [32] Ullah, Shamsher, et al. "Elliptic Curve Cryptography; Applications, challenges, recent advances, and future trends: A comprehensive survey." *Computer Science Review* 47 (2023): 100530.
- [33] Abed, S. E., Jaffal, R., Mohd, B. J., & Al-Shayegi, M. (2021). An analysis and evaluation of lightweight hash functions for blockchain-based IoT devices. *Cluster Computing*, 24, 3065-3084.
- [34] Majumder, Suman, et al. "ECC-CoAP: Elliptic curve cryptography based constraint application protocol for internet of things." *Wireless Personal Communications* 116 (2021): 1867-1896.
- [35] Feng, Y., Zhou, J., Li, J., Zhao, W., Shi, J., Shi, R., & Li, W. (2022). SKC-CCCO: an encryption algorithm for quantum group signature. *Quantum Information Processing*, 21(9), 328.
- [36] Prakasam, P., et al. "An enhanced energy efficient lightweight cryptography method for various IoT devices." *ICT Express* 7.4 (2021): 487-492.
- [37] Bhaskaran, R., et al. "Blockchain Enabled Optimal Lightweight Cryptography Based Image Encryption Technique for IIoT." *Intelligent Automation & Soft Computing* 33.3 (2022).
- [38] Cheng, Leixiao, et al. "AKC-based revocable ABE schemes from LWE assumption." *Security and Communication Networks* 2020 (2020): 1-16.
- [39] Mhaibes, H. I., Abood, M. H., & Farhan, A. K. (2022). Simple Lightweight Cryptographic Algorithm to

Secure Imbedded IoT Devices. *international journal of interactive mobile technologies*, 16(20).

[40] Goyal, T. K., Sahula, V., & Kumawat, D. (2022). Energy efficient lightweight cryptography algorithms for IoT devices. *IETE Journal of Research*, 68(3), 1722-1735.

[41] Jammula, M., Vakamulla, V. M., & Kondoju, S. K. (2022). Performance evaluation of lightweight cryptographic algorithms for heterogeneous IoT environment. *Journal of Interconnection Networks*, 22(Supp01), 2141031.

[42] Hedayati, R., & Mostafavi, S. (2022). A lightweight image encryption algorithm for secure

communications in multimedia Internet of Things. *Wireless Personal Communications*, 123(2), 1121-1143.

[43] Alicea, M., & Alsmadi, I. (2022). New and efficient lightweight cryptography algorithm for mobile and web applications. *Procedia Computer Science*, 203, 111-118.

[44] Regla, A. I., & Festijo, E. D. (2022, April). Performance analysis of light-weight cryptographic algorithms for internet of things (IOT) applications: A systematic review. In *2022 IEEE 7th International conference for Convergence in Technology (I2CT)* (pp. 1-5). IEEE.