International Journal of Engineering Trends and Technology
ISSN: 2231–5381 / https://doi.org/10.14445/22315381/IJETT-V72I1P126

Volume 72 Issue 1, 266-274, January 2024

Original Article

An Intelligence Technique based Elliptic Curve Cryptography Algorithm for Secured Communication in Networks

Ramireddy Navatejareddy[1*], M. Kavitha[1]

[1]*Department of Computer Science & Engineering, Koneru Lakshmaiah Education Foundation, Greenfields, Vaddeswaram, Andhra Pradesh, India.*

[*]*Corresponding Author : rnavateja2233@gmail.com*

Received: 05 September 2023 Revised: 11 December 2023 Accepted: 23 December 2023 Published: 07 January 2024

Abstract *- Cloud computing is a fictional extended computing application where cloud users can store their information remotely in the cloud and configure it from a common set of computer resources for high-quality sorting and convenience. Cloud computing is primarily emerging at the heart of the sensitive data cloud. Secured communication is vital in cloud computing and IoT with advanced optimization techniques. This work aims to provide a reliable and secure cloud-based communications service allowing customers to access their information dynamically. To achieve this, in this article, we advance advances in secure communications over the Adaptive Neuro-Fuzzy Inference System (ANFIS) with Chicken Swarm Optimization (CSO) and Elliptic Curve Cryptography Hellman algorithm (ACECC). At the initial stage, an intermediate database is created, and the ANFIS-CSO algorithm is implemented to manage the optimal classification of nodes from the cloud. Next, we calculate the important information based on the data gain. Finally, we spread ECC to encrypt sensitive information and investigate from databases. The investigation is conducted under the names of PSNR, MSE, and CC with the help of databases to evaluate performance. The convincing results underscore the fact that the proposed method is suitable for ensuring secure data transmission compared to existing techniques such as the Particle Swarm Optimization algorithm (PSO), Fuzzy, Whale Optimization Algorithm (WOA), Gravitational Search Algorithm (GSA), Cuckoo Search (CS) and Genetic Algorithm (GA) techniques.*

Keywords *- Elliptic curve cryptography, Chicken Swarm Optimization, Encryption, Decryption, Mean square error.*

1. Introduction

Nowadays, mobile devices are now part of our daily life. They can be used for various purposes, including making Phone calls, listening to music, and browsing the Internet. They can be used for video conferencing or online transactions [1]. Therefore, security has become a major concern when accessing wireless networks through mobile devices. A mobile user typically accesses a wireless network by connecting to the nearest network access point with a strong signal [2, 3]. These wireless connections must be authorized to block access. Mobile users can get free access to the wireless network. Due to unstable radio signals from mobile devices in power-saving mode, mobile devices may turn off when connecting to different access points [4, 5]. The need to restart when reconnecting creates a significant lag. This header increases as the mobile user surrounds the remote network, which increases line time because the remote network requires the user to be authenticated by the home network's authentication server [6].

Elliptic Curve Cryptography (ECC) computing is well known for its capabilities as enhanced encryption and labelling and is therefore enthusiastically recommended by the National Security Agency (NSA) [7].

The ECC hypothesis relies on the mathematics of elliptical loops, making it difficult to program the new logarithm of elliptical loops in an abelian bundle using reasonable tricks. ECCs are typically secure, more limited and faster than their exemplary counterparts such as Ron Reeves, Adi Shamir Leonard Adleman (RSA), and the Digital Signature Algorithm (DSA) [8, 9]. Therefore, ECC achieves zones such as confirmation, extended signature, secure correspondence and signature handling. The tests allowed in remote sensing organizations are an important issue. The confidentiality of some WSNs renders them unhelpful against bargaining power [10]. The security style of the WSN imposes many stringent requirements for the verification of various assets and organizations and attacks.

The plan of the remote sensor network for this overriding security or validation program must be powerful against attacks leading to sensor transactions and additional security concerns [11]. However, you often cannot find an effective remote security enhancement plan, which usually depends on the keys and encryption/encryption measures used. Likewise, longer cryptographic keys actually require higher baud rates, more memory, and preparation power. An incredible opportunity to create cryptographic keys is ergonomics, vulnerability to input conditions, and competence during long-term operation, which are used for a number of purposes [12].

There are many cryptographic calculations. The numerical hypothesis is central to any cryptographic technique. Each has a unique use case and solves a specific problem. This problem is evolving over time, and as it progresses, the current structure needs to be adjusted to implement this change. Portable data processing is the norm by which all advances in cryptography will be measured over the next decade [13].

Thanks to the approach of Apple Bay, Google Wallet and many other portable exchanges, they are common in most currency exchanges [14, 15]. This requires strong cryptographic calculations for the assets, not benefits, but is an important precondition for the security of more beautiful structures. Legacy conditions, with their limited assets, fuzzy selection standards, and elliptical curvature cryptography, are the most predictable crypto strategies.

In this study, we reveal how to maintain intermediate information security for IoT using the ACECC strategy. We currently make a series of information bases largely dependent on usage. In this step, we perform an ACECC calculation based on organizational information to select the ideal hub. We have already defined the collection of information for all data in order to identify personal and non-confidential data. At this point, we encrypt sensitive information using ECC and then store it with the cloud provider.

The rest of the article is structured as follows: A step-by-step explanation of the proposed system is provided in Section 2. A brief description of results and discussions can be found in Section 3. Finally, Section 5 summarizes the findings and conclusion.

2. Materials and Methods

On suggestions, we give the opportunity to store data in the cloud. Our responsibility is focused on securing the cloud with the Adaptive Neuro-Fuzzy Inference System (ANFIS) with Chicken Swarm Optimization (CSO) and Elliptic Curve Cryptography (ECC) calculation with multiple passwords. After the dataset, first create the established organization information base.Then, select the scope of the organization dataset in the cloud based on ANFISCSO calculation and define it for the cloud provider. To reduce the cost of the encryption strategy, separate the most important and insensitive data related to information retrieval.

The relevant information is then encoded using ECC calculation. Likewise, encrypted information is stored securely in the cloud. As a result, we receive application-based data. The general outline of the proposed security structure is shown in Figure 1. In (1), the formation of the main body of the road dataset is described by moving to the cloud, (2) increasing the age of the classified data, (3) the quality of the sensitive data being sent and uploaded to the cloud, and (4) includes the customer requesting and receiving the encrypted data from the cloud.

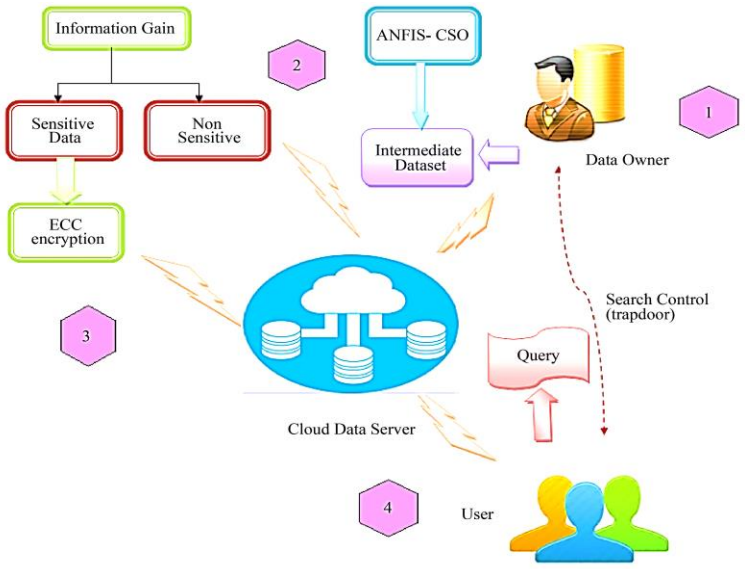

Fig. 1 Proposed architecture for preserving security in the cloud

2.1. Generation of Intermediate Dataset

Suppose the attribute size $K^D$and record count$F$ are not included in the info record Y. First, we split the dataset by N the size of the application data sequence H_i. This intermediate data is stored in the cloud service provider (CSP). CSP supporters have platforms of different sizes, and each platform has its own image.

The complexity of this list of fixtures, not the baseline estimates of use used to satisfy them later. In general, the information for every last billing run is information for every minute since some information is used as if it were for a one-time use. After using additional cycles in the information settings, they become traffic information. Thus, information that gives estimates for data or other timing information is traffic information.

An important segment of street intelligence is that we usually retrieve it when we have information about its cause. Information Sources are a type of critical metadata in workflows when conditions are associated with a dataset. The source of information is very large, as some temporary data stores will be removed after their implementation.

At this point, technicians may need to retrieve them for reuse or re-analysis. The source of information is identified to validate the current data lists of our study. We present the various main archives listed below. Make K^Da special secure entry for it. We use $H = \{H_1, H_2, \ldots, H_n\}$ a number of key recordings for communication, $K^D$where n including those with half the number of recordings.

If this is not a major issue, please be aware that the modified information contained in these advertisements may be interim and final. Directed Acyclic Graph (DAG) is used to maintain the relatively old links between these data files for a topological element.

2.1.1. Sensitive Intermediate Dataset Graph (SDG)

The era of record organization is largely characterized as a complex record Horganization K^Dchart with SIG. Despite $SDG = \langle T, S \rangle$ the fact that several interesting performances where $T = \{K^D\} \cup H$, $S$are desirable. The added field means that $(h_p, h_c)$the entire piece or location $h_c$is being created$h_p, h_c \in \{h_0\} \cup H$.

2.1.2. Sensitive Intermediate Dataset Tree (SIT)

SDGs are always like a tree, indicating a significant dataset in a tree structure. It is a tree h_0 resource. SDGs and SITs created through production links are linked to the first record and progress records. Besides, distributes sensitive data from datasets. Co-uploading different groups of information is an important tool for overcoming privacy. Currently, personal information obtained from an attacker is displayed in such a way that it can be $RQ_t(u)$separated by an s. It also augments $RQ_u(u)$ the confidential information obtained from the endless stream of each dataset in S. Many problems of theoretical significance arise from the existence of performance instructions in various ways $RQ_u(u)$.

2.2. Optimal Location Selection based on Hybrid CSO-ANFIS Technique

When creating a dataset in half, we usually save the data to the CSP. In this process, we select the optimal field for the exchange dataset in the CSP. The main rationale for using this module is to put the access tier location dataset in the best location in the cloud.

For this purpose, an Adaptive Neuro Fuzzy Inference System (ANFIS) with Chicken Swarm Optimization (CSO) was proposed. To increase the productivity of the structure, we have proposed a method that coordinates the CSO with the ANFIS system, where ANFIS is applied to the structure within the CSO.

The fuzzy chicken swarm elliptical curve is a small ECC type for invoking fuzzy chicks and a Multi-Attribute Decision Model (MADM) for basic decision-making. An essential rule of thumb for the use of dark buckwheat chickens in ECC is its ability to learn a flat cycle in standard space by coding a model in a chicken herd. A decisive achievement in constructing a soft group calculation is the breakdown and identification of the parts of the soft skeleton that need to be improved by coding the hen house calculation. The pricing of the primary option in MADM is based on questionable principles. The key is the key factor that shows the encryption time and the unsecured time. The proposed portable ACECC is designed for more limited encryption and many hours of no filtering, so sizing and keying are critical. Computational security is expanded by defining and advancing key boundaries. Limitations of the improvement include key selection, printing, instruction recovery, message encryption, and message decryption.

The vast majority of calculations focus more on printing and correcting research, and the main purpose of this article is to facilitate key decision-making. The CSO calculation is used to determine the best location for the main module. It usually mimics the mating pattern of chicken preservatives, and its food requires action.

In CSO calculations, the best fitness score is associated with the chicken and the worst health score is associated with the chicken coop. The rest of the qualities are given to a flock of chickens. The cycle for choosing the best hub is explained in the accompanying documents;

2.2.1. Steps of CSO Algorithm

Step 1: Initialize the population of N chicken x and choose a 128-cycle key phrase set for ECC.

$$x_{i,j}^{t+1} = lb + Rand(ub - lb) \quad (1)$$

With lb and ub are lower bound and upper bound of the search space. This is done to ensure that subsequent placements are in a popular region.

Step2: To determine the fitness and start the best position N_{best} t=1

$$F = Min(Key_{space}) \quad (2)$$

The closest home furnishings among the roses were chosen using the irregular age subset technique because the chick holding kit consists of a narrow set of key chains made from an elliptical ring. The primary way to use the subset generation technique is to reduce the focal space by controlling the rate of popularity.

Step 3: Assess the reasonableness of the crowd of chickens and show the hierarchy in the group. Divide the chicken sword into many subgroups and evaluate the relationship.

$$x_{i,j}^{t+1} = x_{i,j}^{t} * S1 * Rand * (x_{i,j}^{t} - x_{i,j}^{t}) + S2 * Rand * t \quad (3)$$

$$(x_{i,j}^{t} - x_{i,j}^{t}) = t \quad (4)$$

Step 4: Update the range of chickens, hens and chickens. Updates for roosters are done using the PSO calculation.

$$x_{i,j}^{t+1} = x_{i,j}^{t} * (1 + Rand(0, \sigma^2) \quad (5)$$

$$\sigma^2 = \begin{Bmatrix} 1, if f_i \le f_k \\ exp\left(\frac{f_k - f_i}{|f_i| + \varepsilon}\right) otherwise k \in [1, N], k \ne 1 \end{Bmatrix} \quad (6)$$

ANFIS calculation is used to select the CSP concentration structure ideally. The ANFIS controller input is the current state of the chicken swarm. The crop renews the position of the chicks. The proposed controller updates the position of the chicken according to the cooking, testing and Membership Functions (MF). Thus, the regulator ANFIS is aware of the improvement in the calculation of CSO. ANFIS is a trained sequential network that incorporates the characteristics of a Sugeno-type Fuzzy Inference System (FIS). Unlike other standard frameworks, the most interesting for ANFIS are the fast pace of work, high accuracy and learnability, remarkable features, and MF customization.

A typical ANFIS design, allowing 5 defined levels, is shown in Figure 2. The construction of ANFIS is shaped by two early on and settling parts, which are connected together by a bunch of rules. A straightforward information learning method, ANFIS, applies a fuzzy surmising framework model to change a given contribution to an objective yield.

This forecast concedes enrollment capacities, fuzzy rationale administrators and in the event that rules. There are two kinds of fuzzy frameworks, normally experienced as the Sugeno models and Mamdani. In the ANFIS activity, there are five fundamental preparing stages, including input fuzzification, utilization of fuzzy administrators, application technique, yield collection, and defuzzification. A similar yield enrollment work cannot be shared for different standards. The quantity of rules is must sufficient for the quantity of the participation work. The current situation of the chicken multitude is taken care of by the ANFIS regulator. To accomplish the updation cycle, two fuzzy IF-THEN standards set up on a first-request Sugeno model are considered as conditions (7) and (8),

Rules (1) and (2):

IFΨ isE_1AND$\Psi_1$isF_1, THEN$M_1 = i_1\psi + j_1\psi_1 + k_1$ (7)

IFΨ_1 isE_2ANDΨisF_2, THEN$M_2 = i_2\psi + j_2\psi_1 + k_2$ (8)

Where, the information sources are $\Psi$and Ψ_1 (current specialist position of significant worth), E_1 and F_1 are the fuzzy sets, $M_1$are the yields inside the fuzzy area characterized by the fuzzy principle i_n,j_n and $k_n$are the plan boundaries that are affected all through the preparation interaction. In this figure, a circle proposes a fixed hub, though a square recommends a versatile hub. ANFIS has five-layer engineering. Each layer is clarified in detail in the under region.

Layer 1: All the hubs are versatile hubs. Here, the current position is that trees are taken care of in this layer. The yields of layer1 are the fuzzy participation evaluation of the data sources, which are managed by the accompanying conditions (9) and (10),

$$Y_{out1} = \lambda_{xn}(G), \rightleftarrows n = 1,2 \quad (9)$$

$$Y_{out1} = \lambda_{yn-2}(G^1), \rightleftarrows \rightleftarrows \rightleftarrows n = 3,4 \quad (10)$$

Where, x and $y$are the contributions to the hub$i$, G_i and$G^1{}_i$ are the phonetic names (high, low, and so forth) associated with this hub work. Furthermore, $\lambda_{xn}(G)$ and $\lambda_{yn-2}(G^1)$ can follow any fuzzy enrollment work. The chime molded enrollment work is applied, $\lambda_{xn}(G)$ is managed by in condition (11),

$$\lambda_{xn}(G) = \frac{1}{1 + \left[\left(\frac{x - r_i}{p_i}\right)^2\right] q_i}, i = 1,2 \quad (11)$$

Where p_i, q_i and r_i are the parameters of the membership function

Layer 2: The hubs are fixed hubs. The yield of the layer 1 is taken care of by layer 2. Fuzzy administrators are conceded by this layer; it applies the AND administrator to fluffy the sources of info. They are marked with π, recommending that they execute as a basic multiplier. The yield of this layer can be established as the underneath condition (12),

$$Y_{out2} = A_i = \lambda_{xn}(G) * \lambda_{yn-2}(G^1), \rightleftarrows i = 1,2 \quad (12)$$

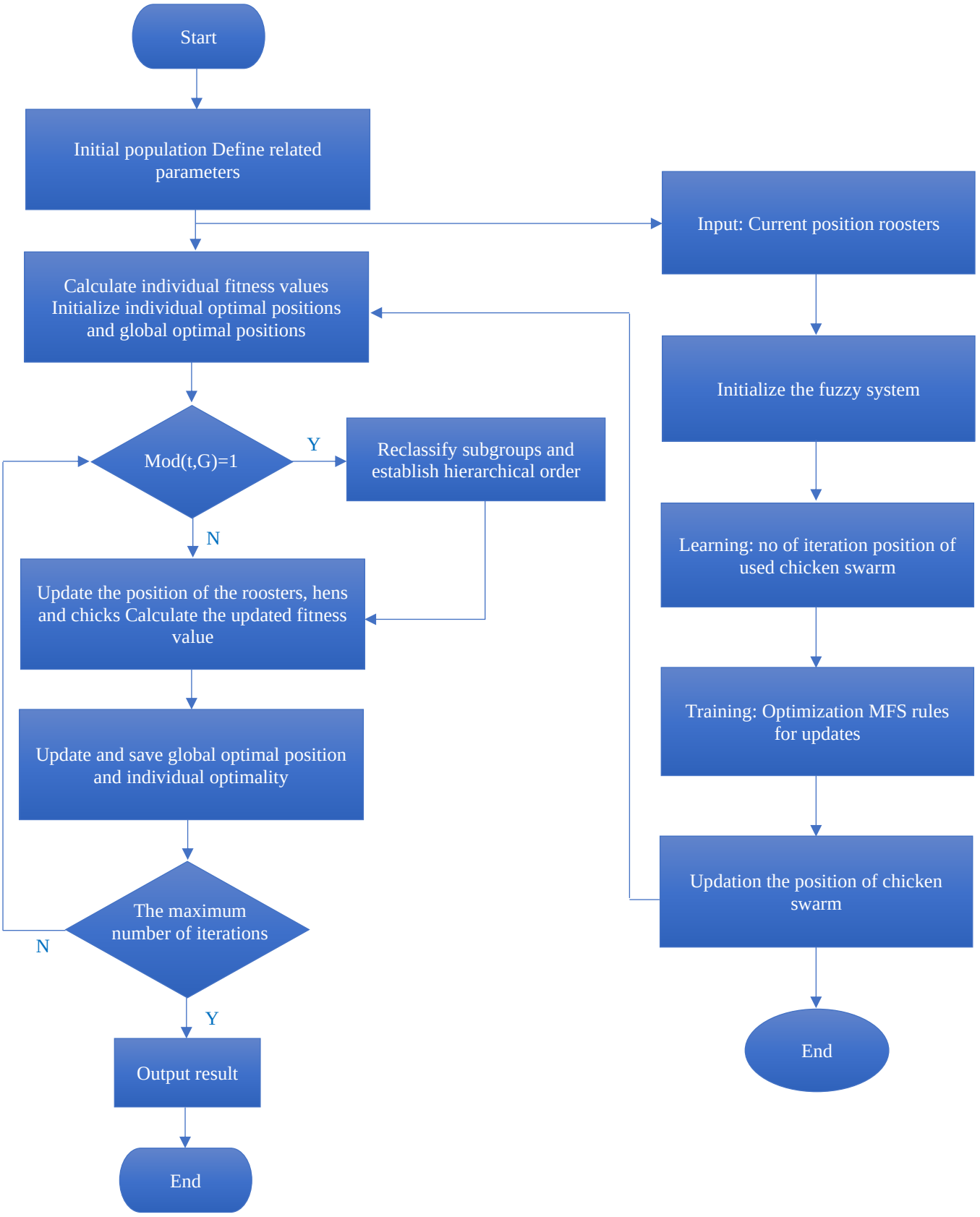

Fig. 2 Flowchart of proposed hybrid technique

Layer 3: The hubs are additionally fixed hubs marked by$N$, to execute that they play a standardization part to the terminating qualities from the past layer. The yield of this layer can be established as the underneath condition (13),

$$Y_{out3} = \overline{A_i} = \frac{A_i}{A_1+A_2}, i = 1,2 \quad (13)$$

Layer 4: The hubs are versatile. The yield of every hub in this layer is just the result of the standardized terminating strength and a first-request polynomial (for a first-request Sugeno model). The yield of this layer is managed by the condition (14),

$$Y_{out4} = \overline{A_i}M_i = \overline{A_i}(i_1X + j_1X^1 + k_1), i = 1,2 \quad (14)$$

Where $\overline{A_i}$is the yield of Layer 4, andi_i,j_i and k_i are the subsequent boundaries.

Layer 5: Only one fixed node is marked with the icon$p$. This node sums all incoming signals. The overall result of the model is determined by equation (15),

$$Y_{out5} = \sum_i \overline{A}\, M_i = \frac{\sum_i A_i M_i}{\sum_i A_i} \quad (15)$$

The five layers are utilized to accomplish the wellness capacity of the refreshing interaction.

Step 5: Update the individual best position N_{best}

Step 6: $t = t + 1$if the cycles meet the required condition, yield the ideal worth; in any case, go to stage 3. The maximization method is achieved by applying the proposed calculation. With the assistance of the ANFIS calculation, the CSO calculation refreshing cycle is accomplished.

3. Results and Discussion

This part presents research results and research on explicit innovation. A Windows computer that includes a 1.6GHz Intel (R) Core i5 processor and 4GB of RAM uses JDK 1.7.0 in the Java programming language working environment - Microsoft Windows 7 Professional. Security is a specific strategy that attempts to use the commonly used local collection of Census Revenue Information (KDD). These informative images of the proposed work are shown in Fig. 3.

3.1. Dataset Description

In our study, we used the Census-Income (KDD) dataset. This dataset contains 299,285 records and 40 credits. The dataset was commissioned from the 1994 and 1995 US Population Surveys. The subset uses the adult dataset as a workable test tool for privacy calculations. Cleans up the dataset by removing datasets with lost quality and properties with highly sloping variance. We get a sterile dataset of 1.53.926 datasets from which we test datasets for companion research.

Twelve credits were selected from the first 40 components, including 9 (4 math and 5 straight) semi-identifiers and 3 (2 math and 1 straight) complex ones.

3.2. Evaluation Metrics

The main goal of the proposed approach is to provide resilient security to protect the intermediate dataset with ANFISCSO. We only encrypt sensitive data to reduce preparation time and costs. Data collection is used to select important data. Circular Curve Cryptography is an encryption calculation used to encrypt sensitive information. Scrambling all informational indexes to ensure safety is widely accepted in river research. In order to evaluate our particular approach to printing images, we need to complete several evaluation steps. We use the following rating systems in our work:

(1) Peak Signal to Noise Ratio (PSNR)
(2) Mean Square Error (MSE)
(3) Cross-correlation (CC)

Peak signal-to-noise ratio & Mean Square Error: In our work, the peak signal-to-noise ratio, which is an indicator of quality, is treated with the premise of mean square error (MSE). Its presentation is also shown below.

$$PSNR = 10\, log\left(\frac{(255)^2}{MSE}\right) dB \quad (16)$$

$$MSE = \frac{1}{N}\sum\left(P_{ref}(i,j) - P_{prc}(i,j)^2\right) \quad (17)$$

Here N is the total number of pixels in the image. These$P_{ref}(i,j)$ and $P_{prc}(i,j)$ are separate pixel estimates of the reference and expected corpus images.

Cross-correlation: The cross-correlation is defined between the reference image and the complex image, which is set in the next state;

$$R_F[i,j] \circ S_F[i,j] = \sum_{i=0}^{M-1}\sum_{j=0}^{N-1} R_F[i,j]S_F[i,j] \quad (18)$$

3.2.1. Analyzing PSNR

Table.1 and Fig.4 show the PSNR rating for shading configurations for both real and clinical images.

3.2.2. Analyzing MSE

Table. 2 shows the MSE rating for shading configurations for both real and shaded images.

3.2.3. Analyzing CC

Table. 3 shows the CC rating for shading schemes for both real and shaded images. From the stimulus given in Table 3 above, we can see that the ACECC image printing innovation has a high percentage of printing for painting over images. Eyes, houses, figures, etc., are images that can appear shaded outwardly. Thus, unmistakably authenticated images can be compressed using the proposed operation without transmission failure.

Table 1. PSNR comparison of proposed vs existing methods with color images

Images	ECC	CSO	PSO	WOA	GSA	GA	CS
1	36.3475	32.8551	25.5802	23.9182	23.4293	24.437	16.3456
2	36.173	32.6656	25.3777	23.7222	23.2361	24.2384	10.3809
3	36.0926	32.5767	25.2478	23.5716	23.0791	24.0946	11.2886
4	36.0955	32.5782	25.2701	23.6243	23.1427	24.1368	8.3623
5	36.0896	32.5678	25.2171	23.5452	23.0568	24.0644	10.628
6	34.6163	31.567	24.7708	23.1609	22.6844	23.6651	4.068
7	34.6011	31.5557	24.7647	23.1555	22.6791	23.6595	16.4125
8	36.1083	32.5934	25.254	23.5723	23.0772	24.0974	10.6613
9	36.1038	32.5875	25.2547	23.5873	23.0984	24.1069	8.5878
10	35.6585	32.2861	25.0906	23.4253	22.9343	23.9458	6.4247

Table 2. MSE comparison of proposed vs existing methods with color images

Images	ECC	CSO	PSO	WOA	GSA	GA	CS
1	15.0776	33.6956	179.9126	263.7892	295.2224	234.0864	1504.078
2	15.6956	35.1979	188.4992	275.9688	308.6545	245.044	5956.554
3	15.989	35.9265	194.2249	285.7091	320.0156	253.2899	4833.057
4	15.9781	35.9137	193.227	282.2588	315.3604	250.8419	9480.829
5	16	36	195.5988	287.4515	321.6625	255.0604	5627.069
6	22.4619	45.3296	216.7711	314.042	350.4639	279.6192	25484.64
7	22.5407	45.4477	217.0756	314.4361	350.8896	279.9826	1485.341
8	15.9314	35.7879	193.9478	285.6615	320.1518	253.13	5584.022
9	15.9478	35.8373	193.9152	284.6753	318.5924	252.5761	9001.104
10	17.6699	38.4121	201.3809	295.4941	330.8652	262.123	14811.76

Table 3. CC comparison of proposed vs existing methods with color images

Images	ECC	CSO	PSO	WOA	GSA	GA	CS
1	0.99994	0.99986	0.99919	0.99878	0.99862	0.99893	0.67856
2	0.99996	0.99992	0.99946	0.99915	0.99902	0.99926	0.021128
3	1	0.99999	0.99978	0.99961	0.99955	0.99967	0.14061
4	1	1	1	0.99999	0.99999	0.99999	0.10084
5	1	1	0.99998	0.99991	0.99987	0.99994	0.42131
6	0.99998	0.99998	0.99997	0.99996	0.99996	0.99996	-0.10381
7	0.99999	0.99999	0.99999	0.99999	0.99999	0.99999	0.68599
8	1	0.99999	0.9999	0.99984	0.99981	0.99986	0.55942
9	1	1	0.99997	0.99995	0.99993	0.99996	0.11679
10	0.99998	0.99998	0.99998	0.99998	0.99998	0.99998	0.086823

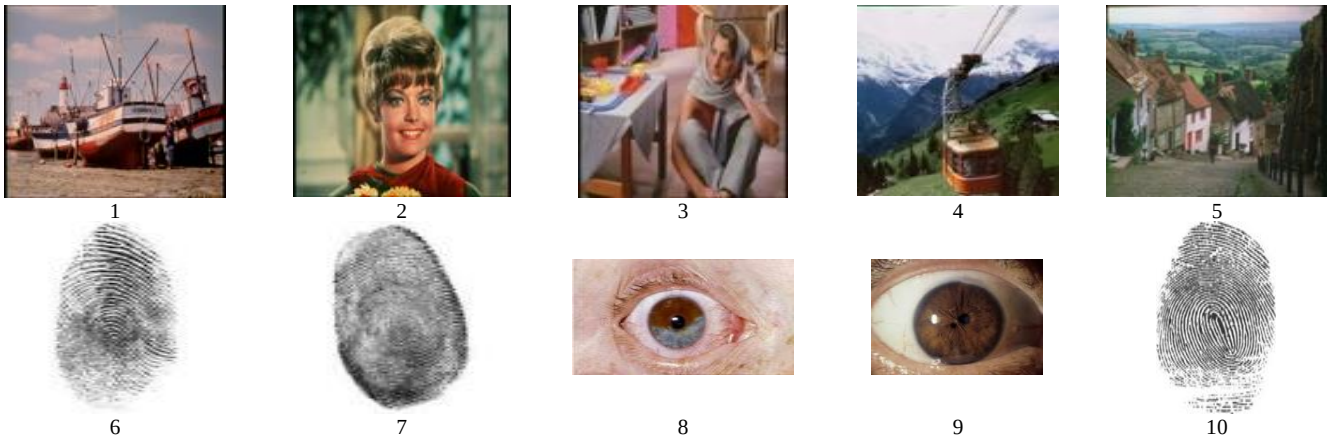

Fig. 3 Input images

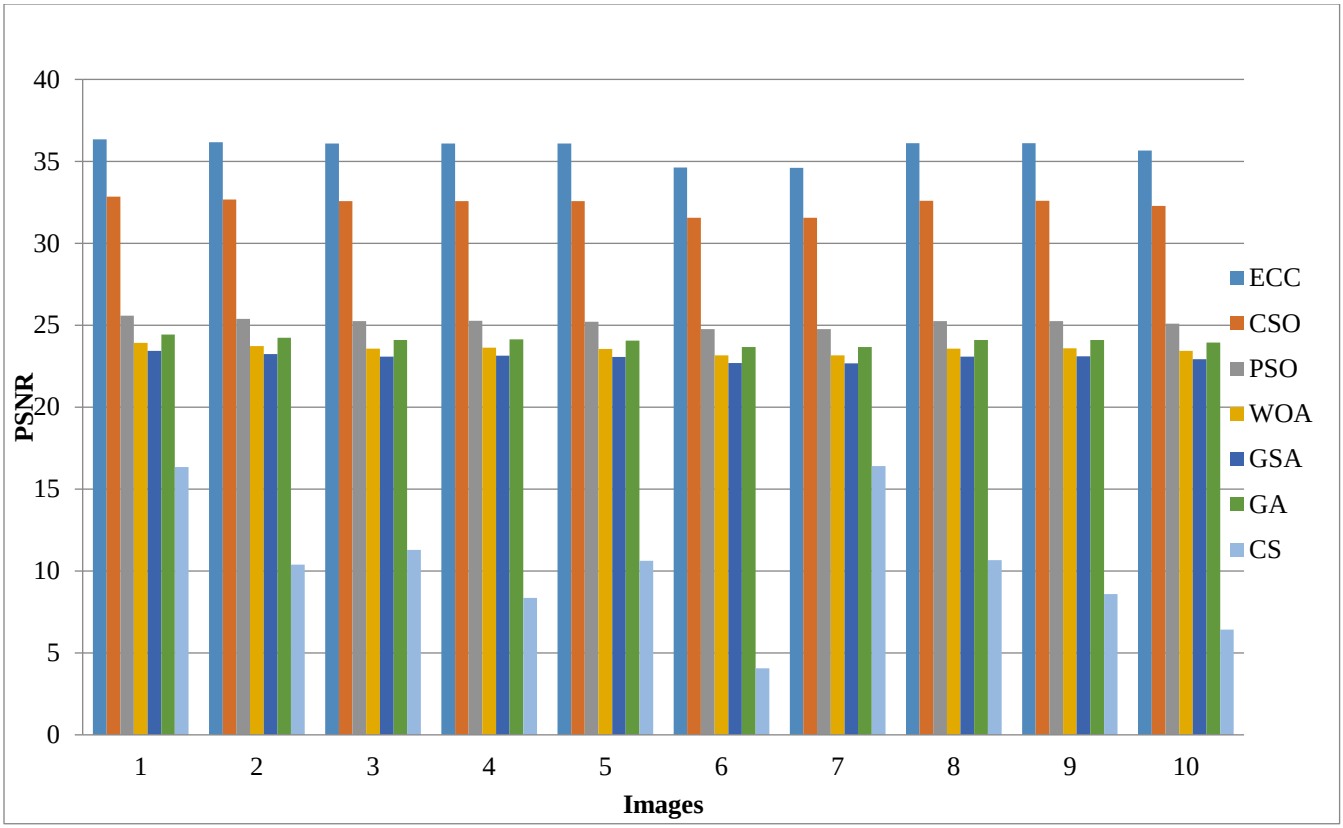

Fig. 4 Comparison analysis of PSNR

In the just published section, remotely enhanced interest scoring is performed on a variety of occasions along with a real incentive over a predetermined period of time. As a result, the estimate of the required energy will exceed the required value. As a result, the special need for the transmitted energy to approach energy use is not satisfied. This usually diminishes or improves compared to the strength interest score. Accordingly, today's unmistakable innovation constantly reacts to the conditions of subtle changes in population and interest in energy.

However, when energy is generated or used, equal benefits offer the best value. Thus, it fails miserably when transporting goods corresponding to a specific required value. Hence, it takes quite a long time, even due to small changes in the evaluation of the encrypted data, and it takes a long cycle to deal with the problem of changing the encrypted properties. The other five modes such as PSO, WOA, GSA, GA, and CS, they can be given a mathematical value. So, it can be concluded that the extended method can offer the sender security and confidentiality messaging methods as compared to certain types of approaches.

4. Conclusion

The proposed elliptic curve encryption method is effectively used to ensure the exchange of messages between the central core system and the cloud in accordance with the network requirements of some nodes of the IoT system. Using customer power consumption data, the system can completely eliminate persistent power failure without continuous power outages. Energy consumption data is efficiently transferred from one end to the other using ECC technology. At the same time, parallel methods are used to communicate the message to the main central system, such as the ANFIS-CSO. When messages are assessed and analyzed using innovative ECC technology, it becomes clear that they cannot simply be processed with a message encrypted by Protestants.

Thus, the proposed ECC method provides the security and protection of the attacker's message. The ECC is to be implemented, and it is important to understand these potentially risky decisions in order to support them adequately in the appropriate system. The application is currently running on JAVA, and the algorithm's performance is being tested against test records.

According to research, the design algorithm makes minimal use of PSNR, MSE and CC when compared to available methods. As a result, ECC is still under study and represents a broad horizon to be discovered. It is hoped that, in the future, it will be possible to use effective ECC methodological techniques to speed up ECC assessment by improving data security.

References

[1] Hua-Yi Lin, Meng-Yen Hsieh, and Kuan-Ching Li, "Flexible Group Key Management and Secure Data Transmission in Mobile Device Communications Using Elliptic Curve Diffie-Hellman Cryptographic System," *International Journal of Computational Science and Engineering*, vol. 12, no. 1, pp. 47-52, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[2] Tarun Kumar Goyal, and Vineet Sahula, "Lightweight Security Algorithm for Low Power IoT Devices," *2016 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, Jaipur, India, pp. 1725-1729, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[3] Ioannis Chatzigiannakis, Andrea Vitaletti, and Apostolos Pyrgelis, "A Privacy-Preserving Smart Parking System Using an IoT Elliptic Curve Based Security Platform," *Computer Communications*, vol. 89-90, pp. 165-177, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[4] Wen-Bin Hsieh, and Jenq-Shiou Leu, "Implementing a Secure VoIP Communication Over SIP-Based Networks," *Wireless Networks*, vol. 24, no. 8, pp. 2915-2926, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[5] Darshana Pritam Shah, and Pritam Gajkumar Shah, "Revisting of Elliptical Curve Cryptography for Securing Internet of Things (IOT)," *2018 Advances in Science and Engineering Technology International Conferences (ASET)*, Dubai, Sharjah, Abu Dhabi, United Arab Emirates, pp. 1-3, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[6] Muneer Bani Yassein et al., "Comprehensive Study of Symmetric Key and Asymmetric Key Encryption Algorithms," *2017 International Conference on Engineering and Technology (ICET)*, Antalya, Turkey, pp. 1-7, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[7] Zhen Wang et al., "Enhanced Instant Message Security and Privacy Protection Scheme for Mobile Social Network Systems," *IEEE Access*, vol. 6, pp. 13706-13715, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[8] Sanjay Kumar, and R.K. Singh, "Secure Authentication Approach Using Diffie-Hellman Key Exchange Algorithm for WSN," *International Journal of Communication Networks and Distributed Systems*, vol. 17, no. 2, pp. 189-201, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[9] Sangram Ray, G.P. Biswas, and Mou Dasgupta, "Secure Multi-Purpose Mobile-Banking Using Elliptic Curve Cryptography," *Wireless Personal Communications*, vol. 90, no. 3, pp. 1331-1354, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[10] Pratima Deshpande et al., "Experimental Study of Diffie-Hellman Key Exchange Algorithm on Embedded Devices," *2017 International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS)*, Chennai, India, pp. 2042-2047, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[11] A. Mullai, and K. Mani, "Enhancing the Security in RSA and Elliptic Curve Cryptography Based on Addition Chain Using Simplified Swarm Optimization and Particle Swarm Optimization for Mobile Devices," *International Journal of Information Technology*, pp. 551-564, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[12] Arjun Rawat, and Maroti Deshmukh, "Tree and Elliptic Curve Based Efficient and Secure Group Key Agreement Protocol," *Journal of Information Security and Applications*, vol. 55, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[13] Balkis Bettoumi, and Ridha Bouallegue, "Evaluation of Authentication Based Elliptic Curve Cryptography in Wireless Sensor Networks in IoT Context," *2018 26th International Conference on Software, Telecommunications and Computer Networks (SoftCOM)*, Split, Croatia, pp. 1-5, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[14] Titus Balan, Alexandra Balan, and Florin Sandu, "SDR Implementation of a D2D Security Cryptographic Mechanism," *IEEE Access*, vol. 7, pp. 38847-38855, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[15] Daya Sagar Gupta, S.K. Hafizul Islam, and Mohammad S. Obaidat, "A Secure Identity-Based Deniable Authentication Protocol for MANETs," *2019 International Conference on Computer, Information and Telecommunication Systems (CITS)*, Beijing, China, pp. 1-5, 2019. [CrossRef] [Google Scholar] [Publisher Link]