International Journal for Modern Trends in Science and Technology
Volume 11, Issue 05, pages 1281-1287
ISSN: 2455-3778 online
Available online at: http://www.ijmtst.com/vol11issue05.html
DOI: https://doi.org/10.5281/zenodo.16008547

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

Chinthakunta Swetha[1], Godina Amruthavani[2]

[1]Academic Consultant, Department of Computer Science and Technology, Yogi Vemana University, Kadapa. reddyswetha704@gmail.com

[2]Academic Consultant, Department of Computer Science and Technology, Yogi Vemana University, Kadapa. amruthagodina@gmail.com

To Cite this Article
Chinthakunta Swetha & Godina Amruthavani (2025). An Intelligence Technique Based Elliptic Curve Cryptography Algorithm for Secured Communication in Networks. International Journal for Modern Trends in Science and Technology, 11(05), 1281-1287. https://doi.org/10.5281/zenodo.16008547

Article Info
Received: 05 May 2025; Accepted: 28 May 2025.; Published: 29 May 2025.

KEYWORDS

Cloud computing, elliptic curve cryptography, ANFIS-CSO, encryption and decryption

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 emerging primarily, increasingly at the heart of the sensitive data cloud. This work aims to provide a reliable and secure cloud-based communications service that allows customers to dynamically access their information. To achieve this, in this article, we advance advances in secure communications over 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 name 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.

1. INTRODUCTION

Nowadays, mobile devices are now part of our daily life. They can be used for a variety of 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: access 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 labeling 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 is 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 organization 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, used in 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 IoT intermediate information security using ACECC strategy. We currently make series 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 brief description of some of the articles written can be found in Section 2. A step-by-step explanation of the proposed system is provided in Section 3. Research options and evaluation discussion are given performance in Section 4. Finally, Section 5 summarizes the findings.

2. LITERATURE REVIEW

To deal with security issues in the IoT climate, experts have introduced different and different security arrangements using cryptography programs. This section depicts past and related works in the IoT security region.

Sethuraman *et al*. [16] Diffie Hellmann has introduced a fuzzy genetic elliptical curve to ensure correspondence between companies. The uniqueness of elliptical curve cryptography (ECC) lies in the ability to produce information using efficient limited keys to provide the RSA's long-standing key prerequisite. Intelligent guidelines are used for stabilization during key determination measurements, and many characteristic dynamic models with fuzzy reasoning to obtain keys and hereditary calculations to compulsorily improve computation in the ECC get the proposed FGECDH calculation.

Dharminder *et al*. [17] have provided a secure letter based on learning error on cell phones using fluffy extraction. The security verification of the proposed method ensures provable-security by learning the problem of errors at some point in the irregular prophecy. Besides, a simple security conversation and execution test shows that our LWESM conference is effective and can be used in many different applications. Joshi *et al*. [18] have implemented a lightweight verification conference for body territory networks based on elliptical-curve cryptography. This conference empowers the customer to refuse by immediately updating the time key. The proposed conference meets different security requirements, for example, non-connectivity, secrecy, forward security, shared confirmation and meeting key security. Experimental testing at AVISPA proved that the cost of verification conference calculation and efficiency on the part of the client was completely reduced compared to the existing arrangements, which are more suitable for property restricted remote body regional systems.

Sowjanya *et al*. [19] presented a guaranteed framework for WBAN using Ciphertext and Attribute-Based Elliptic Curve Elliptic Curve Encryption (CPABE) without implementing linear coordination. The proposed CPABE is provided under Diffie-Hellman's assumption of elliptical curve determination and in addition has a customer / brand disclaimer segment. We investigated the light portion of the proposed CPABE, differentiating it from other ABE plans for WBAN.

Kumar *et al*. [20] have introduced a protected elliptic bend cryptography based common confirmation convention for cloud-helped TMIS. The proposed convention secure against man-in-the-center assault, understanding secrecy, replay assault, known-key security property, information classification, information non-disavowal, message confirmation, pantomime assault, meeting key security and patient unlink capacity. The proposed convention with existing related conventions in same cloud based TMIS. The proposed convention guarantees of all alluring security requirements and dealt with the productivity as far as calculation and correspondence costs for cloud-helped TMIS.

3. PROPOSED METHODOLOGY

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.

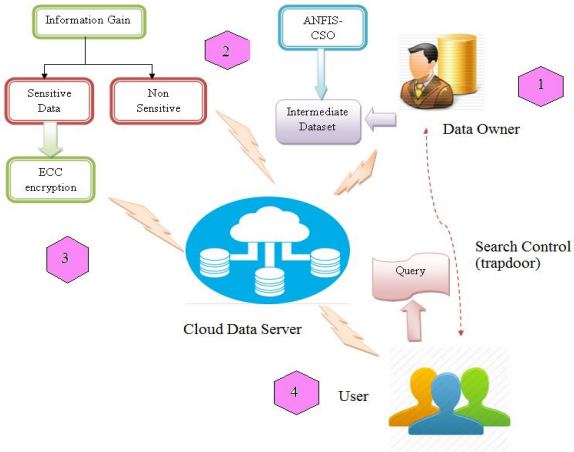

Figure 1: Proposed architecture of preserving security in cloud

3.1. Generation of Intermediate Dataset

Suppose the attribute size K^D and record count F is 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. Therefore, we expect that the data recorded in the data source will be used to determine the proportion of generation in the dataset.

We present the various main archives listed below. Make K^D a special secure entry for it. We use $H=\{H_1, H_2, ..., H_n\}$ 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.

4. RESULTS AND DISCUSSION

This part presents research results and research on explicit innovation. A Windows computer that includes a 1.6 GHz 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 locally collection of Census Revenue Information (KDD). These informative images of the proposed work are shown in Figure 2.

Fig.2: Input images

4.1 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.

4.2 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.

$$PSNR = 10\log\left(\frac{(255)^2}{MSE}\right)dB \tag{38}$$

$$MSE = \frac{1}{N}\sum\left(P_{ref}(i,j) - P_{prc}(i,j)^2\right) \tag{39}$$

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;

$$R_F[i,j] \circ S_F[i,j] = \sum_{i=0}^{M-1}\sum_{j=0}^{N-1} R_F[i,j]\, S_F[i,j] \tag{40}$$

4.2.1. Analyzing PSNR

Table III and Figure 3 show the PSNR rating for shading configurations for both real and clinical images.

Table I: 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

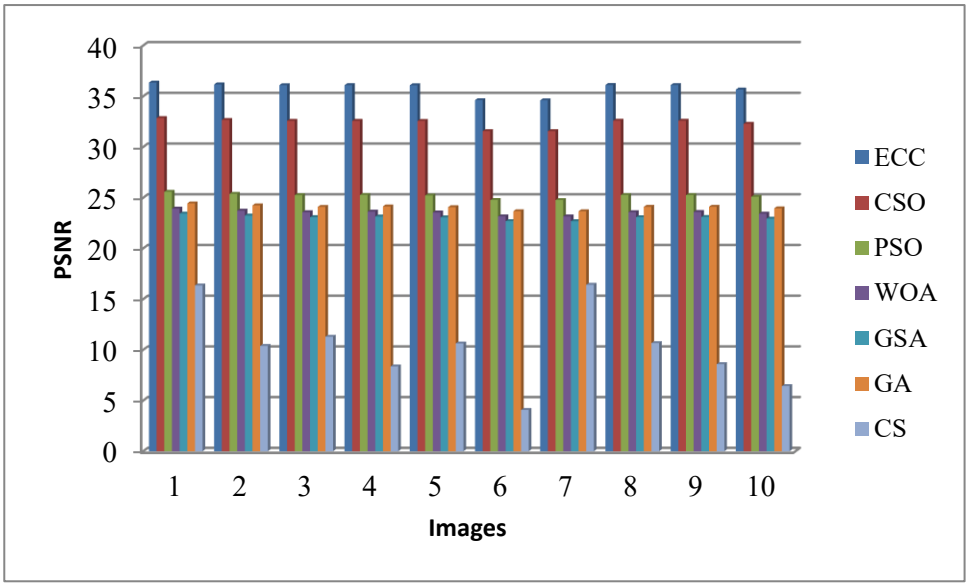

Figure 3: Comparison analysis of PSNR

Shaded PSNR contributes to high PSNR scores in contrasting and varied strategies. Proportion of pressure and PSNR are useful for both clinical and real shaded images.

Conflict of interest statement

Authors declare that they do not have any conflict of interest.

REFERENCES

[1] Lin, H.Y., Hsieh, M.Y. and Li, K.C., 2016. 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, 12(1), pp.47-52.

[2] Goyal, T.K. and Sahula, V., 2016, September. Lightweight security algorithm for low power IoT devices. In 2016 International Conference on Advances in Computing, Communications and Informatics (ICACCI) (pp. 1725-1729). IEEE.

[3] Chatzigiannakis, I., Vitaletti, A. and Pyrgelis, A., 2016. A privacy-preserving smart parking system using an IoT elliptic curve based security platform. Computer Communications, 89, pp.165-177.

[4] Hsieh, W.B. and Leu, J.S., 2018. Implementing a secure VoIP communication over SIP-based networks. Wireless Networks, 24(8), pp.2915-2926.

[5] Shah, D.P. and Shah, P.G., 2018, February. Revisting of elliptical curve cryptography for securing Internet of Things (IOT). In 2018 Advances in Science and Engineering Technology International Conferences (ASET) (pp. 1-3). IEEE.

[6] Yassein, M.B., Aljawarneh, S., Qawasmeh, E., Mardini, W. and Khamayseh, Y., 2017, August. Comprehensive study of symmetric key and asymmetric key encryption algorithms. In 2017 international conference on engineering and technology (ICET) (pp. 1-7). IEEE.

[7] Wang, Z., Ma, Z., Luo, S. and Gao, H., 2018. Enhanced instant message security and privacy protection scheme for mobile social network systems. IEEE Access, 6, pp.13706-13715.

[8] Kumar, S. and Singh, R.K., 2016. Secure authentication approach using Diffie-Hellman key exchange algorithm for WSN. International Journal of Communication Networks and Distributed Systems, 17(2), pp.189-201.

[9] Ray, S., Biswas, G.P. and Dasgupta, M., 2016. Secure multi-purpose mobile-banking using elliptic curve cryptography. Wireless Personal Communications, 90(3), pp.1331-1354.

[10] Deshpande, P., Santhanalakshmi, S., Lakshmi, P. and Vishwa, A., 2017, August. Experimental study of Diffie-Hellman key exchange algorithm on embedded devices. In 2017 International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS) (pp. 2042-2047). IEEE.

[11] Mullai, A. and Mani, K., 2020. 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.1-14.

[12] Rawat, A. and Deshmukh, M., 2020. Tree and elliptic curve based efficient and secure group key agreement protocol. Journal of Information Security and Applications, 55, p.102599.

[13] Bettoumi, B. and Bouallegue, R., 2018, September. Evaluation of Authentication Based Elliptic Curve Cryptography in Wireless Sensor Networks in IoT Context. In 2018 26th International Conference on Software, Telecommunications and Computer Networks (SoftCOM) (pp. 1-5). IEEE.

[14] Balan, T., Balan, A. and Sandu, F., 2019. SDR Implementation of a D2D Security Cryptographic Mechanism. IEEE Access, 7, pp.38847-38855.

[15] Gupta, D.S., Islam, S.H. and Obaidat, M.S., 2019, August. A Secure Identity-based Deniable Authentication Protocol for MANETs. In 2019 International Conference on Computer, Information and Telecommunication Systems (CITS) (pp. 1-5). IEEE.

[16] Sethuraman, P., Tamizharasan, P.S. and Arputharaj, K., 2019. Fuzzy genetic elliptic curve Diffie Hellman algorithm for secured communication in networks. Wireless Personal Communications, 105(3), pp.993-1007.

[17] Dharminder, D. and Chandran, K.P., 2020. LWESM: learning with error based secure communication in mobile devices using fuzzy extractor. Journal of Ambient Intelligence and Humanized Computing, pp.1-12.

[18] Joshi, A. and Mohapatra, A.K., 2020. A novel lightweight authentication protocol for body area networks based on elliptic-curve cryptography. Journal of Information and Optimization Sciences, pp.1-28.

[19] Sowjanya, K. and Dasgupta, M., 2020. A ciphertext-policy Attribute based encryption scheme for wireless body area networks based on ECC. Journal of Information Security and Applications, 54, p.102559.

[20] Kumar, V., Ahmad, M. and Kumari, A., 2019. A secure elliptic curve cryptography based mutual authentication protocol for cloud-assisted TMIS. Telematics and Informatics, 38, pp.100-117.