DS Journal of Digital Science and Technology
Volume 1 Issue 1, 10-16, Jul - Sep 2022
ISSN: 2583-5416/ https://doi.org/10.59232/DST-V1I1P102

Original Article

A Fog Computing Approach for Securing IoT Devices Data using DNA-ECC Cryptography

R.Surendiran[1], K. Raja[2]

[1,2]*School of Information Science, Annai College of Arts and Science, Kumbakonam, India.*

surendiranmca@gmail.com

Received: 12 May 2022 ; Revised: 30 June 2022 ; Accepted: 03 July 2022; Published: 10 July 2022;

Abstract - In recent times, the Internet of Things (IoT) placed a vital role in various applications because various devices are connected to make communication effective. Most people utilize the IoT to gather private information and the gathered details are saved in a third-parties database. Intermediary access or unauthorised individuals attempting to access sensitive information during storage pose a threat to data confidentiality, integrity, and privacy. During this process, fog computing is worked with IoT devices because it collects a large volume of data and is computationally intensive. The security, energy consumption of fog nodes and IoT devices is critical because they generate data that can be exploited by attackers. In order to ensure data security, encryption is an effective method. Various encryption schemes exist, but each has its own constraints. In this paper, we develop a DNA-based Elliptic Curve Cryptography technique with RedFox Optimization algorithm for clustering (RF-DECC) to control data security in fog computing. Initially, the cluster heads are identified according to the Redfox optimization. Once clustering has been completed, the cluster head begins the data encryption process by encrypting cluster members' data with DNA-Elliptic Curve Cryptography (ECC). In comparison to other well-known public key cryptography algorithms, the ECC is the most lightweight cryptography. Using DNA with ECC increases encryption complexity by encoding DNA. Based on the experimental results, proposed RF-DECC method is superior in terms of delays, throughput, energy consumption, and the data security ratio. The proposed RF-DECC method improves the overall data security of 24%, 32% better than existing DIoTA and FUPA respectively.

Keywords -Fog computing, Encryption, IoT, DNA, Elliptic curve cryptography, Cluster head.

1. Introduction

An Internet of Things (IoT) is a system of physical objects, such as automobiles, home appliances, and other devices, that are connected via software, actuators, electronics, and sensors [1]. IoT creates integrated communication situations for networked devices and stages by bringing together the practical and substantial worlds at the same time [2]. A lot of data is generated by IoT devices, requiring a lot of storage space, power, and data transmission capability [3]. Fog computing is a new concept that brings processing and execution capabilities closer to the end-user to improve service quality. It is similar to the cloud paradigm in that it brings processing and execution capabilities closer to the end-user. IoT with fog requires sufficient networking and equipment to ensure low latency and fast response times for IoT applications. Data supplied by IoT devices can be processed and executed with the help of fog computing [4]. IoT devices that generate data can be better served by shifting applications, processing capabilities, and execution closer to them. These problems can be solved using fog computing.

By combining IoT and fog computing, we can increase user experience and service flexibility in the event of problems [5]. Fog computing, when used in a distributed system and closer to the source of data, can provide faster responses and higher quality of service for IoT applications. The fundamental objective of IoT and fog computing integration is to enhance efficiency, productivity, and elapsed time, computation, and storage time [6].

When fog computing and IoT are combined, additional security is provided when transferring sensor data to fog nodes, and network traffic is reduced in its place by means of the cloud. As a result, combining fog/edge computing with IoT is a future expansion in the arena of IoT. However, fog's distinctive attributes like mobility support have also brought in challenges like privacy and security, affecting fog computing's adaptation into the IoT. To overcome these challenges, the present work DNA based cryptography with clustering algorithm. The main contributions of the proposed methodologies are,

- Initially, the cluster heads are identified according to the Redfox optimization.
- Once clustering has been completed, the cluster head begins the data encryption process by encrypting cluster members' data with DNA-Elliptic Curve Cryptography (ECC).
- The proposed RF-DECC technique is evaluated based on metrics such as delay, throughput and energy consumption.
- The highest efficiency is achieved when compared with the existing methods.

The rest of the paper follows. Section 2 depicts the review of several existing techniques, Section 3 includes the proposed technique using RF-DECC, Section 4 comprises with results and discussions and finally Section 5 encloses with conclusion and future enhancement.

2. Literature Review

In recent day several cryptographic techniques were introduced by the researches mainly focus on data security in IoT device communication. Some of the studies are briefly discussed in this section.

In 2020 Xu, L., et al [7] proposed the decentralized internet of things authenticity (DIoTA) for data authenticity protection in IoT devices. To ensure that these applications function properly, these devices and the data they collect must be authenticated. It is essential to authenticate these devices and their data to ensure that these applications work correctly.

In 2021 Murugesan, A., et al [8] proposed a cryptographic technique for data security. ECC technique is used for high level of security while requiring a smaller key size, less storage, and less transmission. For dispersed systems such as fog computing, the hybrid combination of completely homomorphic ECC and PRE also demonstrates higher performance with high speed.

In 2021 Narayana, V.L. and Patibandla, R.L., [9] established a fog-based model for Secured data communication, demonstrating its functional importance and centrality. The suggested approach solves communication challenges in IoT devices by combining fog computing with resource handling, validations, and IoT device configurations to create a strong programming environment. The suggested Fog Computing architecture successfully facilitates connection between IoT devices while also providing data security throughout communication.

In 2021, Chinnasamy, P et al [10] proposed two hybrid algorithms are ECC and Blowfish. Java was used to develop and implement the proposed model. The ECC algorithms and Blowfish are used for key creation, decryption, and encryption. The key distribution problem can be addressed by using steganography to hide the keys. The proposed hybrid state is compared to an existing hybrid technique, demonstrating that it provides high levels of patient confidentiality and integrity.

In 2021 Javanmardi, S et al [11] introduced a security-aware job scheduler namely FUPE in IoT and Fog network. The proposed method combines optimal computing resources with suitable security protection into a single synthetic objective to arrive at a single correct answer by applying fuzzy-based multi-objective particle swarm optimization. When compared to the prior method, the proposed strategy improves network utilization by 22 % and average response time by 17% respectively.

The above-reviewed methodologies possess some drawbacks in Fog-IoT computing and our proposed methodology with DNA based cryptography with clustering technique overcome the Fog-IoT security. The proposed framework is presented in the following section.

3. Proposed Methodology

In this section we propose a DNA-based cryptographic technique with clustering algorithm for data security. In the proposed method, RedFox optimization is used to group data into clusters and choose the cluster head. The DNA Elliptic curve cryptography algorithm is utilized to ensure security of the data by encrypting the collected data given by cluster head and send to the gateway. The entire architecture of DSM is shown in figure.1.

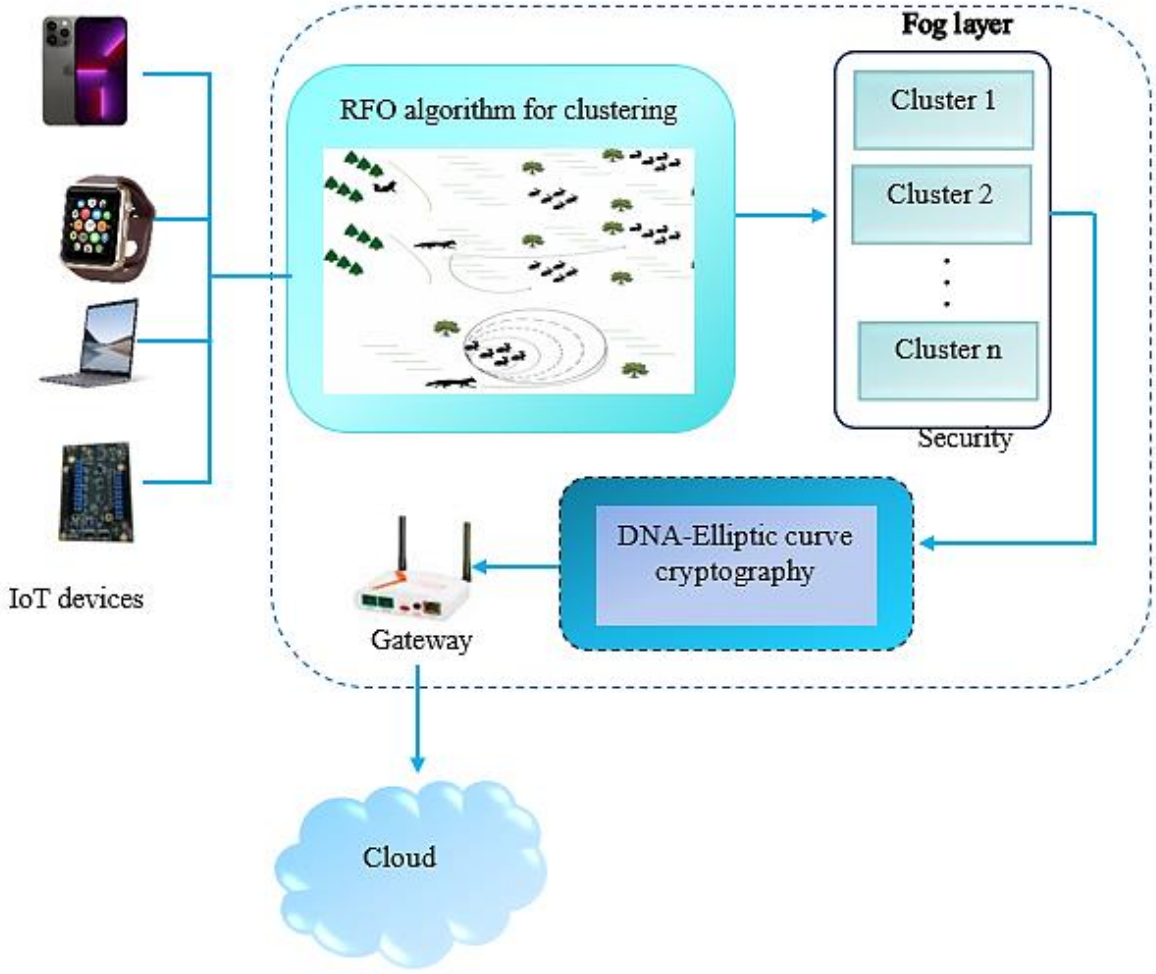


Fig. 1 Overall workflow of proposed methodology

3.1. Clustering Technique

For clustering the data Red Fox optimization algorithm is used. Clustering effectively minimizes network energy consumption and improves network stabilization. As a novel optimization strategy, metaheuristics are presented to select the cluster head using fitness function computations. A new metaheuristic optimization algorithm called Red Fox Optimizer (RFO) is inspired by the red fox hunting behaviour. During hunting, the red fox hides behind bushes and approaches its prey slowly. It surprises its prey by attacking. RFO initialization can be modelled by random individual generation, as shown below

$$Z = \{z_0, z_1, z_2, \ldots, z_{n-1}\} \qquad (1)$$

Where i refers to the number of populations, $(Z_j^i)^t$describes the z_i in iteration t, and j refers to the problem dimensions in the probing space. As f is the function in R_n condition where n refers for the attributes in the range of [x, y] ^{n},

$$(Z)^i = \{(z_0)^i, (z_1)^i, (z_2)^i, \dots, (z_{n-1})^i\} \qquad (2)$$

Where $x, y \in R$. Thus, the optimal solution is attained while $f((Z)^i)$ proposes the global optimum results. All individuals are expected to assist the exploration crew in a specific way. Those individuals that do not find enough prey in one area will move to another for a greater chance to catch prey. In the case of a more appropriate region being acquired, the location is shared with the others. A suitable solution should be proposed in the case of acquiring a more appropriate location. If not, the old location will be retained. After observing the prey, the red fox approaches it. In this case, the RFO algorithm is used, which represents a random values rv in the range of [0, 1]:

$$\begin{cases} move\ closer\ \ if\ rv > \dfrac{3}{4} \\ stay\ and\ hide\ \ if\ rv \leq \dfrac{3}{4} \end{cases} \qquad (3)$$

After that, a more advanced cochleoid formula is utilized to calculate the moment of the member. Among the most important aspects of any medical imaging is classification. A classifier should subsequently be used to identify diseases based on the features obtained from the feature extraction. As previously mentioned, CNN employs the back propagation mechanism for learning. By minimising the mean square error, this study established an RFO technique for the optimal choice of system. The MSE can be expressed numerically as follows:

$$mse = \frac{1}{T}\sum_{j=1}^{q}\sum_{i=1}^{p}(x_j^i - y_j^i)^2 \qquad (4)$$

Where p and q denotes the values of the output layers and the facts, respectively, and x_j^iandy_j^i denotes the attained and the appropriate magnitudes for j^{th} unit in the network's output layer in time T respectively.

3.2. Data Security

To achieve a security mechanism for IoT device data, our method integrates DNA Cryptography and Elliptic Curve Cryptography into a single mechanism. Both of these methods are modern and effective for securing data in the cloud. The first step involves turning text into an ASCII value, then converting it to a binary series value. The binary value of a sequence should be obtained by taking the publicly available DNA nucleotide sequences and converting them to A→00, C→01, G→10, T→11. In order to get a binary sequence, each bit of H must be added to each even number segment of a DNA nucleotide. The generated binary sequence is then translated back into a DNA nucleotide. In the second phase, the DNA sequence is converted into decimal values. These decimal integers were then encoded into an Elliptic Curve point by the Koblitz method. ECC curve points are then used to express the decimal number. These points are encrypted using the ECC encryption technique in equation (5). ECC creates keys for encrypting data.

$$\{VG, Q_n + VQ_m\} \qquad (5)$$

A decryption algorithm called ECC is applied to decode the cipher text by using equation (6). The deciphered points are then converted into numbers via the Koblitz algorithm. Nucleotides are used to decode these numbers, and the plain text is retrieved.

$$Q_n + VQ_m - x_n(VG) = Q_n + V(x_n)G - x_n(VG) = Q_n \qquad (6)$$

Where, G denotes the points generated by the user, Q_n denotes the points of plain text, Q_m denoted the users public key, V denotes the users random number.

The DNA-ECC approach provides more security due to the use of DNA cryptography in its encoding and Elliptic Curve Cryptography in its encryption phases. Thus, the proposed system has two levels of security, the first of which is in the encoding phase, and the second in the encryption phase. In comparison to other cyberspace cryptographic systems, it employs a modest key size (since ECCs are employed, the key size reflects the ECC's key size). It would be challenging for an attacker to break it because it includes two layers of security.

4. Results and Discussion

This paper discussed the IoT communication devices data security has a significant role in the communication field. It is a network that decides on the relative importance of compliance with regulatory sensitivities and the protections required to ensure different data security. Hence in this paper, RF-DECC has been proposed to reduce the delay time, throughput and energy consumption.

4.1. Throughput

The number of data transmitted successfully from one person to another person in a certain period of time is known as throughput. The mathematical formula for throughput T_P is as follows,

$$T_P = \frac{Amount\ of\ data\ transmitted}{Time\ taken\ for\ transmitting\ data}$$

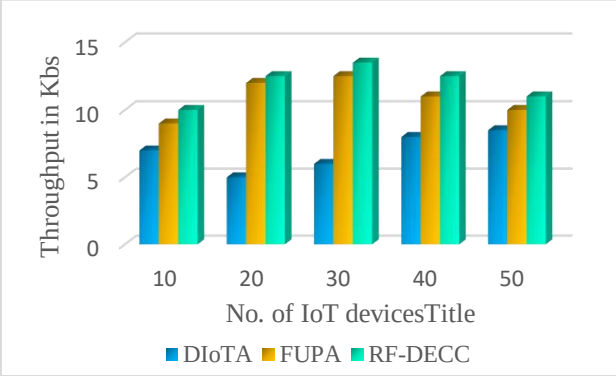


Fig. 2 Comparison on throughput

In Figure 2, the proposed RF-DECC method is compared to existing DIoTA and FUPA methods. The proposed method improves throughput efficiency over prior approaches. The strategy reduces the overload caused by cluster heads sending data. The amount of data transferred is minimized, which reduces data overload.

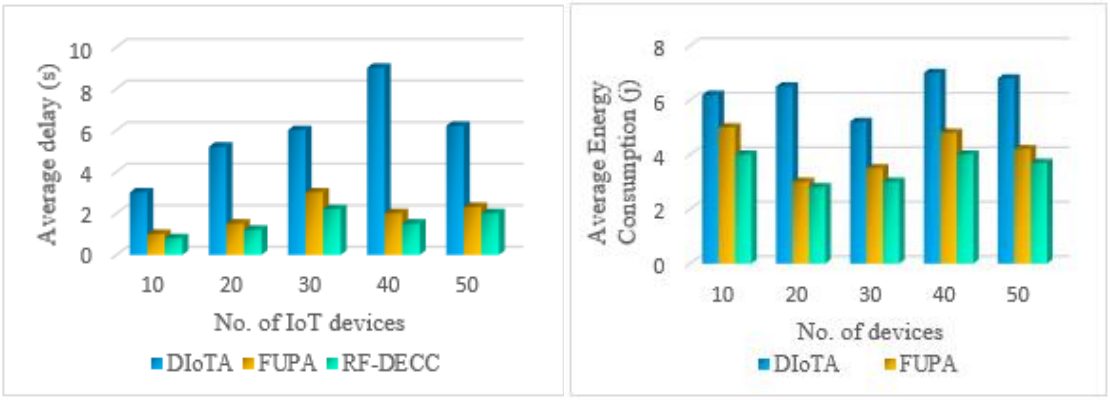
4.2. Delay and Energy Consumption

Delay: The average time taken for data to be transmitted between cluster heads is known as delay. This metric D_y can be calculated mathematically as follows:

$$D_y = \frac{1}{Amount\ of\ data\ transmitted}$$

Energy Consumption: A device's energy consumption is measured by the amount of energy it uses to transmit data in the Internet of Things.

$$EC = P * \frac{T}{1000}$$



(a) **(b)**

Fig.3 (a): Comparison on delay (b): Comparison on Energy Consumption

As shown in figure 3 (a), the delay of the proposed technique is compared with the prior method. Simulation time is low compared to the prior method. As throughput increases, delay measures decrease. Consequently, IoT devices can service each packet with the least amount of delay as the amount of data transmitted decreases. Energy consumption for the proposed method is compared in figure 3 (b). Based on the figure, it can be seen that the rate of energy consumption decreased with an increase in data transfer over simulation time.

Table 1. Data security Ratio (%)

No of devices	DIoTA(%)	FUPA (%)	RF-DECC (%)
10	65	69	83
20	59	63	80
30	50	59	79
40	49	55	78
50	45	52	75

The data security rate of RF-DECC is shown in table. 1. RF-DECC method is focused on enhancing the data security level during the transfer of data among IoT devices. The IoT uses fog computing devices for data transfer protection and database privacy problems. Although certain problems can be dealt with current systems, new difficulties are faced because of different fog computing features such as fog node heterogeneity and fog networks, mobility service requirements, and low latency. User data is outsourced to the fog node, where access to the cloud node. Initially, it is difficult to guarantee data accuracy since the outsourced data can be protected. Secondly, authorized parties may use the uploaded data for other purposes.

5. Conclusion

In this paper, a DNA-based cryptographic technique with clustering algorithm to control data security in fog computing. In first phase, cluster head is chosen using RedFox optimization algorithm. In second phase, once clustering has been completed, the cluster head begins the data encryption process by encrypting cluster members' data with DNA-Elliptic Curve Cryptography (ECC). The proposed method describes higher throughput than DIoTA and FUPA method. As a result of the simulation results, the proposed solution improves throughput and data security while reducing latency and energy consumption. Future development of the proposed work will reduce the risk of hazardous attacks.

References

[1] Mohamed Elhoseny et al., "Hybrid Optimization with Cryptography Encryption for Medical Image Security in Internet of Things," *Neural Computing and Applications*, vol. 32, no. 15, pp. 10979-10993, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[2] Tarek Gaber et al., "Trust-Based Secure Clustering in WSN-Based Intelligent Transportation Systems," *Computer Networks*, vol. 146, pp. 151-158, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[3] R. Surendiran, and K. Alagarsamy, "Privacy Conserved Access Control Enforcement in MCC Network with Multilayer Encryption," *International Journal of Engineering Trends and Technology*, vol. 4, no. 5, pp. 2217-2224, 2013. [CrossRef] [Google Scholar] [Publisher Link]

[4] Mayank Dixit, Jitendra Kumar, and Rajesh Kumar, "Internet of Things and Its Challenges," *2015 International Conference on Green Computing and Internet of Things, IEEE*, pp. 810-814, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[5] Luis M. Vaquero, and Luis Rodero-Merino, "Finding Your Way in the Fog: Towards a Comprehensive Definition of Fog Computing,"*ACM SIGCOMM Computer Communication Review*, vol. 44, no. 5, pp. 27-32, 2014. [CrossRef] [Google Scholar] [Publisher Link]

[6] S. Gavaskar et al., "Three Counter Defense Mechanism for TCP SYN Flooding Attacks," *International Journal of Computer Applications*, vol. 6, no. 6, pp. 12-15, 2010. [CrossRef] [Google Scholar] [Publisher Link]

[7] Jie Lin et al., "A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1125-1142, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[8] Opeyemi Osanaiye et al., "From Cloud to Fog Computing: A Review and a Conceptual Live VM Migration Framework," *IEEE Access*, vol. 5, pp. 8284–8300, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[9] R. Surendiran, and K. Alagarsamy, "A Novel Tree Based Security Approach for Smart Phones," *International Journal of Computer Trends and Technology*, vol. 3, no. 6, pp. 787-792, 2012. [CrossRef] [Google Scholar] [Publisher Link]

[10] Lei Xu et al., "DIoTA: Decentralized-Ledger-Based Framework for Data Authenticity Protection in Iot Systems," *IEEE Network*, vol. 34, no. 1, pp. 38-46, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[11] S. Gavaskar, E. Ramaraj, and R. Surendiran, "A Compressed Anti IP Spoofing Mechanism Using Cryptography," *International Journal of Computer Science and Network Security*, vol. 12, no. 11, pp. 137-140, 2012. [Google Scholar] [Publisher Link]

[12] Arun Murugesan et al., "Analysis on Homomorphic Technique for Data Security in Fog Computing," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 9, p. E3990, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[13] V. Lakshman Narayana, and R. S. M. Lakshmi Patibandla, "An Efficient Fog-Based Model for Secured Data Communication," *Integration of Cloud Computing with Internet of Things: Foundations, Analytics, and Applications*, pp. 41-55, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[14] P. Chinnasamy et al., "Efficient Data Security Using Hybrid Cryptography on Cloud Computing," *Inventive Communication and Computational Technologies*, Springer, Singapore, pp. 537-547, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[15] R. Surendiran, and K. Alagarsamy, "A Crtitical Approach for Intruder Detection in Mobile Devices," *SSRG International Journal of Computer Science and Engineering*, vol. 1, no. 4, pp. 6-14, 2014. [CrossRef] [Publisher Link]

[16] Saeed Javanmardi et al., "FUPE: A Security Driven Task Scheduling Approach for SDN-Based Iot–Fog Networks," *Journal of Information Security and Applications*, vol. 60, p. 102853, 2021. [CrossRef] [Google Scholar] [Publisher Link]